PANEL 2
Thresholds & Technologies: Internet & Information

Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses

by Colonel (Retired) Gary Corn

February 11, 2020

The recent escalation in hostilities between the United States and Iran has raised intense debates about the propriety and legality of both parties' uses of lethal force. These debates highlight the murky and dangerous terrain of grey-zone conflict, the attendant legal ambiguities, both domestic and international, and the risks inherent in aggressively pressing grey-zone strategies up to and across recognized lines set by the U.N. Charter.

Be those debates as they may, one thing seems clear. Despite the temporary pullback from open hostilities, Iran will continue to press its grey-zone strategy through asymmetric means, of which malicious cyber operations are likely to constitute a core component. The need to not just prepare for, but actively counter Iran's ability to execute cyber operations is, as a result, squarely on the table. So too are the difficult questions of how international law applies in the current context and should inform U.S. options.

This reality provides an important backdrop to assessing Chatham House's recent foray into the debate arena over how international law should govern cyber operations below the use-of-force threshold. In this article, I scrutinize Chatham House's report on the international law rule of non-intervention and the principle of sovereignty.

Iran's Strategic and Tactical Posture

The Iranian cyber threat is nothing new. Since at least 2012, Iran has employed near-continuous malicious cyber operations as a core component to its grey-zone strategy of confronting the United States. It has conducted operations ranging from multiple distributed denial of service (DDOS) salvos against US banks to destroying company data in an operation against the Sands Casino, not to mention a number of substantial operations directed against targets throughout the Middle East. Well before the current crisis, the US Intelligence Community identified Iran as a significant cyber threat actor with the capability and intention to at least cause localized, temporary disruptive effects,

and assess that it is actively "preparing for cyber attacks against the United States and our allies." And as these assessments make clear, the Iranian threat is not limited to cyber effects operations against data and infrastructure. In true copycat fashion, Iran is also positioned to engage in online influence and election interference operations a la Russia.

Given this background, it is no surprise that many, like my colleague Paul Rosenzweig, have warned that hostile Iranian cyber operations are likely in the offing. The recent step back from the dangerous escalation of open hostilities that culminated in the strike on Soleimani and Iran's retaliatory missile strike is at best a strategic pause, and more likely a return to the pre-existing, if not an escalated, grey zone conflict in which asymmetric cyber operations form a key component of Iran's modus operandi. Indications are that Iran has stepped up its cyber reconnaissance activities since the strikes and some predict it may conduct a substantial cyber operation to exact revenge or send a message.

United States Strategy and Tactical Posture

And so although the threat is not new, it is now more acute and brings into sharp focus key aspects of the shift in U.S. cyber strategy over the last several years, with its emphasis on persistence and proaction—in particular the concepts of defending forward and persistent engagement. As these strategies and the Command Vision for U.S. Cyber Command make clear, addressing cyber threats such as the one emanating from Iran may require "defend[ing] forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."

As anyone with even a passing understanding of the strategic and operational environment of cyberspace knows, the effectiveness of counter-cyber operations will often depend on speed and surprise. Further, the ability to "[i]dentify, counter, disrupt, degrade, and deter" adversary cyber capabilities and operations will often require interaction with globally distributed, adversary owned or illicitly controlled infrastructure. From the perspective of international law, this implicates not only the rights and obligations of the two states involved, but potentially those of third-party states, for example, those in whose territory adversary-controlled infrastructure resides.

Orientation to International Law

Accounting for the nature of the threat and the particulars of the domain is essential to assessing how international law applies in the cyber context, especially to cyber operations conducted below the use-of-force threshold and how states are likely to approach these issues. In the final analysis, states and states alone are the authors of international law, and they will form views about how the law applies mindful of these realities; realities that will grow increasingly more challenging with the inevitable introduction to cyber arsenals of artificial intelligence, automation, and machine learning. Determining the legal basis for any specific operation aimed at countering or disrupting cyber threats is complex and highly fact specific, and in the absence of clear state practice and *opinio juris,* general claims to customary rules broadly proscribing states' response options should be viewed with caution.

Chatham House's Report and Recent State Pronouncements on International Law

With its recently released report titled, "The Application of International Law to Cyberspace: Sovereignty and Non-Intervention," Chatham house has weighed in on important debates about how international law applies to states' conduct of cyber operations below the threshold of a use of force and outside the context of armed conflict. Focusing on the principle of sovereignty and the rule of prohibited intervention, the report concludes with an overarching recommendation that, given conflicting state views over the normative status of the principle of sovereignty and uncertainties about how it applies in the cyber context, states are better off approaching the regulation of malicious cyber activities through the prism of the customary international law (CIL) prohibition on intervening in the internal affairs of another state.

To a certain extent, this is sound advice. The CIL foundations of the non-intervention rule are much firmer and the rule has the potential to address aspects of foreign influence efforts in ways that the purported sovereignty rule would not. Considering the unprecedented scope, scale, and depth of malicious foreign interference campaigns that cyber capabilities now enable, advocating against overly narrow articulations of the non-intervention rule has resonance. But ultimately the recommendation rests on the report's argument that the rule of prohibited intervention is broader in scope than generally understood, and so it would do much of the same work as the sovereignty rule. However, it is unclear whether the report is arguing a good faith interpretation of existing law or urging states to evolve the rule of prohibited intervention to broaden its ambit in

the cyber context. Ultimately, states will have to determine the best role the non-intervention rule can play in addressing foreign interference, and hence the rules acceptable parameters. At present, it is simply unclear.

The report's preference for approaching the regulation of malicious cyber operations through the lens of prohibited intervention is also premised on the recognition that there is disagreement among states, at least those that have opined publicly, over the normative status of the sovereignty principle, and virtually no agreement as to a definable set of criteria for determining what cyber operations would run afoul of a professed sovereignty rule. As the report correctly notes, overstatements about the principle of sovereignty not only crash head on with the reality of ubiquitous state practice, but "as such could increase the risk of confrontation and escalation" since violations of international law give the affected state the right to take countermeasures—actions that are otherwise unlawful—in response.

Unfortunately, and in spite of acknowledging the divergence of states' views on the sovereignty question, the Report throws its weight on the debate scale in favor of the sovereignty-as-a-rule camp. In this regard, its arguments are neither novel nor availing, and its effort to better define the internal content of a sovereignty rule adds little clarity. More on that below, but first, a little more on the rule of prohibited intervention.

Prohibited Intervention

Russia's ongoing and concerted campaign to interfere in the elections of numerous democratic states, sow dissension, and undermine democratic institutions more broadly is by now evident and has provided a blueprint for other states like Iran seeking to challenge the existing order and weaken Western democracies. The targets of these efforts have struggled to come up with effective responses, due in no small measure to the legal and policy ambiguities surrounding these sub-use-of-force, grey zone operations. States like Russia and Iran are not so much engaging in novel behavior as much as engaging in traditional, albeit adversarial statecraft through technologically new means and methods. It is the qualitative and quantitative difference in impact that calls into question traditional understandings of the existing legal architecture.

That customary international law contains a prohibition against states intervening in the internal and external affairs of other states is not controversial. As evidenced by the 2015 UN GGE report and subsequent official statements from a growing number of states, it is

generally accepted that this prohibition applies to states' activities conducted in and through cyberspace. Like the U.N. Charter prohibition on the use of force, the non-intervention rule derives from the general principle of sovereignty and is intended to protect the same basic sovereign interests in states' territorial integrity and political independence.

The rule is also of finite scope, prohibiting states from employing an ill-defined notion of "coercion" against an equally ill-defined set of core "sovereign prerogatives" of the targeted state to force a particular outcome. According to the International Court of Justice (ICJ), employing forcible measures such as direct military action or indirect support to an insurgency, actions that would also likely run afoul of Article 2(4) of the U.N. Charter, would violate the non-intervention rule. In contrast, states can and routinely do seek to influence the sovereign decisions of other states through a variety of means, even if heavy handed like sanctions, that do not run afoul of international law. Between these extremes, the standard lacks clarity, making it difficult to easily map to the cyber domain or any other domain for that matter. Unfortunately, only a handful of states have offered official views on the application of the non-intervention rule in the cyber context, providing little insight into their views of the rule's internal content.

Like others, the Chatham House report would fill the void of official state views on the subject by pointing to non-binding sources as "useful guidance," such as the ICJ's articulation of the rule in its 1986 Nicaragua decision. These sources generally focus on the element of coercion as the rule's touchstone, the ICJ describing it as "defin[ing], and indeed form[ing] the very essence of, prohibited intervention." Others, drawing on sources such as Oppenheim, who the Chatham House report cites liberally, yet selectively, articulate the rule in slightly broader terms. They assert that to be internationally wrongful, an intervention "must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question." But as Oppenheim also notes, although intervention and interference are frequently used interchangeably, international law only proscribes the former as wrongful. In his view "[i]nterference pure and simple is not intervention," an important limitation on the intent and purpose of the rule's coverage, and directly relevant to the sovereignty debate discussed below.

A number of commentators take a very narrow view of the non-intervention rule's scope, a point with which the Chatham House report takes issue. According to the report's author, writing in Just Security, it rejects "overly rigid interpretation and application" of the ICJ's description of the coercion element as leaving "unacceptable leeway to aggressor states," and setting a threshold of action and harm that will rarely be crossed. In her view, "the non-intervention principle is in practice capable of broader application." Thus, according to the report, the rule should be understood in light of its central focus on protecting the free will of states regarding core sovereign prerogatives and should operate to prevent states from employing pressure, whether successful or not, aimed at overcoming the free will of the target state in an attempt to compel conduct or an outcome involving a matter reserved as a sovereign right to that state.

The report's focus on efforts to overcome the free will of targeted states is understandable and has merit. Actions aimed at subverting a state's free will undermine the sovereign equality of states and the international order, and present a direct threat to international stability, peace and security. Covert disinformation and influence campaigns may not be new, but the internet and cyber capabilities have exacerbated their impact and elevated the risk they pose. The threat has started to galvanize attention and action, but primarily through domestic-law approaches such as Australia's recent national security and foreign interference laws. In those instances where states have reportedly taken more proactive measures to counter foreign influence campaigns, they have not offered a legal rationale.

There is no doubt work to be done on the international law front if states are going to set boundaries around destabilizing influence campaigns. As Eric Jensen and I stated, the non-intervention rule is indeed in need of clarification and perhaps evolution. As we said, the rule should be understood "to encompass actions involving some level of subversion or usurpation of a victim state's protected prerogatives, such as the delivery of covert effects and deception actions that, like criminal fraud provisions in domestic legal regimes, are designed to achieve unlawful gain or to deprive a victim state of a legal right."

Unfortunately, where the report falls short is in proffering greater evidence of state practice and *opinio juris* in support of its broader interpretation of the rule. Given the dearth of official statements on the subject, this is understandable. Nevertheless, the report would have been better to offer its views not in the form of legal conclusions, but

as recommendations for good faith extension or modification of existing law, which is ultimately a policy question reserved for states that must be carefully considered and weighed against the potential impact on external sovereign prerogatives.

Before turning to the sovereignty question, one aspect of the report's analysis is worth particular mention. In challenging an overly narrow construction of the non-intervention rule, the report was quick to downplay the importance of the ICJ's pronouncements on the subject in the *Nicaragua* decision, dismissing them as dicta. On this point, the report is correct. The matters before the ICJ involved forcible measures addressed separately under the court's use-of-force analysis. Further, the court's entire discussion of the non-intervention principle was only for the purpose of dispelling an argument that the forcible measures were justified as countermeasures. As such, its broader pronouncements on the elements of the rule were unnecessary and deserving of limited weight. Unfortunately, when it comes to the issue of the normative status of sovereignty, the report is less circumspect of ICJ pronouncements.

The Sovereignty Debate

On the question of sovereignty, the report unfortunately tacks in a different direction. It relies on the same sort of ICJ dicta it correctly downplayed with respect to prohibited intervention and fails to adequately reflect the marked divergence in states' views on the sovereignty question and its applicability to the cyber context. In so doing, the report elevates in importance factually inapposite ICJ opinions over actual state practice and *opinio juris*. It also adopts the same flawed syllogism used in the Tallinn Manual 2.0 that rests on the erroneous premise that international law contains a blanket trespass rule against states sending their agents into the territory of another state without consent. Overwhelming state practice, most notably in the context of espionage, says otherwise; a point that neither the report nor the Tallinn Manual 2.0 account for adequately.

Where the report diverges with the Tallinn Manual 2.0 is on its views of what actions might constitute violations of the asserted rule of sovereignty, adopting what the author describes as a more holistic approach and concluding that there may be "some form of *de minimis* rule in action." On this point the report, like the Tallinn Manual 2.0, wades deep into uncharted waters without the benefit of even rudimentary navigational tools. Fortunately, here the report does recognize the limits the distinct absence of state practice or *opinio juris* place on any effort to identify the contours of a claimed

sovereignty rule or to assert controlling thresholds, concluding that "[t]he assessment of whether sovereignty has been violated therefore has to be made on a case by case basis, if no other more specific rules of international law apply."

Notwithstanding claims to the contrary, to date only two states, the United Kingdom and the Netherlands, have put on record their positions as to whether sovereignty is simply descriptive of legal personality or a prescriptive primary rule of international law. Their polar opposite views, coupled with the distinct absence of comment on this core question from the handful of states such as Estonia, Australia, and the U.S. that have offered official statements on international law's applicability to cyber operations is *prima facie* evidence of the unsettled nature of the question.

The United Kingdom's position is clear: that as a matter of current international law, there is no "cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent." The U.K. assesses legality against the accepted prohibitions on the use of force and intervention. Based on my professional dealings, there are a number of key states that find sympathy with this view.

The Netherlands takes the opposite view, stating its belief that "respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act." As to what that obligation entails, in what can only be understood as a strong dose of pragmatism the Netherlands is far more vague. Beyond "generally" endorsing the Tallinn Manual 2.0 Rule 4 approach, it notes that in light of the unique nature of cyberspace, the precise boundaries of what may or may not be permissible have yet to crystallize. And in an interesting twist, the Netherlands goes on to intimate that cross-border cyber law enforcement activities may not be captured by the rule, as "[o]pinion is divided as to what qualifies as exercising investigative powers in a cross-border context …." Such an acknowledgment is anathema to strict sovereigntists, and although the Netherlands letter to Parliament is conspicuously silent on the issue, perhaps this was a nod to the difficult question of espionage.

Recently France also lent its voice to the cyber international law discussion. But despite claims to the contrary, including in the Chatham House report itself, France did not assert that sovereignty constitutes a standalone primary norm of international law.

First, it should be noted that despite numerous assertions to the contrary, the French document does not claim to be the official position of the French government. It was written and published by the French Ministère des Armées (MdA), in the same vain as the DoD Law of War Manual which does not necessarily reflect the views of the U.S. Government as a whole. Further, although the MdA does state that cyberattacks, as it defines that term, against French digital systems or any effects produced on French territory by digital means *may* constitute a breach of sovereignty in the general sense, at no point does it assert unequivocally that a violation of the principle of sovereignty constitutes a breach of an international obligation. To the contrary, obviously aware of the debate, the document is deliberately vague on this point and simply asserts France's right to respond to cyberattacks with the full range of options available under international law consonant with its assessment of the gravity of the attack.

Tellingly, while noting that cyber operations are not unlawful per se, the MdA states that it is actively taking "a number of measures to prevent, anticipate, protect against, detect and respond to [cyberattacks], including by neutralizing their effects." Yet when discussing France's right to take countermeasures the document is again vague, and perhaps more so, stating in measured fashion that they are available only when cyberattacks *in fact* infringe international law (with a distinct focus on uses of force)—not simply when they "breach" sovereignty. These are not simply my observations. They were confirmed in discussions with a senior French official involved in the drafting and publication of the document.

The French paper offers a number of important and helpful views on the role international law should play with respect to cyber operations, and the authors should be commended. But it is first and foremost a pragmatic statement of the MdA's views on its authority to proactively respond to malicious cyber operations and is conspicuously silent on whether and how France, or the MdA, feel international law constrains its own freedom of action. Reports that France conducted a mass crypto-currency mining Botnet takedown across multiple states only weeks after publishing the paper is notable in this regard. Simply put, the Chatham House report, like several commentators, places undue weight on the paper and overstates its conclusions on the sovereignty question.

Notwithstanding the documented divergence of states' views, the report relies on ICJ pronouncements in a handful of factually inapposite cases to support its conclusion that sovereignty constitutes a primary rule of international law. This itself raises an import

question about the weight to be given ICJ opinions in general as "sources" of international law; a discussion beyond the scope of this post. Suffice it to say that, although the court's views should not be dismissed lightly, they are often not in conformity with those of the majority of states, and as is evidenced in Article 38(d) of the ICJ statute, states never intended to imbue the court with the power of *stare decisis*.

So while it is true that the ICJ has referred in general terms to violations of sovereignty in certain cases such as Corfu Channel, Certain Activities carried out by Nicaragua, and the 1986 Nicaragua decision, the court's pronouncements were binding only on the parties before it and in each instance the facts ruled on involved substantial military presence, de facto control of territory, and in some instances, violent operations, all of which implicate higher thresholds than the sovereignty-as-a-rule proponents assert.

Further, the pronouncements are often in the form of dicta, which the report relies on selectively. For example, the report ignores the foundational holding in the SS Lotus case that restrictions on states' sovereignty cannot be presumed, citing instead to dicta that, absent a permissive rule to the contrary, states may not "exercise their power in any form" inside the territory of another state. Again, this is an overbroad proposition at odds with extensive state practice in the area of, among other exercises of state power, espionage.

As the report acknowledges, states routinely send agents into the territory of other states without consent, and those agents often alter physical and virtual conditions inside the territory to permit access to and exploitation of information. These activities are broadly recognized as unregulated in international law. Notwithstanding those facts, in an effort to bolster its sovereignty-as-a-rule position, the report follows the Tallinn Manual 2.0's lead and attempts to establish a loose syllogism based on the flawed premise that all physical trespasses violate international law. According to this faulty logic, the entry of a state agent into the territory of another state without consent is a breach of sovereignty; therefore the execution of a close-access cyber operation against a state from within its territory is a breach of sovereignty; and *a fortiori*, remote cyber operations conducted against a state from outside its territory constitute a breach of sovereignty.

The principle of sovereign equality is at the heart of the *Lotus* principle. Turkey's exercise of criminal jurisdiction over a French national in that case involved obvious interference in France's sovereign prerogatives with respect to its national, yet the court found no

impediment in law to Turkey's action. The report disregards the central tenet of the *SS Lotus* case, which is that states are free to act on the international plane except to the extent that their actions are proscribed by clearly identifiable treaty or customary international law. There is simply no evidence that the Lotus principle does not apply with equal force in the cyber context.

In describing the report, the author states that there is no reason the principle of sovereignty "should not apply in the cyber context as it applies in every other domain of State activity." This statement is at odds with the report's own closing observation that in "due course, further state practice and *opinio iuris* may give rise to an emerging cyber-specific understanding of sovereignty, just as specific rules deriving from the sovereignty principle have crystallized in other areas of international law." More important, the statement assumes, counter factually and historically, that sovereignty and the rules that flow from it operate consistently across every other domain of state activity. It does not, and precisely for reasons grounded in the very bundle of sovereign rights and obligations that the paper references.

States' rights flowing from internal and external sovereignty are frequently in tension, and it is only through a process of accommodation that states consent to restrictions on their external sovereign prerogatives—accommodations that start from the Lotus principle and are almost always context specific. Even Judge Alvarez, one of the original judges to sit on the ICJ and a staunch advocate of the court having expansive power to "remodel international law" recognized in his *Corfu* dissent that the rights and obligations that sovereignty confers on states:

> are not the same and are not exercised the same way in every sphere of international law. I have in mind the four traditional spheres—terrestrial, maritime, fluvial and lacustrine—to which must be added three new ones—aerial, polar and floating (floating islands). The violation of these rights is not of equal gravity in all these different spheres.

Had it existed at the time, he would have certainly added to his list the cyber sphere, and like the accommodation of competing sovereign interests reflected in the rule of transit passage *sub judice* in Corfu Channel, it remains for states to settle on any prescriptive regime that would limit their external prerogatives in cyberspace beyond the domain agnostic prohibitions against the use of force and prohibited intervention.

Having adopted the sovereignty-as-a-rule approach, the report turns to an unavailing effort at identifying the rule's content. It points to a number of flaws in the Tallinn Manual 2.0 Rule 4 approach, correctly highlighting the dissension among the Tallinn contributors on how the purported rule operates in practice. I have commented on these weaknesses (here, here, and here). The report correctly rejects an absolutist view of the purported sovereignty rule as unsupported by state practice and dangerously escalatory. To this critique the report should have added that such an overbroad rule would be too constraining to states' ability to conduct effective counter-cyber operations by limiting them to the cumbersome and problematic remedy of countermeasures, which Eric Jensen and I have pointed out.

In rejecting this absolutist view, the report claims to take a more holistic approach to the issue and states that some threshold must be at play. In so doing the report repeats a number of the same unsubstantiated claims as the Tallinn Manual 2.0 and ignores Oppenheim's admonition that mere interference in the internal affairs of another state is to be distinguished from prohibited intervention. Further, the report provides no evidence of state practice or *opinio juris* to demonstrate that states agree or that they would declare such a threshold to be anything other than the non-intervention rule. In fact, a number of the examples offered in the report in support of its sovereignty argument directly implicate prohibited interventions. To the author's credit, on these points the report is more prudent in its approach, concluding that there is currently insufficient evidence to establish governing thresholds as a matter of customary international law.

The paper closes with a number of recommendations to states that, although likely unintentional, lose some persuasion by straying at times from recommendatory to prescriptive, such as telling state intelligence agencies and foreign services how to coordinate their strategic communications. As I noted at the beginning, of greater value is the report's overarching recommendation that states focus on evolving the rule of non-intervention as the most effective tool for establishing greater normative boundaries around state actions in the cyber domain while preserving space for states to execute effective counter-cyber strategies. The real-world scenario I described involving the threat from Iran is a good case study. It is difficult to imagine states like the United States and others that are increasingly on the receiving end of these malicious activities will rally around the sovereignty rule that Chatham House articulates. In the face of concrete and persistent cyber threats from states like Iran, Russia, China, and North Korea, states

will of necessity need to ensure that international law evolves not only to deter irresponsible behavior but to do so in a way that preserves victim states' ability to detect, disrupt, and counter cyber threats.

About the Author(s)

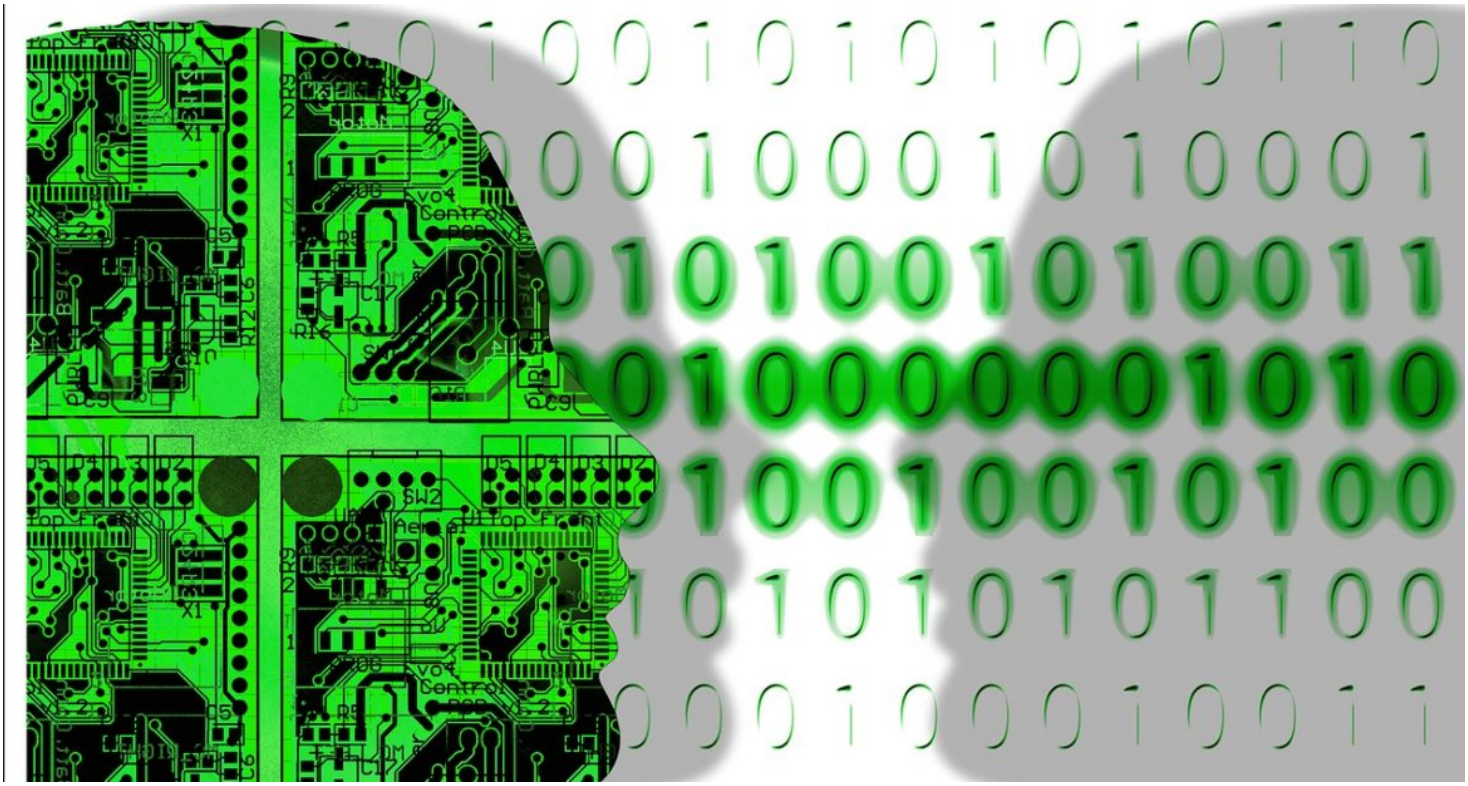
Gary Corn

Director of the Technology, Law & Security Program and Adjunct Professor of Cyber and National Security Law at American University Washington College of Law; retired U.S. Army Colonel; served as the Staff Judge Advocate to US Cyber Command and as a Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff

The human nature of international humanitarian law

August 23, 2018, Analysis / Autonomous Weapons / Conduct of Hostilities / Law and Conflict

Eric Talbot Jensen



International humanitarian law (IHL) regulates the use of force in armed conflict. It inherently provides protections to victims of armed conflict while humanizing, at least to some degree, some of man's most inhumane acts. Thus, IHL principles of distinction, humanity, unnecessary suffering and proportionality serve to temper the application of military necessity. In an age of emerging technologies, the international community is deep in discussion about how these principles will be applied, particularly in weapon systems that will make autonomous decisions involving life and death through the application of machine learning and the development of artificial intelligence.

Such discussions should cause us to reflect on a foundational question with respect to the application of IHL—**Is the law regulating armed conflict designed to provide the 'best protections possible' for victims of armed conflict or the 'best protections humanly possible?'** In other words, the current standards for general IHL compliance are often described in terms of human decision-making, i.e., a human commander must make a specific lega determination such as with proportionality as discussed below.

Does this mean that the actual legal standard is tied to human decision-making? If the standard is 'bes humanly possible', then any emerging technology would have to remain subject to human determinations of IHL application, including the recognition that these decisions will continue to be subject to human oversight and potential human error. Note that the ICRC has made two relevant statements applicable to this question *[1]*.

If, however, the requirement is the 'best possible' application of IHL, and we have any belief that autonomous weapons—or artificial intelligence or weapons using machine learning—can factually apply force in a way that in at least some circumstances results in better protection for humans, then w reach a different result. In this case, the international community should be encouraging the development of autonomous weapons that apply machine learning or artificial intelligence on the battlefield because they might (are likely to) be able to apply the legal requirements of IHL in a way tha results in greater protections for victims of armed conflict.

It should be noted at this point that every weapon system, including any autonomous weapons that apply machine learning or artificial intelligence, must undergo and meet the requirements of a *weapon review*. There is no legal possibility of fielding weapons that do not comply with all the requirements of a legal review. The significance of determining the role of a human in a lethal targeting decision is to provide the foundational rationale for that review. For an autonomous weapon to be fielded, it absolutely must be thoroughly tested and prove that it can apply IHL correctly on the battlefield.

The important question raised here is the standard for that review. If that standard is that the weapon system is to be able to apply the law in a way to provide the best protections humanly possible, then certain types of autonomous capabilities need not be researched and developed. However, if the standard is to apply IHL in a way that results in the best protections possible to potential victims of armed conflict, a vast array of possible autonomous weapons that utilize machine learning and artificia intelligence without real-time human involvement may now be capable of development and deployment.

Principle of distinction

Best protection humanly possible

To illustrate the difference between 'best protections possible' and 'best protections humanly possible consider the principle of distinction (e.g., *here* and *here*). Under IHL, every individual who engages in ar attack has an obligation to apply the principle of distinction. In particular, it is unlawful to ever target civilians. It is also unlawful to not take feasible precautions to protect civilians that might be incidentally injured or killed from an otherwise lawful attack. Failure to comply with these legal requirements is a violation of the law of war. Members of armed forces can be held individually criminally liable for failures to properly apply distinction, and assertions are routinely made alleging such violations.*[2]*

At the same time, few who have been in armed conflict will argue that mistakes never happen and that civilians are never wrongly, though unintentionally, targeted. Often these cases of unintentional death occur through a misapplication of the principle of distinction, based on a failure of intelligence, or sometimes just human error. In such decisions, the ability to quickly gather and analyze all available data on a target will often make the difference to a military commander who is making the targeting decision.

Best protection possible

Now, consider an autonomous weapon system that is tied to a vast array of sensors and designed to incorporate machine learning which can gather and analyze huge amounts of data much more quickly than the human brain. It might be able to do this, for example, by possessing greater capability to discern the difference between a hostile fighter and a non-hostile civilian in a crowd of people, based o sensors spread across the area that are providing otherwise unobservable data on the individuals in the crowd. Note that autonomous systems, driven by machine learning, have already demonstrated the ability to outperform humans when conducting very intricate and complex analyses, such as *correctly diagnosing medical conditions* and *playing complex games*.

If such a system could be fielded with a statistically better chance of reaching a correct distinction conclusion based on the ability to more quickly gather and analyze a much larger set of data, it would likely result in a decreased chance of innocent deaths. From a view of IHL where human decision-making is not an integral part of legal compliance, it doesn't matter that a human was not applying the principle of distinction. Rather, what matters is that the principle was applied correctly more often or that the death and injury to civilians was less than when compared to the result of human decision-making.

Principle of proportionality

Best protection humanly possible

Similarly, consider the application of *proportionality*. Commanders are obliged to refrain from attacks ir which death or injury to civilians and/or damage to civilian objects would be excessive to the concrete and direct military advantage anticipated from the attack (*API Article 51*). Perhaps the most 'human' aspect of that decision is the balancing of the anticipated military advantage and the potential collatera

damage. For those who believe IHL requires the best decision 'humanly' possible, the human aspect of that decision is likely very important, even if the outcome of some proportionality decisions are strongly criticized.

Under this view, where no lethal targeting decision without human input can comply with IHL, talk of technological innovation must be tied to creating better ways to support humans in their inherently human decisions. This view does not make AI and machine learning research and development useless, but it should scope such research and development in a way that is designed to support the human decision-maker, not to create an independent decision-maker.

Best protection possible

For those who believe that the 'best' application of IHL, such as the principle of proportionality, is the one that results in the least collateral damage while still accomplishing the military mission, an autonomous decision or one based on machine learning or artificial intelligence may result in a 'better' application of the principle because it has the potential to result in fewer civilian casualties.

Technology optimists

A technology optimist will believe that the ability for autonomous weapons to come to 'better' conclusions than humans is absolutely possible, and in fact, probable in certain situations given enough research and development. An autonomous weapon system that is not affected by emotions (such as anger, fear and aggression) or subject to physical limitations (such as limited senses, fatigue or an inability to quickly process all the factual data available at the point of decision) is likely going to be able to apply these principles in a more legally compliant way. To the extent that the optimistic view of technology is accurate, it seems clear that the international community should be strongly encouraging the research and development of autonomous weapons with these capabilities in order to enable humans to more accurately apply IHL principles. If autonomous weapons that apply machine learning or artificial intelligence could be developed, and more civilian lives could be spared, some will even argue that States will have an obligation to develop such weapons.

Technology skeptics

In contrast, technology skeptics will argue that such technology does not currently exist and is unlikely to ever be developed. Therefore, we should not research and develop these technologies for application in weapons or at least we should move forward with great caution. Skeptics argue that there is significant uncertainty that such research and development will ever result in machine learning or artificial intelligence that will demonstrate an ability to apply IHL principles in a way that produces 'better' results than humans.

Role of human decision-making in IHL

Despite the fact that there may be reason for serious caution as to the path technology will take with respect to decision-making capability, technology skeptics often do not really address the fundamental

issue of the role of human decision-making in IHL. Whether or not research and development is likely to reach a successful conclusion is not determinative as to whether States who take a more optimistic view can/should engage in research and development to that end. **Rather, the fundamental question is if IHL precludes non-human decision-making with respect to the application of lethal force such that States are precluded from pursuing these technological developments.**

And so, as technology continues to develop, the issues concerning the development of AI and machine learning as part of autonomous weapon systems come back to the fundamental question of whether IH requires the best 'human' application of the law or simply the best 'possible' application of the law. Th fact that it may be possible, sometime in the future, to have IHL applied in a way that reduces the death and injury to civilians because of the application of non-human decision-making should encourage us to consider and answer this question now.

Footnotes

[1] ICRC Statement, 18 April 2018 at the Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts on Lethal Autonomous Weapons Systems: *Towards limits on autonomy in weapon systems*; ICRC Statement 15 November 2017 at the Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts on Lethal Autonomous Weapons Systems: *Expert Meeting on Lethal Autonomous Weapons Systems.*

*[2]*ICTY, Prosecutor v Ante Gotovina, Ivan Čermak and Mladen Markač, Judgment, IT-06-90-T, Trial Chamber I, 15 April 2011 (*Gotovina Trial Judgment*); ICTY, Prosecutor v Ante Gotovina and Mladen Markač, Judgment, IT-06-90-A, Appeals Chamber, 16 November 2012 (*Gotovina Appeals Judgment*).

***

Related blog posts

- *Autonomous weapons: Operationalizing meaningful human control* **Merel Ekelhof**
- *Human judgment and lethal decision-making in war* **Paul Scharre**
- *Autonomous weapon and human control* **Tim McFarland**
- *Autonomous weapon systems: An ethical basis for human control?* **Neil Davison**
- *Autonomous weapon systems: A threat to human dignity?* **Ariadna Pop**
- *Ethics as a source of law: The Martens clause and autonomous weapons* **Rob Sparrow**
- *Autonomous weapons mini-series: Distance, weapons technology and humanity in armed conflict* **Alex Leveringhaus**

Introduction to Mini-Series: Autonomous weapon systems and ethics

Tags: *AI*, *artificial intelligence*, *autonomous weapons*, *AWS*, *CCW*, *human control*, *IHL*, *law of armed conflict*, *LAWs*, *LOAC*, *machine learning*, *protection*, *weapons reviews*

Comments

STEPHANE OJEDA, 24 August 2018

Thank you so much for this very interesting and thought-provoking article. One issue I am struggling with is how can machines better apply IHL rules or concepts that humans do not even agree upon or interpret differently? Will each government program machines according to its own interpretations of IHL? Even the core principles are not agreed upon. Fo instance, you write "it is unlawful to ever target civilians", well actually you can target civilians as long as they take a direct pa in hostilities, but there is no universal agreement on the constitutive elements of such "direct participation". I fully agree with you that we should ask ourselves such hard questions now. Thanks again.

Leave a comment

*Name **

*Email address * This is for content moderation. Your email address will not be made public.*

The Technicolor Zone of Cyberspace – Part I

by Colonel (Retired) Gary Corn and Eric Jensen

May 30, 2018

The Right Honourable Jeremy Wright's recent remarks at Chatham House on Cyber and International Law in the 21st Century added a welcome dash of color to the otherwise gray zone of cyberspace. While full-HD resolution may still be in the offing, this all-too-rare official pronouncement of opinio juris reinforces the baseline maxim that existing international law applies to states' activities in cyberspace and provides some needed clarity on how certain key provisions of international law govern interstate relations at and below the threshold of armed conflict. As the Attorney General notes, the efficacy and resilience of the international rules-based order depend on states' being open and clear about their understandings of, and commitment to international law. Just as important is his reminder that international law is not static and if it is to remain relevant must "adapt to meet the particular demands" of the modern world and the unique security threats that cyberspace presents. In this regard, his pronouncements on the applicability of the jus ad bellum and the principle of non-intervention to cyber operations, the normative role sovereignty plays in cyberspace, and the substantive requirements of countermeasures are important contributions to advancing understandings of international law's role in regulating states' use of this emerging technology. In this post we offer comment on the first two points. We will address the Attorney General's important statements on sovereignty and countermeasures in a follow-on post.

For a growing number of states, cyber operations are now firmly ensconced as a means of conducting traditional and not-so-traditional statecraft, to include conflict. Cyberspace has delivered tremendous benefits, but its unique construct and ubiquity have also created significant national security vulnerabilities, generating unprecedented challenges to the existing framework of international peace and security. One need look no further than North Korea's destructive and subversive actions against Sony Pictures,

its launch of the Wannacry ransomware, Russia's launch of the indiscriminate NotPetya malware against the Ukraine, or its cyber-enabled covert influence campaigns against the U.S. and other western democracies to realize that cyber capabilities are increasingly part of a powerful arsenal states are using to pursue their interests, oftentimes through aggressive actions aimed at disrupting the status quo. As the recently released Command Vision for US Cyber Command recognizes, the emerging cyber-threat landscape is marked by adversary states engaging in sustained, well-constructed campaigns to challenge and weaken western democracies through actions designed to hover below the threshold of armed conflict while still achieving strategic effect. And as the Cyber Command Vision also makes clear, passive, internal cyber security responses have proved inadequate, ceding strategic initiative and rewarding bad behavior.

The UK's position on this is point is now clear: Both in peacetime and in conflict, states cannot engage in hostile cyber campaigns free of consequence. "States that are targeted by hostile cyber operations have the right to respond to those operations in accordance with the options lawfully available to them and that in this as in all things, all states are equal before the law." Actively contesting adversaries in and through cyberspace must form a key component to any strategy aimed at defeating these threats and reinforcing norms of acceptable and unacceptable state behavior. The Attorney General's remarks implicitly, if not explicitly, recognize that international law must take account of this increasingly evident reality.

At the same time, not all unfriendly or even prejudicial actions by one state against another constitute breaches of international law, whether effected through cyberspace or otherwise. Understanding the line between internationally wrongful and permissible cyber operations is therefore critical to framing legitimate cyber strategies and response actions. The customary laws of state responsibility provide the start point for properly analyzing and characterizing these malicious cyber activities and the response options available to victim states.

The customary law of state responsibility, reflected in much of the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts, holds that states are legally responsible for acts or omissions that are both attributable to them and that constitute a breach of an international obligation of the responsible state. Where these constituent elements are met, victim states have recourse to a range of

remedies, to include certain self-help measures that themselves would otherwise be considered breaches of international law. A victim state's use of force in response to an imminent or actual armed attack by another state being a case in point.

The Attorney General's remarks are a welcome contribution to advancing the understanding of the state-responsibility framework and its application to state-mounted cyber operations. Four points are of particular importance. First is the Attorney General's affirmation of the generally accepted view that the jus ad bellum governs states' activities in cyberspace. Second is his recognition that considering the novel vulnerabilities attendant to new technologies, the rule of non-intervention has taken on new importance. Third is the U.K.'s emphatic rejection of the assertion that, beyond the jus ad bellum and the rule of prohibited intervention, international law includes a primary rule of territorial sovereignty that would bar cyber activity. Last is the Attorney General's recognition that the extant law of countermeasures must adapt to the realities of cyberspace and the unique nature of the threat. For now, we limit comment to the first two of these important points.

The Jus ad Bellum

While important, the AG's reaffirmation of the applicability of Articles 2(4) and 51 of the UN Charter to state actions in cyberspace is perhaps the least remarkable aspect of his speech. Notwithstanding some retrogression in the last round of the UNGGE, by and large states have accepted this view. Other than intimating that attacks such as Wannacry that target essential medical services might trip the armed attack threshold, his remarks avoid edge cases. The high level of destruction attendant to the Attorney General's hypothetical examples that would qualify them as armed attacks are clear cases and consistent with views presented in the DoD Law of War Manual as well as Tallinn 2.0. While this will leave some critics unsatisfied, perhaps their expectations are unreasonably high.

Given the spate of malicious cyber operations mounted over the last few years, especially Russia's aggressive activities, calls for action are reaching a crescendo. Recent reports of Russia's hacking of U.S. energy and other critical infrastructure and the poisoning of Sergei Skripal and his daughter in the UK will only add to the pressure to respond. Whether and how to hold states like Russia accountable for such actions is ultimately a

political question. And while it is certainly a fair and relevant question whether Russia's actions, individually or taken together, rise to the level of a use of force or armed attack in violation of the U.N. Charter, it is not one likely to yield a satisfying answer.

Greater understanding of the use-of-force and armed attack legal triggers and how they apply to cyberspace is, of course, vital to evolving and strengthening the international rules-based order, and perhaps to deterring malicious cyber operations. However, in the absence of physical harm to individuals or tangible things, there is little consensus on whether or how cyber operations might constitute breaches of these rules. Further, the prevailing view is that most, if not all, documented cyber actions taken by states to date have fallen below the "use of force" threshold. More important, in the absence of political will to use armed force in response to Russian election interference or other malicious cyber actions, the question of whether a cyber operation might constitute an unlawful use of force or armed attack is at best one of limited utility.

In light of the lack of certainty as to how international law applies to cyber and information operations below the threshold of armed conflict, and the obvious brazenness with which Russia has operated to date, the visceral "casus belli" reactions are understandable. Unfortunately, from the perspective of sound policy and strategy development, framing the question in the dichotomy of war and peace is not particularly helpful and perhaps even counterproductive for at least two reasons. First, such reactions are based on a dangerously flawed premise—that armed conflict can be legally or factually confined to the single operational domain from within which it is initiated. That's not so as militarized conflict in the cyber realm can easily trigger actions and reactions in the kinetic realm. The so-called and oft invoked "cyber war" is simply a misnomer. Second, the gap between such rhetoric and inaction only serves to amplify the costs some, like Jack Goldsmith, have identified and risks distorting policy discussions.

That, of course, does not mean that a victim state is left without options. For example, the U.S. has made use of a mix of sanctions and other diplomatic responses, all in the category of retorsions. However, as both the former and current Commanders of Cyber Command have testified before Congress, none of these prior responses seems to have been effective in stopping or deterring Russia or other adversaries like China, the DPRK, or Iran, from continuing to push boundaries and engage in malicious cyber operations. Retired General Michael Hayden echoes this assessment and calls for "a legal and policy

zone that authorizes robust, sometimes destructive responses, well above normal peacetime competition but below what we would define as the threshold of conventional conflict and open interstate war." Absent Security Counsel authorization, the legal zone he seeks per force rests on a predicate finding that Russia has violated international law which would preclude the wrongfulness of the countermeasures he alludes to. Greater clarity on the international rules governing these more pervasive sub-use-of-force cyber operations is therefore of much greater value to reinforcing the international rules based order than continued focus on jus ad bellum thresholds. It is here that the U.K. Attorney General's remarks offer the greatest elucidation.

Prohibited Intervention

The customary international law rule that some sub-use-of-force interventions into the sovereign affairs of another State are considered internationally wrongful is also well established. The Attorney General's affirmation of the non-intervention rule's applicability to cyberspace and the concomitant implication that violations trigger a state's right to employ countermeasures in response is an important contribution to buttressing the normative framework governing state behavior below the level of a use of force. The prohibition on intervention protects against certain impairments of a state's sovereignty below the threshold of a use of force, and the Attorney General is correct to note the rule's "particular importance in modern times when technology has an increasing role to play in every facet of our lives, including political campaigns and the conduct of elections." At the same time, not all infringements on the sovereign interests of another state fall within the scope of the rule, and the Attorney General is also correct to note that the precise boundaries of the interests protected by the rule as well as the nature and scope of conduct it proscribes remain the subject of debate. However, beyond offering some examples as self-evident violations, including an interesting assertion that cyber operations aimed at destabilizing the UK's financial sector would qualify, the speech unfortunately misses an opportunity to better illuminate the UK's views on the vague language of the International Court of Justice's *Nicaragua* decision so often cited as defining the rule's elements, or how those elements might be adapted to account for the modern exigencies of cyberspace. In the meantime, greater insight into the non-intervention framework will have to be found elsewhere.

Citing the *Nicaragua* decision, the rule is generally described as prohibiting forcible, dictatorial, or otherwise coercive measures against a relatively limited but important zone of sovereign interests falling within what is commonly referred to as the state's *domaine réservé*. The *domaine réservé* is generally understood to refer to those matters reserved in international law to the sole prerogative of states, matters such as the right to choose a political, economic, social, and cultural system, and to formulate and execute foreign policy. As noted in Tallinn Manual 2.0, a state's choice of both its political system and its organization is a "matter most clearly within a State's *domaine réservé,*" and coercive actions that deprive or substantially impair a State's freedom of choice—for example over the democratic selection of its political leaders—by forcing it to take or refrain from taking an action against its will, are prohibited. In this, the Attorney General's remarks are entirely consistent with prevailing views.

Unfortunately, as David Jens Ohlin notes, "despite the patina of precision in its French rendering, the concept [of *domaine réservé*] has little internally generated content." Nor is the concept without limits. Those "domains or activities" not strictly reserved to states fall outside of the rule's zone of protected interests—for example purely commercial activities and matters otherwise subject to international legal regulation. Like international law itself, the concept of *domaine réservé* is of necessity malleable and subject to evolution over time. Notwithstanding, a more precise articulation of the boundaries between protected and unprotected interests would better serve international peace and security by placing states on greater notice of the areas of interference most likely to generate legal consequence and potentially escalatory responses.

In even greater need of clarification, and perhaps evolution, is the element of coercion. As others have pointed out, overly rigid interpretation and application of the ICJ's description of this element leaves unacceptable leeway to aggressor states. We submit that the ICJ's framing of prohibited intervention solely in terms of coercion was imprecise and, when applied dogmatically, fails to capture significant modes of state action that could be considered internationally wrongful.

By definition, coercion involves an element of force or the threat thereof to achieve an intended result. As set out in the *Nicaragua* decision, there is no question that use of a level of force violative of Article 2(4) would constitute the "lesser-included offense" of prohibited intervention. However, leaving aside debates about the existence of a force gap between uses of force and armed attacks, in this sense the prohibition adds little if

anything to the jus ad bellum framework set out above. For the prohibition to have any true normative effect *below* the use-of-force threshold, the ICJ's recitation of the actus reus element of the prohibition must be understood as encompassing more than forceful deprivations. Its scope must be understood to encompass actions involving some level of subversion or usurpation of a victim state's protected prerogatives, such as the delivery of covert effects and deception actions that, like criminal fraud provisions in domestic legal regimes, are designed to achieve unlawful gain or to deprive a victim state of a legal right. For example, covertly disseminating on the eve of an election false information that a candidate for office had dropped from the race would likely deprive the victim state of a free and fair electoral process without using coercion in the most common senses of the term.

As Steven Barela argues, perhaps better understanding of the rule's force and effect as applied to cyber operations can be found in an unlikely source—the Special Counsel's indictment of the thirteen Russians and three Russian organizations. In essence, the Mueller indictment reveals a compelling exposition, albeit in the vernacular of U.S. domestic law, of a prohibited intervention into the U.S. electoral process, the overall gravamen of the indictment being that the Russians' "knowingly and intentionally conspired . . . to *defraud* the United States by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes . . ." The rich set of facts of intervention set out in the indictment are only buttressed by the Intelligence Community's report on Russia's influence campaign targeting the 2016 election and its attribution to Russia of the DNC hack.

Professor Michael Schmitt, who led both Tallinn Manual processes, points to the link between a domestic crime and an internationally wrongful act of intervention, arguing that "when you engage in what is a domestic crime to distort the electoral process, then in that case you are intervening in the internal affairs of another state." The connection Schmitt draws between the domestic crime committed and the principle of unlawful intervention reinforces the instructive value of the Mueller indictment for international law. According to Paragraph 28 of the indictment, the "conspiracy had as its object impairing, obstructing, and defeating the lawful government functions of the United States by dishonest means in order to enable the Defendants to interfere with the U.S. political and electoral processes, including the 2016 U.S. presidential campaign." Against the backdrop of the U.S. Government separately attributing the election meddling to

Russia and the IC's assessment that Russia's harmful activities are ongoing and aimed at impacting the 2018 mid-term elections, the charge of conspiracy to impair lawful government functions by means of fraud and deceit seems a clear case of prohibited intervention in violation of international law.

The Attorney General calls for states to accept the responsibility to be clear about how international law obligations bind them. In this regard, perhaps his speech could have done more to clarify the scope of the jus ad bellum and the non-intervention rule as applied to state activities in cyberspace. Nevertheless, his declaration of the UK's view on the applicability of these baseline obligations is an important contribution to greater transparency and understanding of the normative structure surrounding this new technology. With respect to other aspects of international law as applied to cyberspace, namely sovereignty and countermeasures, Mr. Wright's statement adds considerably more. But that is for our next post.

The views expressed are those of the authors and do not necessarily reflect the views of the United States Cyber Command, the Department of Defense, or the U.S. Government.

Image: Getty

About the Author(s)

Gary Corn

Director of the Technology, Law & Security Program and Adjunct Professor of Cyber and National Security Law at American University Washington College of Law; retired U.S. Army Colonel; served as the Staff Judge Advocate to US Cyber Command and as a Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff

Eric Jensen

Professor at Brigham Young Law School, Special Counsel to the General Counsel of the Department of Defense, Former Chief of the Army's International Law Branch, and Former Legal Advisor to US Military Forces in Iraq and Bosnia

The Technicolor Zone of Cyberspace, Part 2

by Colonel (Retired) Gary Corn and Eric Jensen

June 8, 2018

In Part I of this two-part post, we outlined the importance of United Kingdom Attorney General Jeremy Wright's recent speech setting out the UK's views on cyber operations and international law. In that post, we focused on two of the four most salient points of his speech: the applicability of the jus ad bellum and the rule of prohibited intervention to cyber operations. As we noted, Wright's comments on these two central primary norms were an important contribution to reinforcing international law's role in regulating states' activities in cyberspace. We also identified some aspects of these primary norms in need of clarification, or perhaps of adaptation to the particularities of cyberspace as the attorney general correctly counseled, but did not necessarily provide. We now return to his speech to discuss the two remaining and much more groundbreaking points that he made: the normative status and applicability of the principle of sovereignty to cyberspace, and the content of the rule of countermeasures as a self-help remedy to cyber-enabled breaches of international law.

Sovereignty

We pointed out in our last post that when appropriately applied, and perhaps adjusted to account for the novel threats presented by emerging technologies, the rule of prohibited intervention can serve as a powerful tool for enforcing acceptable state behavior in cyberspace. However, the prohibition does not bring within its scope all sub-use-of-force cyber activities and must be distinguished from mere interferences in the internal affairs or against the sovereign interests of another state. This raises the important question of whether, and if so, how, international law regulates cyber activities that fall below the threshold or outside the scope of a prohibited intervention. It is on this point that the attorney general's speech does its most important work in offering the UK's resounding

rejection of the existence of a primary norm of territorial sovereignty, which would make internationally wrongful a nonconsensual interference in the computer networks of another state.

Although the shortest part of his speech, Wright's statement on sovereignty is perhaps the most impactful. In less than 100 words he summed up the current debate on the issue of the normative force of sovereignty in cyberspace and made crystal clear the UK's position:

> "Some have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law."

Since at least the launch of Tallinn 2.0., a lively debate has been had among academics, practitioners and commentators over whether sovereignty exists as a primary rule of international law applicable to cyber operations, the violation of which would be an internationally wrongful act in and of itself, or as a foundational principle, which could only be violated by infringing on some other sovereignty-based primary rule.

As one of the authors of this post, along with his co-author Robert Taylor, argued here, contrary to the views expressed in Tallinn 2.0, and separately by some of its authors, there is insufficient evidence of either state practice or opinio juris to support claims that the principle of sovereignty operates as an independent primary rule of international law that regulates states' actions in cyberspace. The UK clearly comes down on the sovereignty-as-principle-vice-rule side of the ledger.

The significance of Wright's statement on sovereignty cannot be overstated. Until now, no states have offered an official view on this fundamental issue. Hence, his speech is an extremely important statement by one of the major cyber powers in the international community. That alone is worthy of note. In addition, how states ultimately resolve the

sovereignty question will have a profound impact on the options available to them to confront the growing threats emanating from, or enabled by, cyberspace. In this regard, the substance of the UK's position is even more significant.

Since its inception, the concept of sovereignty has been tightly tied to geography. The same cannot be said of cyberspace. There is at most a tenuous connection between geography and the logical and social layers of cyberspace, i.e., the software, protocols, and data that combine to generate outputs, and the various digital identities and aliases of the human users of the internet. Further, the undeniable reality is that owing to the nature and construct of cyberspace, malicious cyber operations are nearly always mounted from globally dispersed and often coopted infrastructure. Countering these threats without implicating at least some of these nodes in third-party states is nearly impossible. One of the authors previously pointed this out in the context of a non-state terrorist organization's use of the internet to conduct or facilitate its operations, and the impact the sovereignty issue has on a state's ability to confront this threat. The same holds true equally, if not more, in the context of state-sponsored or conducted malicious cyber operations where their offensive capabilities are likely far more substantial.

As the problem highlights, a robust view of sovereignty as a rule would preclude any action against the aggressor's cyber infrastructure without the consent of the third-party state. Wright made clear in his speech that such a sweeping rule is too strong and not supported by current international law. Rather, a state wishing to take action to disrupt malicious cyber operations, terrorist or otherwise, must certainly consider sovereign interests before taking non-consensual activity on the IT infrastructure located within the territory of a third-party state, but seeking advance permission of that state in all cases is not required as a matter of international law. Activities that themselves do not breach the rule of prohibited intervention are legally available options of response.

Academics and commentators who oppose Wright's view point to due diligence and the plea of necessity as affording viable response options to victim states. The myriad reasons these assertions prove unavailing are too numerous to address here. Suffice it to say that even assuming these rules apply, under the most generous reading of them, victim states would still be unreasonably constrained from adequately responding to malicious cyber actors leveraging globally dispersed infrastructure. As Wright intimates, ceding that type of operational maneuver space to aggressors is unsustainable.

This is not to say the attorney general's declaration is conclusive on the issue. It is the considered view of but one state, and more will have to weigh in on the matter before firm conclusions can be drawn about the status of the debate. Hopefully, more states will heed Wright's call to do so. In the meantime, as a clear expression of opinio juris, his declaration on the normative status of sovereignty not only moves the debate where it needs to be—in the hands of states—but does so by setting the tone and bringing a sorely needed degree of clarity to this critical question.

Countermeasures

As is the case with the issue of sovereignty, much has been written on the potential use of countermeasures in cyber operations, including a full analysis in the Tallinn Manual, a discussion of the inequities between countermeasures and self-defense, and a caution on the potentially escalatory nature of cyber countermeasures. Wright's statement adds critical understanding to how at least one cyberpower views the role of countermeasures with respect to cyber operations.

Countermeasures are traditionally viewed as otherwise unlawful actions that do not amount to a use of force, but are considered lawful when taken for the sole purpose of causing another state to stop its unlawful conduct. According to Article 53 of the Draft Articles on Responsibility of States, because of the connection to an original unlawful action, countermeasures must be reversible and must be terminated as soon as the violating state returns to lawful compliance. Further, the use of countermeasures must be necessary and proportionate. Wright confirmed these traditional requirements on the use of countermeasures:

> "Consistent with the de-escalatory nature of international law, there are clear restrictions on the actions that a victim state can take under the doctrine of countermeasures. A countermeasure can only be taken in response to a prior internationally wrongful act committed by a state, and must only be directed towards that state. This means that the victim state must be confident in its attribution of that act to a hostile state before it takes action in response. In cyberspace of course, attribution presents particular challenges, to which I will come in a few moments. Countermeasures cannot involve the use of force, and they must be both necessary and proportionate to the purpose of inducing the hostile state to comply with its obligations under international law."

Another traditional limitation on a state's use of countermeasures is that the state contemplating the use of countermeasures must put the violating state on notice of the illegality of their actions and of the impending use of countermeasures in order to allow them a chance to stop the illegal activity. With respect to this aspect of countermeasures in cyber operations, Wright's statement signaled a significant departure.

> These restrictions under the doctrine of countermeasures are generally accepted across the international law community. The one area where the UK departs from the excellent work of the International Law Commission on this issue is where the UK is responding to covert cyber intrusion with countermeasures.
>
> In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it. The covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.

The Tallinn Manual came to a similar conclusion, noting "the Experts agreed that if notification of intent to take a countermeasure would likely render that measure meaningless, notice need not be provided."

Wright's statement of opinio juris is important not only in clarifying that the traditional requirements generally apply, but perhaps more importantly in denouncing the notice requirement. In addition to the simple statement of law, it reflects that state's will understand the application of cyber norms in a very practical way. Wright's justification for the UK's departure from the accepted norm was not a legal one, but rather a practical concern about the sensitive nature of cyber operations. The signal that cyber norms will be governed by the unique nature of cyber operations, even when it might require the evolution of accepted legal requirements is an important clarification for international law.

Finally, Wright confirmed that countermeasures are not bound by the nature of the original violation.

> "In addition, it is also worth stating that, as a matter of law, there is no requirement in the doctrine of countermeasures for a response to be symmetrical to the underlying unlawful act. What matters is necessity and proportionality, which means that the UK could respond to a cyber intrusion through non-cyber means, and vice versa."

Again, the Tallinn Manual agrees with this approach, noting that

> "Proportionality does not imply reciprocity; there is no requirement that an injured State's countermeasure breach the same obligation violated by the responsible State. Nor is there any requirement that countermeasures be of the same nature as the underlying internationally wrongful act that justifies them. Non-cyber countermeasures may be used in response to an internationally wrongful act involving cyber operations, and vice-versa."

While this particular part of the attorney general's speech is not necessarily an innovation on the use of countermeasures, it solidifies the generally accepted view among commentators that has been assumed to be the approach of states, but not necessarily openly confirmed.

This departure from at least one traditional limitation on the use of countermeasures in the cyber context may signal that states are willing to revisit other aspects of cyber countermeasures. For example, countermeasures do not allow collective action on behalf of a victim state, even if that victim state is technologically incapable of responding on its own. Further, in an age where much of the malicious cyber activity originates from non-state actors, countermeasures may only be used against states. Additionally, there is no ability to use countermeasures in anticipation of an illegal act, only in response to one. These three examples are meaningful when reflecting on countermeasures because states have made exceptions to the traditional rule of self-defense to allow its exercise in precisely these three instances. And cyber countermeasures seem ideally suited for these three exceptions as they could most likely be effected without the cautioning concern of inevitable escalation.

The fact that the UK is looking at the law applicable to countermeasures in a way that allows for potential evolution from traditional norms, or at least a clarified understanding, is a valuable and informative statement. Further clarification by the UK, and by other states, is still necessary and will hopefully be forthcoming.

Conclusion

There is no doubt that this statement by the UK attorney general is one of the most important and clear official statements on the application of international law to cyber operations by a state. The particular points dealing with the use of force, prohibited intervention, sovereignty, and countermeasures are all vitally important because by letting the international community clearly know where the UK stands, it encourages other to likewise step forward. Wright said as much in his remarks.

> [A]s authors and subjects of international law, states have a responsibility here. A responsibility to be clear about how our international law obligations bind us. A responsibility we fulfil through our treaty obligations, our actions and our practice, as well as through our public statements. And a responsibility I believe extends to cyberspace.
>
> The very pervasiveness of cyber makes silence from states on the boundaries of acceptable behaviour in cyberspace unsustainable. If we stay silent, if we accept that the challenges posed by cyber technology are too great for the existing framework of international law to bear, that cyberspace will always be a grey area, a place of blurred boundaries, then we should expect cyberspace to continue to become a more dangerous place.

While a current reading of the statement may be profitable to outline specific views on well-recognized and accepted doctrines of international law and state interaction, the more important achievement of this statement will certainly be if it spurs other states to take up Wright's call to speak up and not "stay silent." If states want to ensure that the international law governing cyber space develops in an acceptable and sustainable way, they should follow Wright's lead and be clear about their "international law obligations" in cyberspace.

The views expressed are those of the authors and do not necessarily reflect the views of the United States Cyber Command, the Department of Defense, or the U.S. Government.

About the Author(s)

Gary Corn

Director of the Technology, Law & Security Program and Adjunct Professor of Cyber and National Security Law at American University Washington College of Law; retired U.S. Army Colonel; served as the Staff Judge Advocate to US Cyber Command and as a Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff

Eric Jensen

Professor at Brigham Young Law School, Special Counsel to the General Counsel of the Department of Defense, Former Chief of the Army's International Law Branch, and Former Legal Advisor to US Military Forces in Iraq and Bosnia

LAWFARE

INTERNATIONAL LAW

Syria Strikes: Legitimacy and Lawfulness

By **Laurie Blank** Monday, April 16, 2018, 3:06 PM

"Justified, legitimate and proportionate." These are the words that U.N. Ambassador Nikki Haley at an emergency United Nations Security Council session and the director of the Joint Staff, Lt. Gen. Kenneth McKenzie, in a Pentagon briefing used to describe the U.S. and allied strikes on Syrian chemical weapons facilities last Friday evening. Note, however, the absence of the word "lawful" or "legal." Indeed, the word "legitimate" is used in the context of one common definition: "able to be defended with logic or justification."

In contrast, law figured prominently in a separate briefing on the conduct of the strikes, the specific targets, the precautions taken to avoid civilian casualties—indeed, Chairman of the Joint Chiefs of Staff Gen. Joseph Dunford's detailed recitation offered a veritable catalogue of law of war obligations with which the United States has complied.

Both the resort to force—the "why"—and the conduct of hostilities—the "how"—must be lawful under international law. Nonetheless, here it appears that *why* the United States used force is a question of legitimacy, while *how* the United States uses force is a question of lawfulness. The difference between the two is important—not only for what it reveals about the authority to launch the strikes, but as a new step in the long-standing and often inseparable dance between legitimacy and lawfulness in the context of military operations.

To anyone who saw the photos of the aftermath of the attacks, with at least 70 killed and countless children gasping for air, destroying Syria's chemical weapons capability and punishing the regime for its continued use of chemical weapons against its own population in flagrant violation of international law surely seems like a textbook example of "justified" or "legitimate." After all, as both Defense Secretary James Mattis and Pentagon spokesperson Dana White reiterated countless times, no civilized nation can or should tolerate the use of chemical weapons.

This legitimacy, however, does not derive from international law. Although international law flatly prohibits the use of chemical weapons—in wartime or peacetime—international law also prohibits the use of force by one state against another. This ban is the central foundation of our international system. The only exceptions are self-defense, a U.N. Security Council authorization, or the consent of the territorial state concerned. (Although a few states, including the United Kingdom, recognize a narrow exception for humanitarian intervention, the United States does not, and there is no international consensus that such an exception is accepted international law.) Notwithstanding the moral imperative that chemical attacks might generate, retaliation or punishment for the use of chemical weapons, or deterrence against the future use of such weapons, are not lawful reasons to use force.

In fact, there is no international legal authority for the strikes, as the deafening silence from the Trump administration regarding an international law justification for its actions attests. The administration has rightly condemned Syria's violations of international law, but it has instead turned to the language of justness and moral outrage to justify its use of force, pitting the allied forces' "righteous power" and "noble warriors" against Syria's "barbarism and brutality."

The United States is thus using legitimacy in a four-step effort to create lawfulness. Step one: Catalogue and denounce Syria's extensive violations of international law, which by now are too numerous to count. Step two: Affirm the need for accountability for violations of international law, surely critical for any effective enforcement of international law and deterrence for future violations. Step three: Harness the universal moral outrage at the horror of last week's chemical weapons attacks and seven years of unending brutality against civilians and the desire to "make Assad pay" for what he has done. Step four: Add moral legitimacy to international law violations and the need for accountability, and the result is an appearance of lawfulness.

This rhetorical tactic has proved quite effective, as evidenced by the glaring absence of questions or reporting on whether the U.S. and its allies complied with international law in the resort to force against Syria. However, beyond this messaging success, there is now a new step in the *pas de deux* between legitimacy and lawfulness that is as old as war itself.

Legitimacy has always been an essential component of military operations, particularly with regard to public support for both the launch and continuation of such operations. Although the lawful *resort* to force was once the primary key to legitimacy, in recent years, compliance with the law of armed conflict—namely the principles of distinction, proportionality and precautions—in the *conduct* of military operations has become the central pillar of legitimacy.

Even a cursory glance at the discourse on military operations demonstrates this link between compliance with the law of armed conflict and legitimacy. In today's world of nearly instantaneous media and social-media coverage of military operations even in the farthest reaches of the globe, civilian casualties and the mere perception of war crimes can drastically undermine legitimacy both at home and abroad. In many

military operations, such as counterinsurgencies, protection of the civilian population is central to mission success, and therefore compliance with legal rules designed to protect civilians is essential for legitimacy. Similarly, a military that is or appears to be committing war crimes may lose legitimacy at home, eroding valuable public support necessary to sustain military operations. Finally, compliance with the law of armed conflict is the centerpiece of legitimacy in the international community, such that violations can undermine cohesion and diplomatic efforts among the coalition. For these reasons and many more, the United States and its allies go to great lengths to demonstrate their adherence to the fundamental principles and rules of the law of armed conflict.

Lawfulness has thus been the touchstone for legitimacy, whether in the form of compliance with the international law governing the resort to force, historically, or compliance with the law of armed conflict, in today's operations. But legitimacy is now being used as the measure of lawfulness in the absence of actual compliance with the law. Obfuscating the lack of international legal authority for Friday's strikes is, of course, the immediate consequence. After all, the combination of Syria's atrocities and U.S. moral justifications seems to have done the trick—moral legitimacy may not merely be substituting for lawfulness here (such as the "illegal but legitimate" description of the 1999 NATO bombing of the former Yugoslavia), but actually appears to be creating lawfulness.

But a far more damaging consequence may well be a steady erosion of law and legality in favor of legitimacy alone. Legitimacy is essential, but it must rest on law—not righteousness, political imperatives, religion, shared cultural ties, or the exigencies of a given moment. No less than the stability and predictability of our international system—and the ultimate legitimacy of U.S. actions—is at stake.

Topics: International Law, Jus ad Bellum/UN Charter/Sovereignty

---

Laurie R. Blank is a clinical professor of law and director of the International Humanitarian Law Clinic at Emory University School of Law, where she teaches international humanitarian law and works directly with students to provide assistance to international tribunals, non-governmental organizations, and law firms around the world on cutting-edge issues in humanitarian law and human rights.

doi:10.1017/aju.2019.15

SYMPOSIUM ON THE NEW SPACE RACE

INTERNATIONAL LAW AND SECURITY IN OUTER SPACE: NOW AND TOMORROW

Matthew T. King, and Laurie R. Blank***

Once the domain of a few spacefaring nations, outer space has exploded with new actors, state and private, in recent years. New actors and activities bring new potential threats and concerns for new and existing actors alike. In this complex environment, where mistrust and misunderstanding often prevail, international law can play an important role in bridging gaps and creating predictability, clarity, and consistency. Although new treaty law is unlikely, the ordinary incremental international law processes of state practice, *opinio juris*, and international jurisprudence will help to resolve critical questions about the content and application of international law in outer space over time.

The Military Space Environment: Main Players

Space has become bustling, with over seventy states, commercial entities, and international organizations operating in some fashion.[1] The U.S. Department of Defense (DoD) previously described the space environment as "congested, contested, and competitive," highlighting the challenges of expanding players and increasing numbers of objects vying for finite locations and operationally advantageous orbits and capabilities in outer space.[2] Although DoD excised this articulation from its 2016 *Space Policy*,[3] the actors continue to grow and a recent assessment continued the "Competing in Space" theme.[4] This congestion and competition is especially heightened in national security space operations, which include military, intelligence, national technical means, and command and control assets.

Although the overall number of military space players remains small, both the number and capabilities (particularly in command and control, computers, communications, intelligence, surveillance, and reconnaissance (C4ISR) platforms) have expanded in the new space race. The United States, Russia, and China—two Cold

* *Lieutenant Colonel, U.S. Air Force; Staff Judge Advocate, 30th Space Wing, Vandenberg AFB, California. The views expressed herein represent the personal views and conclusions of the author writing in his personal capacity and are not necessarily the views, ideas, or attitudes of the U.S. Air Force, Department of Defense, or U.S. Government.*

** *Clinical Professor of Law; Director, Center for International and Comparative Law; Director, International Humanitarian Law Clinic, Emory University School of Law.*

[1] Secure World Foundation, Handbook for New Actors in Space (Sept. 25, 2017); Saadia M. Pekkanen, *Introduction to the Symposium on the New Space Race*, 113 AJIL Unbound 92 (2019).

[2] Robert Gates & James Clapper, National Security Space Strategy (Unclassified Summary) 1 (Jan. 2011); U.S. Dep't of Defense, Dir. 3100.10, Space Policy para. 1 (Oct. 18, 2012 incorporating Change 1, effective Nov. 4, 2016) [hereinafter DoD Dir. 3100.10].

[3] DoD Dir. 3100.10, *supra* note 2.

[4] U.S. Dept. of Defense, Providing for the Common Defense 13 (Sept. 2018).

War powers from the dawn of the space age and a recently recognized peer player—remain the primary actors. Emerging participants include NATO members, Japan, New Zealand, and Australia working independently and with the United States,[5] and others less openly aligned with major space players, such as India, Iran, and Israel. At present, counterspace capabilities—such as antisatellite missiles (ASATs), rendezvous and proximity operation platforms (RPOs), space or terrestrially-based lasers, and other technology[6]—offer a key distinction between the primary actors and these emerging military space powers, which have only limited capability.

U.S. space doctrine calls for both offensive and defensive, kinetic and nonkinetic[7] space capabilities with the understanding that "peaceful purposes" in the Outer Space Treaty (OST) means nonaggressive uses of space—not nonmilitary uses.[8] This long-held position allows for intelligence, communications, and all other activities that do not breach Article 2(4) of the United Nations Charter prohibiting "the threat or use of force" in international affairs.[9] Although U.S. doctrine ensures maintenance of viable self-defense options in space[10] and the U.S. considers space a military domain,[11] DoD guidance emphasizes protection, deterrence, resiliency, redundancy, and international partnership as avenues for continued freedom of operations in space.[12]

Detailed Chinese and Russian doctrine, policy, and regulation are less accessible. However, both recognize space as a domain of potential conflict and an environment for the assertion of self-defense. China's space policy omits discussion of military uses, highlighting "peaceful purposes," noting its opposition to weaponization of space, and endorsing international cooperation and engagement.[13] However, Chinese military doctrine[14] and external assessments thereof recognize preparations for military competition in space, namely the 2015 reorganization of the People's Liberation Army to enhance space-based C4ISR, without limiting any counterspace options[15]—a capacity China maintains and has already displayed.[16] Russia's doctrine similarly notes space militarization as an "external hazard" and recognizes potential conflict in space, while stressing the importance and legitimacy

[5] Clayton Wear, *Liaison Officers at Vandenberg*, Vandenberg air force base (Nov. 8, 2018) (explaining that the Combined Space Operations Center (CSpOC) hosts officers from Australia, Canada, France, Germany, and the United Kingdom); Steven Hirsch, *Making the Most of Military Space*, Air Force Mag. (Aug. 2018) (reporting that the United States added Japan and New Zealand to the Schriever Wargames).

[6] *See* Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment (Brian Weeden & Victoria Sampson eds., 2018); Center for Strategic & International Studies, Space Threat Assessment 2018 (Todd Harrison et al. eds., 2018) [hereinafter Space Threat Assessment 2018].

[7] Space Threat Assessment 2018, *supra note* 6, at 3.

[8] *See* U.S. Dep't. of Defense, Law of War Manual para. 14.10.4 (updated Dec. 2016) [hereinafter DoD LoW Manual]; s*ee also* Central Intelligence Agency, Position Paper: Definition of Peaceful Uses of Outer Space (Contingency) [declassified] (Nov. 7, 2000); Central Intelligence Agency, Attachment 2: Definition of Peaceful Uses of Outer Space [declassified] (Mar. 13, 1962).

[9] UN Charter art. 2(4).

[10] DoD Dir. 3100.10, *supra* note 2, at para. 4.b; Pres. Donald Trump, National Security Strategy of the United States of America 31 (Dec. 2017) [hereinafter NSS].

[11] Joint Chiefs of Staff, Joint Publication 3–14, Space Operations para. I.2.a (vice II.16.d) (Apr. 10, 2018) [hereinafter JP 3–14].

[12] *See, e.g.*, *id.* at para II.16.d (vice 2.a); DoD Dir. 3100.10, *supra* note 2, at para. 4.c.

[13] Information Office of the State Council, Full Text of White Paper on China's Space Activities in 2016, at I.3, IV.5, V.1 (Dec. 28, 2016).

[14] Information Office of the State Council, China's Military Strategy (May 27, 2015).

[15] Kevin Pollpeter et al., The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations (RAND, 2017).

[16] *See, e.g.*, Brian Weeden, *Through a Glass, Darkly: Chinese, American, and Russian Anti-Satellite Testing in Space*, Space Rev. (Mar. 17, 2014); Steven Lee Myers & Zoe Mou, *'New Chapter' in Space Exploration as China Reaches Far Side of the Moon*, N.Y. Times (Jan. 2, 2019).

of self-defense assertions.[17] Russia has an active Space Force[18] and is developing counterspace capabilities, including RPOs and antisatellite lasers.[19]

All three major players thus recognize space as a military domain of operations, and appear to act accordingly. They generally focus on developing new terrestrially-focused space applications and security of extant space assets (through deterrence or active defense) rather than offensive space operations. This focus is reasonable given the likelihood of kinetic activities only serving to diminish each state's own use of space for terrestrially useful applications through the creation of orbital debris or adverse political or military reactions.

Space may be an infinite expanse, but its useful zones or orbits for space and terrestrial applications are limited. As the number of sovereign and "newspace" actors seeking finite advantageous orbital locations, the range of military capabilities, and the number of states developing counterspace capacities all grow, so will tensions related to space activities. With new technologies now bringing old security concerns to the fore, the space race is at a new inflection point: geostationary orbit-reaching ASATs, RPOs, lasers, and hypersonic weapons may now be an imminent and distributed reality. Although kinetic-only options have an implicit practical limitation if the launching state also intends to use space (due to debris), emerging nonkinetic and nonattributable technology may allow for hostile activities without collateral harm to one's own assets, and without a guarantee of any response or reprisal. As the military space environment leans towards one of realistic threat of action—not just major-state planning for a distant, potential technological future—the national security space community is coming to a crossroads. One way to address competition in this congested, contested environment may be through shared understandings of the law governing state behavior in space.

Room for International Law in Military Space Operations?

Any discussion of international law and military space operations starts with two fundamental questions: does international law apply and, if so, how? It is well settled that international law applies in outer space, both as the law governing the interaction of states, and under the specialized regime of outer space law set forth in Article III of the OST. Whether and how the law of armed conflict (LOAC) applies to military space activities appears less established, however. U.S. views appear clear, but the views of other military space actors are less so given the paucity of open source materials or statements on topic.

The U.S. applies LOAC to all military operations in outer space—space is a warfighting domain, where military members conduct military operations. In accordance with DoD Directive 2311.01E, "[m]embers of the DoD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations."[20] The DoD Law of War Manual explains:

> [LOAC] regulate[s] the conduct of hostilities, regardless of where they are conducted, … includ[ing] the conduct of hostilities in outer space. In this way, the application of [LOAC] to activities in outer space is the same as its application to activities in other environments, such as the land, sea, air, or cyber domains.[21]

[17] Military Doctrine of the Russian Federation I.8.d & I.6.g (Feb. 5, 2010).

[18] Russian Ministry of Defence, Aerospace Defence Forces.

[19] Maddy Longwell, *State Department Concerned over Russian Satellite's Behavior*, C4ISRNet (Aug. 14, 2018); Patrick Tucker, *Russia Claims It Now Has Lasers To Shoot Satellites*, DefenseOne (Feb. 26, 2018).

[20] U.S. Dep't of Defense, Dir. 2311.01E, DoD Law of War Program para. 4.1 (Feb. 22, 2011).

[21] DoD LoW Manual, *supra* note 8, at para. 14.10.2.2.

U.S. partners—NATO states, Australia, and Japan—do not necessarily have similarly clear articulations, but share this general disposition towards the application of international law (and particularly LOAC) and can be expected to extend it to military activities in outer space.[22]

For the United States, adherence to the law is strategically advantageous and contributes positively to legitimacy and operational success.[23] DoD's National Defense Strategy focuses on near-peer competition, enhancing lethality for credible deterrence of (or reactions to) threats, and competition along the full spectrum of military operations (above and below the threshold of armed attack).[24] One of three pillars is to strengthen alliances and international cooperation, including by "maintaining the rules which underwrite a free and open international order" and deepening interoperability with allies.[25]

Less information regarding China and Russia's views on international law and military space operations is openly available. Their doctrine documents and seeks efforts to advance the draft Treaty on the Prevention of Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (PPWT); a No First Placement of Weapons resolution; and a Code of Conduct in Space suggest at least some reliance on international law. Questions remain, however, concerning whether these states will actually adhere to the law even if a treaty comes into force, a concern animating U.S. views on space cooperation.[26] Thus, U.S. diplomats openly lament the lack of verification and trust and confidence building measures in the PPWT draft and other arms and Code discussions.[27]

The next question is *how* international law applies. U.S. policy is to compete in the full spectrum of military operations, including when adversaries use "areas of competition short of open warfare to achieve their ends."[28] The *jus ad bellum*, LOAC, law of state responsibility, and law of friendly relations are therefore all implicated. However, the technology, geophysics, and geopolitics of outer space make tackling the contours and the sometimes domain-specific intricacies of general principles and customary international law a challenge. State practice will therefore be a, if not the, significant determining factor.

Applying International Law in Space: Key Issues and Challenges

As in other arenas of international engagement, international law is the primary mechanism for creating, implementing, and enforcing shared understandings of the rights, privileges, and duties of states, nonstate entities, and individuals in space. State actors seek to maintain freedom of action and protect their sovereign national interests.

[22] *See* German Ministry of Defence, Law of Armed Conflict Manual (Joint Service Regulation (ZDv)) 15/2 paras. 201 & 212 (May 2013); United Kingdom Ministry of Defence, The UK Military Space Primer ch. 2 (2010).

[23] NSS, *supra* note 10, at 4, 41.

[24] U.S. Dep't of Defense, National Defense Strategy (Unclassified Summary) (Jan. 2018) [hereinafter NDS].

[25] *Id.* at 8–9; *see also* JP 3–14, *supra* note 11, at para. IV.3.d; DoD Dir. 3100.10, *supra* note 2, at para. 4.f.

[26] U.S.-China Econ. & Sec. Rev. Comm'n, China's Position on a Code of Conduct in Space 5 (Sept. 8, 2017) ("China has frequently broken its agreements, [including its] … promise not to further militarize land features in the … South China Sea, … agreements with India, and its bilateral cyber security agreement with the United States."); Yleem Poblete, Assistant Secretary, Bureau of Arms Control, Verification and Compliance, United Nations, Remarks at the 73rd UNGA First Committee Thematic Discussion on Outer Space (Oct. 23, 2018) ("They are fundamentally flawed proposals advanced by a country [Russia] that has routinely violated its international obligations.").

[27] *See* Poblete, *supra note* 26 (calling NFP a "Potemkin resolution"); Ambassador Robert Wood, U.S. Permanent Representative to the Conference on Disarmament, Explanation of Vote in the First Committee on Resolution L.54: Further Practical Measures for the Prevention of an Arms Race in Outer Space (Oct. 20, 2017).

[28] NDS, *supra* note 24, at 3, 5 (adversaries use "corruption, predatory economic practices, propaganda, political subversion, proxies, and the threat or use of military force to change the facts on the ground").

Doing so often requires cooperative efforts and states are therefore willing to create mechanisms for greater understanding and foreseeable and predictable responses to challenges. The existing foundations of outer space law—the five primary international law treaties on outer space—are the fruits of earlier efforts to provide a critical foundation for this complex environment. Treaty law is the strongest, most enforceable, and most likely to define and regulate state behavior, and therefore to provide concrete guidance and parameters for states to assess threats, including the use of force in, through, or from outer space, and appropriate forcible and nonforcible responses. The likelihood of new treaties being developed and coming into force is slim, however, given the steadily growing cast of characters with an equally expansive set of competing interests in outer space. As a result, customary international law is the most likely tool for development of rules, as states develop patterns of practice and a willingness to accept such practice as binding legal obligation.

Among the most likely legal issues to arise and engender dispute in military space operations are the principle of nonintervention, the threshold for use of force and armed attack, the meaning and application of proportionality, and the status of military-oriented "newspace" objects. Although each has been examined, applied, and interpreted extensively in terrestrial domains, their application in outer space adds an additional layer of complexity.

With respect to the threshold for the use of force, interesting questions arise as to whether nonkinetic acts can meet the threshold for the use of force and whether the temporary or permanent loss of functionality of a space object can suffice to meet that threshold. In the context of armed attack, additional questions include whether, and which, space objects and activities constitute critical national infrastructure such that any attack on such objects or activities will be an armed attack. State practice, and the response of states to hostile or potentially hostile acts in, through, or from outer space, will begin to highlight the contours of these fundamental principles and thresholds, and will be essential in elucidating the content of international law in this domain.

Proportionality introduces further complexities, given the difficulty of understanding and predicting the consequences of attacks on space objects and the potential for objects that are destroyed to contribute to space debris in a consequential manner or to fall to Earth and cause harm on land. The LOAC principle of proportionality prohibits an attack if the expected harm to civilians will be excessive in relation to the anticipated military advantage gained. Although the military advantage of attacks in, through, or from outer space likely rests on the same or analogous information and assessments as in other domains, understanding the nature and foreseeability of civilian harm, including harm to the environment, is extraordinarily difficult.

As military and political practitioners in spacefaring states assess and develop legal positions on these matters, academics and other nongovernmental entities are seeking to help shape the understanding of the legal landscape. In particular, two projects—the Woomera Manual on the International Law of Military Space Operations[29] and the Manual on International Law Applicable to Military Uses of Outer Space[30]—seek to inform the analysis of existing international law related to military operations in outer space. Both projects have a stated goal to objectively articulate the law, including discussion of the contours and application of the relevant treaties and customary international law. Law provides a key framework from which state actors evaluate concerns, threats, or provocations in space operations—military practitioners must know the behavioral baseline, established in law or practice, before they can judge any deviations therefrom. Although the manuals will not be binding law, they can help state practitioners work through new challenges of the extant law, namely LOAC in the space domain. In particular, these manuals evince the recognition that prospective consideration of the law and legal challenges in outer space, as in any domain, is essential for efficient and effective application of the law when incidents arise.

[29] The Woomera Manual (last updated Jan. 11, 2019). Both authors are core experts.

[30] McGill Centre for Research in Air & Space Law, Manual on International Law Applicable to Military Uses of Outer Space.

NEW TECHNOLOGIES AND THE INTERPLAY BETWEEN CERTAINTY AND REASONABLENESS

Laurie R. Blank[*]

in COMPLEX BATTLESPACES: THE LAW OF ARMED CONFLICT AND THE DYNAMICS OF MODERN WARFARE xx (Christopher M. Ford & Winston Williams eds., Oxford University Press forthcoming 2018)

1. INTRODUCTION

Cyber. Unmanned aerial vehicles. Autonomous weapons systems. Nanotechnologies. New technologies have sparked extensive discourse on the application of the law of armed conflict (LOAC) to such technologies. Governments, advocacy organizations, and scholars strive to keep pace with technological developments amid debates regarding the applicable law, the need for new international legal regimes, and campaigns to ban certain technologies.

Underlying these intensive efforts to understand how LOAC does, could and should apply to the use of new technologies is an equally comprehensive effort to understand precisely what these new weapons are and how they work. Each of the new technologies above introduces unique questions for human understanding, often driven and exacerbated by the fact that the technology is out of sight or out of reach of human senses, making actual concrete understanding of how it works challenging and elusive. Effective legal analysis and guidance for the use of any weapon rests on an accurate understanding of how that weapon works. For example, the debates regarding autonomous weapons systems often appear to stagnate in a morass of questions about the meaning of autonomy, autonomous and other essential descriptive and defining characteristics of these systems.[1] Without agreement on the meaning of basic terms and descriptions, it is difficult, if not impossible, to proceed to the thorny legal questions at the heart of these debates.

This uncertainty and quest for more determinative information about the nature of certain new technologies has consequences beyond the overt ones of complicating discussions or stalling debates, however. The desire for certainty has the potential for unintended and possibly untoward effects on the very implementation and application of the law itself—in effect, it has the potential to change the law. As in many other legal regimes, critical components of legal analysis and interpretation in LOAC involve reasonableness: that is, whether the actions of a commander were reasonable in the circumstances prevailing at the time. In contrast, the need to understand how a

---

[*] Clinical Professor of Law and Director, International Humanitarian Law Clinic, Emory University School of Law.
I am grateful to Zachary Needell (J.D. expected, 2018), Christina Zeidan (J.D. expected, 2018) and Kyle Hunter (J.D. expected, 2018) for their outstanding research assistance.

[1] *See e.g.* Chris Jenks, *False Rubicons, Moral Panic, & Conceptual Cul-De-Sacs: Critiquing and Reframing the Call to Ban Lethal Autonomous Weapons*, 44 PEPPERDINE L. REV. 1, 9 (2016).

new technology works and what it might do in a given situation, particularly with regard to autonomy, is not an inquiry resting on reasonableness, but rather on the desire for as much certainty as possible.

This chapter examines how the development and use of new technologies in weapons may impact the balance between reasonableness and certainty in LOAC. Difficult questions about quantifying reasonableness and certainty for purposes of assigning criminal responsibility for actions taken during military operations have already emerged as international criminal justice has brought military operations into the courtroom. At the same time, the development of hi-tech weapons introduces enormous challenges for understanding how such weapons work and how to assign responsibility when things go wrong. Demands for greater certainty are likely to increase, in turn, to help humans understand how to judge these weapons and the decisions involved in their programming and deployment. As certainty becomes an overarching need and consideration, an important question is whether that quest for certainty will bleed over into the application and interpretation of the law and, over time, affect the development and understanding of the law itself.

The first section provides the foundation for this analysis, introducing the already evolving tensions between reasonableness and certainty in the application of LOAC. It first briefly sets forth the role of reasonableness in determining the lawfulness of targeting and related decisions during armed conflict, and then considers efforts to understand what reasonableness means and how to measure or assess it in some productive manner. Finally, this section highlights how questions regarding certainty have already begun to emerge in the context of international criminal accountability, regarding both certainty in decision-making and certainty in the analysis of information or intent.

The second section explores how new technologies are driving more frequent and overt demands for certainty. Using lethal autonomous weapons systems as a primary example, this section analyzes three primary certainty issues: the certainty of technology, of knowing how it works and what it does; the certainty of legal norms at issue in debates about if and how the law applies; and the certainty of analysis and decision-making by the autonomous weapons. These efforts to know with certainty what a machine does and will do collide directly with the notion of reasonableness in legal analysis and application. In particular, such efforts raise questions about whether effective analysis of an autonomous weapon's targeting decisions should and will rest on whether the weapon system acted reasonably—a methodology resting on qualitative measures—or whether such system computed the facts and information correctly in acting upon that information—a methodology resting on certainty and quantitative measures.

The final section tackles the consequences of greater reliance on and search for certainty for the long-term development of LOAC. The role of certainty in the discourse on autonomous weapons, and potentially other new technologies, raises significant questions about whether a growing comfort level with measures of certainty will impact the traditional reliance on reasonableness in driving the implementation of and assessments of compliance with LOAC. In effect, if a gap between the operational standard of good faith determinations and a quantitative, certainty-based standard driven by technologies appears and continues to grow, such a mismatch

may undermine the law's effectiveness and the development of expertise and experience in implementing the law in military operations and in post-hoc analysis of such operations.

2. Reasonableness and Certainty in the Implementation of the Law of Armed Conflict

LOAC governs the conduct of both States and individuals during armed conflict and seeks to minimize suffering in war by protecting persons not participating in hostilities and by restricting the means and methods of warfare.[2] LOAC applies during all situations of armed conflict, whether between two or more States, between a State and a non-State group, or between two or more non-State groups.[3] Although LOAC governs all aspects of armed conflict, the issues raised by reasonableness and certainty arise predominantly in the context of the use of force, the focus therefore of the discussion in this chapter.

In particular, this chapter primarily addresses lethal autonomous weapon systems (LAWS). A weapons system that is or could be designed to reach its own judgments regarding the lawfulness of a particular target and of attacks on that target at a particular time goes to the essence of the complicated relationship between reasonableness and certainty and the likely consequences of this interplay over time. Like any weapon, LAWS must be used in accordance with the fundamental principles of targeting: distinction, proportionality and precautions. Debates over the legality of LAWS generally center on the anticipated or perceived ability or inability to comply, or obstacles to compliance, with these fundamental obligations and protections. More important, the actual use of such weapons and any post-hoc assessment of an attack using LAWS will be based on the rules and obligations these principles mandate.

As the following discussion highlights, reasonableness is the touchstone for the implementation of these central targeting obligations. At the same time, several factors, including the needs of international criminal accountability and the role of the advocacy community, have begun to inject certainty questions into this traditional reasonableness realm. This trend, already apparent over the past decade, offers a window into the potential consequences and important considerations as LAWS and other new technologies bring quantitative questions and a question for certainty into a more central role in the analysis and application of LOAC.

---

[2] LOAC is codified primarily in the four Geneva Conventions of August 14, 1949 and their Additional Protocols. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 21, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea art. 34, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Convention Relative to the Protection of Civilian Persons in Time of War art. 19, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II].

[3] With regards to international armed conflicts, see e.g., Geneva Convention I, *supra* note 2, art. 2. With regards to non-international armed conflicts, see e.g., Common Article 3, Geneva Convention I, *supra* note 2, art. 3.

A. The Law of Targeting and the Touchstone of Reasonableness

The lawfulness of targeting individuals and objects during armed conflict is determined by the principles of distinction,[4] proportionality,[5] and precautions in attack.[6] The principle of distinction, one of the "cardinal principles" of LOAC,[7] requires that any party to a conflict distinguish between military and civilian personnel and objects and direct attacks solely at persons who are fighting and military objectives. Proportionality requires that parties refrain from attacks in which the expected civilian casualties will be excessive in relation to the anticipated military advantage gained.[8] Finally, LOAC mandates that parties to a conflict take all feasible precautions in launching attacks that may affect the civilian population. All three principles are widely recognized as customary international law.[9]

Across these three essential principles of targeting, reasonableness remains the touchstone for determining the appropriate application of specific targeting rules and for assessing the lawfulness of action after the fact. Each principle requires commanders and individual soldiers to make decisions in good faith based on the information available to them at the time of the attack. Underlying the treaty law, commentary and jurisprudence is the idea that "decisions are based on reasonable expectations rather than results. In other words, honest mistakes often occur on the battlefield due to the 'fog of war' or when it turns out that reality does not match expectations."[10] This approach dates back to the post-World War II trials, when the Nuremberg Tribunal acquitted General Lothar Rendulic of the crime of wanton destruction of property. Notwithstanding the extraordinary destruction Norway suffered at General Rendulic's hands as he embarked on his "scorched-earth" retreat in the face of the approaching Russian army, the tribunal found that his actions were not criminal because they were based on his judgment in the circumstances. In a clear statement of this fundamental rule of reasonableness for both decision-making and post-hoc assessment of such decisions, the tribunal declared:

> [w]e are not called upon to determine whether urgent military necessity for the devastation and destruction . . . actually existed. We are concerned with the question

---

[4] Additional Protocol I, *supra* note 2, art. 48.
[5] *Id*., art. 51(5)(b), 57(2)(a)(iii) and 57(2)(b).
[6] *Id*., art. 57(1).
[7] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8) (declaring that distinction and the prohibition on unnecessary suffering are the two cardinal principles of LOAC).
[8] Additional Protocol I, *supra* note 2, art. 51(5)(b).
[9] JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 3-8 (2005); Legality of the Threat or Use of Nuclear Weapons, *supra* note 4, at 587 (dissenting opinion of Judge Higgins) (distinction as customary law); YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 120 (2004); 1 HENCKAERTS & DOSWALD-BECK, *supra* note 5, at 46; Michael N. Schmitt, *Fault Lines in the Law of Attack*, *in* TESTING THE BOUNDARIES OF INTERNATIONAL HUMANITARIAN LAW 277, 292 (Susan Breau & Agnieszka Jachec-Neale eds., 2006) (proportionality as customary law); JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW Rule 15 (2005) (precautions as customary law).
[10] MICHAEL N. SCHMITT, CHARLES B. GARRAWAY, AND YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT, International Institute of Humanitarian Law (2006), p. 23.

> whether the defendant at the time of its occurrence acted within the limits of honest judgment on the basis of the conditions prevailing at the time. . . . It is our considered opinion that the conditions, as they appeared to the defendant at the time were sufficient upon which he could honestly conclude that urgent military necessity warranted the decision made. This being true, the defendant may have erred in the exercise of his judgment but he was guilty of no criminal act.[11]

Although this basic framework of reasonableness in the circumstances prevailing at the time is most often emphasized in the context of proportionality decisions, it applies across the full spectrum of targeting decisions and acts.

With regard to distinction, an attacker must determine whether the potential object of attack is a legitimate target: a combatant, a member of an organized group, a civilian directly participating in hostilities, or a military objective. For each of these possible lawful targets, the law rests on the attacker's honest efforts to distinguish them from persons or objects protected from attack. The very structure of the law and the criminal accountability paradigm reinforce this approach. For example, combatants are subject to attack except when *hors de combat*, and the determination of whether a person is *hors de combat* is based on the attacker's reasonable belief at the time regarding either a clear affirmative act of surrender or incapacitation due to wounds or sickness.[12] The *travaux préparatoires* demonstrate that the decision whether someone is in the power of an attacker and thus protected from attack as *hors de combat* is based on an objectively reasonable determination by the attacker.[13]

Similarly, distinction with regard to civilians is not a strict liability standard for which any mistake is a violation, but rests on the same reasonableness paradigm that permeates LOAC. International criminal accountability offers the most direct manifestation of this framework: the war crime of unlawful attacks on civilians is a crime of intent. Article 85 of Additional Protocol I declares that it is a grave breach to "wilfully . . . mak[e] the civilian population or individual civilians the object of attack," and includes both deliberate and reckless attacks within its scope.[14] As a result, a "willfully unlawful attack on civilians would thus be one that either deliberately

---

[11] USA v. Wilhelm List and Others (The Hostages Trial), Case No. 47, Judgment (U.S. Mil. Trib., Nuremberg, Feb. 19, 1948), *in* VIII LAW REPORTS ON THE TRIALS OF WAR CRIMINALS XX (1950).

[12] *See* Geoffrey S. Corn et al, *Belligerent Targeting and the Invalidity of a Least Harmful Means Rule*, 89 INT'L L. STUD. 536, 587 (2013).

[13] Federal Political Department, XV Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflict, Geneva (1974-1977), CDDH1236/Rev.1, at 383 ¶ 21 (1978). The Commentary to Additional Protocol I reaffirms the reasonableness framework, noting that "it would be useless to deny that in the heat of action and under the pressure of events, this rule is not always easy to follow." COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 480 (Claude Pilloud et al. eds., 1987) [hereinafter AP I COMMENTARY]. *See also* Corn et al., *supra* note 12, for a comprehensive discussion of the *hors de combat* determination, the presumptions underlying that determination, and the burden of rebutting those presumptions.

[14] Additional Protocol I, *supra* note 2, art. 85. The Commentary explains that willfulness includes recklessness, which is "the attitude of an agent who, without being certain of a particular result, accepts the possibility of it happening." AP I COMMENTARY, *supra* note 28, ¶ 3474.

sought to target civilians, or deliberately ignored the affirmative duty to take care by making no effort to distinguish."[15] However, in the absence of direct evidence that the attacker believed the victims to be civilians, international tribunals rely on a reasonableness framework to assess the attacker's intent. The International Criminal Tribunal for the former Yugoslavia (ICTY), for example, held in *Prosecutor v. Galić* that a prosecutor must prove that "in the given circumstances a reasonable person could not have believed that the individual he or she attacked was a combatant."[16] This reliance on reasonableness to assess intent affirms that, at the time of an attack, a commander or soldier must make a reasonable determination regarding whether an individual is a civilian. The law mandates that in case of doubt, an individual is presumed to be a civilian but the determination remains one of reasonableness based on the information available, not one of perfect decision-making.[17]

Proportionality is the targeting principle most commonly associated with reasonableness. A proportionality determination requires that a commander assess, at the time of the attack, the expected likely civilian casualties and the anticipated military advantage gained from the attack and then determine, based on good faith judgment, whether the expected civilian casualties will be excessive so as to preclude the attack.[18] Proportionality thus operates as an "international version of the common law's reasonable man, who has carefully considered all the evidence available at the critical time and shaped a rational choice between available means."[19] International jurisprudence,[20] military manuals,[21] statements upon ratification of Additional Protocol I[22] and national courts[23] all confirm the role of the "reasonable commander" in the implementation of proportionality and any post-hoc determinations regarding the validity of such decisions taken at the time. As the ICTY held in *Galić*, one of few international tribunal judgments to address proportionality, "[i]n determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack."[24]

---

[15] John J. Merriam, *Affirmative Target Identification: Operationalizing the Principle of Distinction for U.S. Warfighters*, 56 V.J.I.L. 84, 112 (2016).
[16] Prosecutor v. Galić, Case No. IT-98-29-T, Judgment ¶ 55 (Int'l Crim. Trib. for the former Yugoslavia Dec. 5, 2003). The tribunal took the same approach with regard to attacks on objects. *Id*. at ¶ 51.
[17] Additional Protocol I, *supra* note 2, art. 50(1). *See also* infra Part II(B).
[18] *See* Additional Protocol I, *supra* note 2, art. 51(5)(b), 57(2)(a)(iii) and 57(2)(b).
[19] Thomas Franck, *On Proportionality of Countermeasures in International Law*, 102 A.J.I.L. 715, 737 (2010).
[20] Prosecutor v. Galić, *supra* note 31, at ¶ 58.
[21] See e.g., OFFICE OF THE JUDGE ADVOCATE GENERAL, NATIONAL DEFENCE OF CANADA, THE LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS §5, ¶ 27 (1992) ("consideration must be paid to the honest judgement of responsible commanders, based on the information reasonably available to them at the relevant time.")
[22] HENKAERTS & DOSWALD-BECK, *supra* note 5 at 332 (citing Declaration and Reservations Made Upon Ratification of Additional Protocol I, Ireland § 9 (May 19, 1999)) ("military commanders and others responsible for planning, deciding upon, or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is reasonable available to them.").
[23] See e.g., Federal Court of Justice, Federal Prosecutor General, Decision at 47-49 (Apr. 10, 2010), http://www.icrc.org/customary-ihl/eng/docs/v2_cou_de_rule8_sectionf, ¶ 3(cc)(4) (an infringement of proportionality occurs when the commander "refrained from acting 'honestly', 'reasonably' and 'competently'.").
[24] Prosecutor v. Galić, *supra* note 31, at ¶ 58. *See also* REVIEW COMMITTEE, OFFICE OF THE PROSECUTOR, INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA, FINAL REPORT TO THE PROSECUTOR BY THE

Finally, the implementation of precautions rests on reasonableness and feasibility. As the treaty law, commentary and state practice[25] affirm, the obligation to take precautions, including which precautions and to what extent, is based on the commander's honest and reasonable judgment in the circumstances at the time of the attack. Article 57 of Additional Protocol I uses the language of feasibility in setting forth the obligations to take precautions, including to "do everything feasible" and to "take all feasible precautions".[26] Although neither the treaty nor the International Committee of the Red Cross (ICRC) Commentary specifically define "feasible," the Commentary explains that any assessment of the steps taken "will be a matter of common sense and good faith,"[27] a description akin to reasonableness. Across the spectrum of the law of targeting, therefore, reasonableness is the overarching framework, the fundamental measure for guiding commanders and soldiers in the implementation of and compliance with the law and for judging responsibility for potential violations of the law after the fact.

B. Attempts to Quantify Reasonableness and the Trend Towards Certainty

Increasing analysis of military operations after the fact by non-governmental organizations, national investigations, international commissions of inquiry, or national and international courts and tribunals, has begun to put significant stress on the reasonableness construct. Although the law is clear that "commanders are held to an objective standard of reasonable conduct assessed by considering the context in which the judgment was made,"[28] analyses of military operations and potential LOAC violations in varied contexts often veer away from this well-established framework.

The very dissonance between the courtroom and the battlefield underscores how the imperative of reasonableness in assessing targeting decisions has slowly morphed towards a reliance on effects and other post-hoc information in a quest for more certainty in the analysis of

---

COMMITTEE ESTABLISHED TO REVIEW THE NATO BOMBING CAMPAIGN AGAINST THE FEDERAL REPUBLIC OF YUGOSLAVIA ¶ 50 (2000) (explaining that "[i]t is unlikely that a human rights lawyer and an experienced combat commander would assign the same relative values to military advantage and to injury to noncombatants. Further it is unlikely that military commanders with different doctrinal backgrounds and differing degrees of combat experience or national military histories would always agree in close cases. It is suggested that the determination of relative values must be that of the 'reasonable military commander.'").

[25] DEPARTMENT OF THE ARMY, THE LAW OF LAND WARFARE FM 27-10, ¶ 41 (1956) (mandating that an attacker "must take all reasonable steps to ensure . . . that the objectives are identified as military"); DEP'T OF THE NAVY & DEP'T OF HOMELAND SECURITY, NWP 1-14 M/MCWP 5-12/CMODTPUB P5800.7A, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS (2007), ¶ 8.1 ("all reasonable precautions must be taken"); OFFICE OF THE JUDGE ADVOCATE GENERAL, NATIONAL DEFENCE OF CANADA, THE LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS §4, ¶ 418(3) (2001) (requiring commanders to take all feasible steps to verify that targets are legitimate military objectives and explaining that the test for assessing whether that "standard of care has been met is an objective one: Did the commander, planner or staff officer do what a reasonable person would have done in the circumstances?").

[26] The Commentary to Additional Protocol I notes that the ICRC's original draft text of Article 57 used the expression to "take all reasonable steps," which was later changed to "everything feasible." AP I COMMENTARY, *supra* note 28 at 681.

[27] *Id*., at 682.

[28] Geoffrey S. Corn, *Regulating Hostilities in Non-International Armed Conflicts: Thoughts on Bridging the Divide Between the* Tadić *Aspiration and Conflict Realities*, 91 INT'L L. STUD. 281, 313 (2015).

potential violations during military operations. Although existing treaty law and the associated ICRC Commentaries emphasize reasonableness as the standard, neither "indicates the quantum of information necessary to render 'reasonable' a judgment of target legality."[29] In a criminal prosecution for unlawful attacks on civilians or civilian objects, a tribunal needs tools or methodology for assessing the reasonableness—or unreasonableness—of the attack decision. An objectively reasonable decision that the object of attack is a lawful target will foreclose a finding that the attacker deliberately or indiscriminately attacked civilian objects, making the determination of objective reasonableness a key part of the analysis. In seeking to identify some quantifiable measures for determining reasonableness, however, it has become common for tribunals, commissions of inquiry or other mechanisms to substitute a subjective measure of reasonableness, thus subjecting "the commander under scrutiny to a post hoc judgment based not on the standard of reasonableness analogous to that used at the time of the decision, but on the subjective instincts of the reviewing official or entity."[30]

The so-called effects-based analysis of targeting decisions is the most obvious and problematic example. Given the challenges of measuring whether a commander's judgment was objectively reasonable, a reliance on the effects of the attack to tell the story has become common. Made infamous in the ICTY's trial judgment convicting General Ante Gotovina, an effects-based analysis uses the actual consequences of the attack to draw inferences and conclusions regarding the intent of the commander and the reasonableness of his decision. To assess the reasonableness—and thus lawfulness—of Gotovina's attack decisions, the ICTY concluded that evidence demonstrating that artillery shells landed more than 200 meters from identified military objectives proved that he acted unreasonably in launching such attacks—the foundation of its finding of unlawful attacks on civilians, a crime based on intent.[31]

In so doing, the judgment failed to consider or attribute relevant weight to the myriad of operational variables that impact the execution of combat operations and the use of force against both planned and fleeting targets. Variables such as the quality and quantity of intelligence about enemy and civilian locations, the quality of munitions, training, terrain, weather, quality of equipment, fatigue and many others are "integral to any targeting process at the time of the planning and the attack; they are all also relevant for a tribunal or court in assessing the reasonableness of the commander's decision-making process."[32] The failure to incorporate these operational considerations into an analysis of operational decision-making was glaring and undermined the effective implementation and application of LOAC.[33]

---

[29] Geoffrey S. Corn, *Targeting, Command Judgment, and a Proposed Quantum of Information Component: A Fourth Amendment Lesson in Contextual Reasonableness*, 77 BROOKLYN L. REV. 1, 15 (2012).
[30] *Id*. at 19.
[31] Prosecutor v. Gotovina, Case No. IT-06-90, Judgement, Vol. II of II, ¶ 2620 (Int'l Crim. Trib. for the former Yugoslavia April 15, 2011).
[32] OPERATIONAL LAW EXPERTS ROUNDTABLE ON THE *GOTOVINA* JUDGMENT: MILITARY OPERATIONS, BATTLEFIELD REALITY AND THE JUDGMENT'S IMPACT ON EFFECTIVE IMPLEMENTATION AND ENFORCEMENT OF INTERNATIONAL HUMANITARIAN LAW 13 (2011), https://inavukic.files.wordpress.com/2012/01/gotovina_meeting_report.pdf.
[33] *See e.g. id*.; Geoffrey S. Corn & Lt. Col. Gary P. Corn, *The Law of Operational Targeting: Viewing the LOAC Through an Operational Lens*, 47 TEX. INT'L L. J. 337 (2012).

Although the judgment was ultimately overturned on appeal, this type of effects-based analysis has begun to permeate the discourse on LOAC over the past several years. The most common manifestation appears in the consideration of attacks leading to civilian casualties, in which the frequent reaction in the media, commission of inquiry reports and other discourse is that the existence of civilian casualties must mean that the attack was an unlawful attack on civilians. As noted above, however, LOAC in general, and proportionality specifically, simply does not operate on the basis of after-the-fact determinations.

Rather than engage in the complex and multi-faceted analysis required to assess whether the commander's decision was reasonable at the time of the attack, such reports and analyses simply count up the casualties and damage and pronounce that the attack was disproportionate or perhaps even intentional. While this approach represents a fundamental misunderstanding of LOAC, it also likely stems from a desire to find tools to bring greater certainty to the analysis — although it may be difficult or complicated to assess whether a commander's decision was objectively reasonable given the circumstances and information available at the time of the attack, it is quite simple to reach a conclusion on the basis of casualties and destroyed or damaged buildings alone.

As discussed in greater detail in Part III, an effects-based analysis poses substantial risks for the effective implementation and long-term development of, and respect for, LOAC. First, an effects-based approach disregards the notion of targeting as a methodology that guides law-compliant militaries in implementing LOAC in military operations. Second, because an effects-based approach is divorced from the operational realities of combat operations, it may well lead to a situation in which commanders faced with such a rule begin to disregard the law as irrelevant, a development that has extraordinary consequences for the protection of all persons and the dedication to the rule of law. Finally, the most direct and evident consequence of the effects-based approach is that it opens the door to a grave danger: the exploitation of the law by the defending party for its own defensive and propaganda purposes.

3. Lethal Autonomous Weapons Systems and the Quest for Certainty

As if on a parallel track, the discourse about LAWS and their development, use, and compliance with LOAC is dominated by questions of certainty. Underlying the debate is a desire to understand how these systems work and how humans would interact with them. At a fundamental level, this search for greater clarity, certainty, and predictability is obviously sensible. Knowing and understanding how a weapon works is central to assessing how it can be used effectively and lawfully.

For most weapons, one can see how they work and what they do, in order to use that information to assess the weapon's legality and effectiveness. In contrast, a LAWS that is programmed and then deployed to make targeting decisions without human involvement is quite different and it is difficult to grasp precisely what such a system is doing and how it is making those decisions. And yet, to perform a weapons review for compliance with LOAC, or to determine when and in what circumstances deployment of LAWS is appropriate, predicting what

an autonomous weapon will do and how it will take that action is essential. Similarly, in order to assess the legality of an attack by LAWS for the purposes of accountability, we need to be able to understand what information the system gathered, how it processed that information and assessed the possible options for action, how it determined the identity and legality of the target, how it assessed any harm to civilians and the requisite proportionality determinations, and how it assessed the precautions that were needed and feasible and how to take them. Each of these analyses rests on information and understanding — which rest, in turn, on a level of certainty or predictability. Three issues stand out in particular with respect to the effect on LOAC going forward: certainty of technology, certainty of legal norms, and certainty of analyses and decisions.

A. Certainty of Technology

At the most basic level, significant uncertainty and disagreement persist regarding exactly which types of weapons and weapons systems fall within a category of autonomous weapons. In the face of "confused and circular discussion about terminology"[34] and attempts to define autonomy, the discourse remains mired in this initial search for common ground, hampering attempts to examine the ethical and legal ramifications or boundaries of using LAWS. Any attempt to apply the law to a weapons system, whether autonomous or not, requires definition in order to determine how the law applies, how specific treaty provisions apply, when they apply and so forth. The very workings of LAWS are not entirely understood — certainly by lawyers tasked with assessing the application of the law in using such weapons — resulting in a steady discourse to try to reach a greater level of understanding and certitude. Cyber, nanotechnologies and other new capabilities pose similar challenges for understanding how something one cannot see or perhaps even touch functions. At the operational level, "[t]he logic and behavior of such systems can be quite opaque to the airman, and often the system developers do not fully understand how the autonomy will behave.[35] When these opacities and complexities need to be translated to the lawyers and other advisors, the nature and degree of uncertainty increase significantly, driving still greater demands for certainty and predictability for purposes of assessing the appropriate parameters for use.

A second area concerns the survivability and reliability of LAWS. Survivability can likely be measured with a high degree of confidence during testing and development and is understood as a function of detectability, susceptibility, vulnerability, stability and crashworthiness.[36] Reliability, in contrast, poses enduring certainty issues. As the Office of the Chief Scientist of the

---

[34] Jenks, *supra* note 1, at 9. *See also* ARMIN KRISHNAN, KILLER ROBOTS: LEGALITY AND ETHICALITY OF AUTONOMOUS WEAPONS 43 (2009) ("[a]s the discourse on autonomous robots gets seized more and more by philosophers . . . the confusion about 'autonomous weapons' in the public debate increases").

[35] U.S. Air Force, Office of the Chief Scientist, *Autonomous Horizons: System Autonomy in the Air Force — A Path to the Future* 22-23 (June 2015), http://www.af.mil/Portals/1/documents/SECAF/AutonomousHorizons.pdf?timestamp=1435068339702.

[36] DEP'T OF DEFENSE, UNMANNED SYSTEMS INTEGRATED ROADMAP 4.5.3 (2013). Detectability is the probability of being discovered by an enemy force; susceptibility is the probability of being hit or jammed; vulnerability is the probability of surviving if hit or jammed; stability is the probability the vehicle will reliably operate in the manner that was intended after it has been hit or jammed; and crashworthiness is the probability the vehicle and its load will survive an impact without serious damage. *Id*.

U.S. Air Force explained in a recent report, new tools for verification and validation must be developed, because "[t]raditional methods . . . fail to address the complexities associated with autonomy software [and t]here are simply too many possible states and combination of states to be able to exhaustively test each one."[37] If LAWS will always function the same way in the same situation, then we have a basis to analyze the lawfulness or morality of that action; if not, we are handicapped in making an effective assessment of how well LAWS can or will comply with the law.

Finally, in the absence of extensive operation of LAWS or other new technologies in competitive environments, there is significant uncertainty regarding how such systems will respond in the face of malfunction, jamming, spoofing, errors or infiltration. The increased complexity of LAWS, for example, undermine our ability to predict or even expect how it might act and react. Like any hi-tech item, the more complex the system, the more lines of code and number of interlocking parts and systems it has, thus increasing possibilities for breakdown or malfunction.

Once in an operational environment, additional challenges for predicting behavior arise. First, the increased "number of potential interactions . . . can make testing the autonomous system's operation under every possible environmental condition effectively impossible."[38] Second, adversaries will seek to disable or exploit a LAWS, like any other vulnerability. Such exploitation is most likely achieved "through hacking, spoofing (sending false data), or behavioral hacking (taking advantage of predictable behaviors to 'trick' the system into performing a certain way)."[39] One unfortunate effect of the system's enhanced complexity, however, is that it is "fundamentally more difficult to detect inadvertent bugs or deliberately embedded malware."[40]

The purpose of highlighting these uncertainties is not to argue regarding the propriety or legality of developing and using LAWS. Rather, these uncertainties and complexities are driving ever greater efforts to secure a more precise understanding of what LAWS do and their levels of resilience and reliability. The ICRC notes that, at present, "it is uncertain whether commanders or operators would have the necessary knowledge or understanding to grasp how an autonomous weapon system functions."[41] This understanding—or minimization of uncertainty, to put it another way—is essential to the lawful use of LAWS or any other advanced technology. The commander or operator tasked or intending to deploy LAWS "must personally decide whether the autonomous weapon can perform lawfully given the specific battlefield situation."[42] To do so, she must "be thoroughly familiar with the system's particular capabilities and must know what embedded values have been pre-programmed into it"[43] and how it is likely to act and react as a result. A firmer

---

[37] U.S. Air Force, *supra* note 42, at 23.
[38] Paul Scharre, *Autonomous Weapons and Operational Risk* 14, Center for New American Security Ethical Autonomy Project (February 2016).
[39] *Id*.
[40] U.S. Air Force, *supra* note 42, at 23.
[41] INT'L COMM. RED CROSS, AUTONOMOUS WEAPON SYSTEMS: TECHNICAL, MILITARY, LEGAL AND HUMANITARIAN ASPECTS 87 (2014).
[42] Jeffrey S. Thurnher, *Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective*, *in* NEW TECHNOLOGIES AND THE LAW OF ARMED CONFLICT 213, 224 (Hitoshi Nasu & Robert McLaughlin eds. 2014).
[43] *Id.*

grasp on the likelihood of error or divergence from the intended action is equally important. For example, just as extensive testing and development in the software industry have reduced the error rate substantially,[44] similar efforts are and will be underway to continually reduce the uncertainties of function and result with LAWS. The question for the interplay with LOAC, as examined in Part III, is whether this trend toward certainty of result will bleed over into legal analysis as well.

B. Certainty of Legal Norms in the LAWS Context

Building on extensive discussions regarding the application of LOAC in the development and programming of LAWS and, equally important, in the implementation of combat operations using such weapons systems, this section highlights how select LOAC principles and rules drive efforts at greater certainty regarding the content and the application of the law. This search for greater certainty with regard to how LOAC principles operate in the LAWS context can then trigger a shift towards greater demands for certainty in the application of LOAC and a fundamental change in the reasonableness construct underlying much of LOAC.

The implementation of the principle of proportionality by humans already engenders significant debate. Rather than a quantifiable concept, proportionality is "above all a question of common sense and good faith for military commanders."[45] It requires that commanders weigh vastly different concepts — civilian casualties and military advantage — in the midst of dynamic and uncertain circumstances, without any specific quantitative measure for doing so. As the ICRC Commentary explains, the rule of proportionality "is by no means as clear as it might have been, but in the circumstances it seems a reasonable compromise between conflicting interests and a praiseworthy attempt to impose some restrictions in the domain where arbitrary behaviour has existed too often."[46] Over decades of training and operations, militaries have honed the methodology of proportionality and the ability to gather the intelligence essential to an informed and reasonable judgment. Nonetheless, assessments of military advantage and how many civilian casualties would be excessive in comparison in various situations continue to pose intellectual and operational challenges for both commanders and outside commentators. The notion of the "reasonable commander" accounts for these challenges and difficult qualitative assessments, recognizing in effect a zone of reasonableness rather than one true answer.

However, once we introduce machines into this framework, there is an inherent slide from the qualitative idea of reasonableness and judgment to a more quantitative notion of measuring and programming. For an autonomous system to apply proportionality, it needs to be programmed to "attribute[e] values to objects and persons and mak[e] calculations based on probabilities and context."[47] Some argue that "no known software [is] capable of mechanizing qualitative decision-making [because the] process of evaluation that is implicit in the application of the proportionality

[44] Scharre, *supra* note 46, at 14.
[45] AP I COMMENTARY, *supra* note 28 at 683-4.
[46] *Id*. at 685.
[47] INT'L COMM. RED CROSS, *supra* note 59, at 82.

test is one that only a human brain can properly undertake."[48] Others, however, explore what would be required for LAWS to implement proportionality: the likelihood and extent of civilian casualties, the military advantage, and a comparison of the two.

Using algorithms similar to the U.S. military's collateral damage estimate methodology (CDEM),[49] an autonomous system could assess "factors such as a weapon's precision, its blast effect, attack tactics, the likelihood of civilian presence, and the composition of buildings"[50] and reach results of comparable reliability to the CDEM system currently used. Military advantage, in contrast, poses more significant challenges: "Given the complexity and fluidity of the modern battle space, it is unlikely in the near future that, despite impressive advances in artificial intelligence, 'machines' will be programmable to perform robust assessments of a strike's likely military advantage."[51] Over time, however, quantitative measures assigning value to specific military equipment might serve as a simplistic substitute for the more qualitative judgment inherent in assessing military advantage.

To make proportionality work for an autonomous system, we need to quantify both the component parts of the proportionality methodology and the balancing or comparative aspect that produces the decision to attack or refrain from attack. Quantifying relies on specific measures or metrics, leading to efforts to impose greater certainty on the entire proportionality construct to develop a measurable paradigm rather than one based primarily on good faith and objective reasonableness. In effect, the challenges of translating proportionality into the world of autonomy may well lead to the world of autonomy imposing certainty and quantitative analysis on the methodology of proportionality.

A second LOAC rule that introduces concerns about certainty is the rule mandating that in case of doubt, a person is presumed to be a civilian.[52] Like many other such judgments in LOAC, any rebuttal of the presumption of civilian status must be based on the attacker's reasonable assessment based on the information available at the time. Although LAWS may be well-suited to make distinction determinations regarding some military objectives, given "established technology which enables sensors to detect and recognize pre-determined categories of military equipment,"[53] doing so with respect to persons raises significantly more difficult questions. A machine needs to determine not only whether an individual is a combatant or member of an

---

[48] William Boothby, *How Far Will the Law Allow Unmanned Targeting to Go?*, *in* INTERNATIONAL HUMANITARIAN LAW AND THE CHANGING TECHNOLOGY OF WAR 46, 57 (Dan Saxon ed. 2013).

[49] Chairman of the Joint Chiefs of Staff Instruction 3160.09, No-Strike and the Collateral Damage Estimation Methodology (Feb. 13, 2009).

[50] INT'L COMM. RED CROSS, *supra* note 59, at 83.

[51] Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARV. NAT'L. SEC. J.: FEATURES ONLINE 20 (2013).

[52] Additional Protocol I, *supra* note 2, art. 50(1). The customary law status of this rule or the precise contours of the rule remain in dispute. *See* Int'l Comm. Red Cross, Customary International Humanitarian Law Rule 6 and associated commentary; DOD LAW OF WAR MANUAL, *supra* note 5, at 5.4.3.2.

[53] Boothby, *supra* note 66 at 55 (The technology uses algorithms, such that the sensors on the attacking aircraft detect features in the target object which accord with data pre-programmed into the fire control system. When sufficient points of recognition have been achieved to a given level of probability, the unmanned aircraft will, depending on the instructions programmed into the system in advance of the mission, characterize the observed object as a target and may then commence attack procedures").

organized armed group — in which case the individual is not a civilian at all — but also whether an individual who appears to be a civilian is directly participating in hostilities so as to lose the protection from attack otherwise inherent in civilian status. Both this latter step and the assessment of doubt with regard to civilian status pose challenges for LAWS that are likely to introduce a trend towards certainty, much like proportionality.

First, the definition of civilian in LOAC is a negative definition, based on what a civilian is not—a combatant or a member of an organized group. As a result, we may lack identifiable definitional characteristics for a civilian that could be fed into a machine's processes.[54] Second, as the ICRC explains, "programming [direct participation in hostilities] criteria into a machine would appear a formidable task because of the qualitative analyses required . . ., such as the assessment of the likely adverse effects of an act, . . . whether the individual is acting in support of a party to the conflict"[55] and the individual's intentions. Third, it is unclear that a machine can measure doubt in a manner similar to humans or to how we currently understand the LOAC rule. Doing so would require the development of an "algorithm that can both precisely meter doubt and reliably factor in the unique situation in which the autonomous weapon system is being operated," which is "hugely challenging."[56]

The very notion of presuming civilian status in case of doubt means that any change in how an individual is perceived depends on additional information, but how much and what type of information is not specified. Efforts to program a machine to assess when a civilian is no longer a civilian, or when a civilian is no longer protected from attack because of direct participation in hostilities, will therefore seek to introduce quantifiable measures for the types and amount of information required. Attaining greater understanding of how to apply these essential rules of LOAC is, of course, highly desirable. But on a broader level, the continued injection of certainty or quantitative measures into areas traditionally understood as qualitative, based on reasonableness, may well prove destabilizing for LOAC.

C. Certainty of Analyses and Decisions

Understanding how an autonomous system undertakes analysis and reaches decisions is a final area driving demands for greater certainty. In an environment in which the commander's decision and judgment are critical facets of any determination of legality, we have an innate comfort level in both relying on and judging the propriety of another human's decision-making and judgment. Human beings take certain steps in a decision-making process: using senses to collect data; thinking about the data in order to reason; making plans; and making decisions and acting on those decisions.[57] Since we all do this in some form or another, we have the capacity to

---

[54] *See e.g.*, Noel Sharkey, *Grounds for Discrimination: Autonomous Robot Weapons*, 11 RUSI DEFENCE SYSTEMS 86, 87 (2008) ("A computer can compute any given procedure that can be written down in a programming language. We could, for example, give the robot computer an instruction such as, 'if civilian, do not shoot'. This would be fine if and only if, there was some way of giving the computer a clear definition of what a civilian is").

[55] INT'L COMM. RED CROSS, *supra* note 59, at 80.

[56] Schmitt, *supra* note 68, at 16-17.

[57] Darren Ansell, *Research and Development of Autonomous 'Decision Making' Systems*, *in* INT'L COMM. RED CROSS, *supra* note 59, at 39.

judge when these steps are taken or not taken, when the process is carried out well or is carried out in an unreasonable manner.

However, reaching a comfort level with autonomous decision-making requires more clarity about how an autonomous system makes decisions and analyzes information. With machines, certainty is often quantified by a confidence rating or error rating, which measures how certain the machine is that what it senses is in fact what it actually is. Quantifying decisions in this manner is useful for assessing how well a machine does the individual parts of its job, but does not offer much guidance for determining how well it makes complex decisions in a dynamic environment and whether it does so better or worse than a human operator. As a result, much of the debate about many new technologies rests on how much certainty we can have — about the decisions LAWS would make, for example, or how other hi-tech weapons would operate.

For decades, machines have replaced humans for many tasks, and in nearly all cases, we expect that the machine will be more precise—machines do not get distracted or make silly errors. Clearly we would not tolerate a calculator that made periodic errors like a human being. Translating this perception of perfection in machines raises interesting challenges for both the application of the law and any long-term ramifications for the law in the world of high technology weapons. Although there is "an implicit assumption that a system will continue to behave in a predictable manner after commands are issued[,] clearly this become problematical as systems become more complex and operate for extended periods."[58]

This unpredictability is a function of the dynamic environment in which LAWS and other high technology systems operate and is also a source of consternation in attempting to understand sufficiently how a system works and what it would do in a given circumstance. An underlying question therefore will ultimately be how comfortable we are with uncertainty in a machine, rather than in a human. Here lies the key issue for the relevant discussion: whether the method and process of machine decision-making will lead to a quantitative approach to judging what LAWS do. In effect, because analyzing whether a machine's decision is reasonable is difficult, if not impossible, given the wholly different decision making process machines currently do or would use, any judgment regarding a machine's decision is effectively based on a series of certainty measures—for example, a 99% confidence rating regarding the identification of an object and similar measures—and the programmable response to different levels of certainty.

4. WHAT EFFECT ON LOAC: SEPARATING CERTAINTY FROM REASONABLENESS

For any weapon or piece of equipment, there is a level of information or knowledge we expect to have before approving or deploying it. That differs, however, from how we view or judge the attacker's decision to launch an attack using that weapon, which is assessed on the basis of objective reasonableness. LAWs and other new technologies challenge the distinction between these two considerations, because an autonomous system is not simply being used, but is or would

[58] UK Ministry of Defence, Development, Concepts and Doctrine Centre, *The UK Approach to Unmanned Systems, Joint Doctrine Note 2/11* ¶ 510 (March 30, 2011). *See also* INT'L COMM. RED CROSS, *supra* note 59, at 71 ("Since autonomous systems are adaptable (within programmed boundaries) they are necessarily unpredictable").

be making its own decisions as an autonomous actor. Nonetheless, it is important to separate the quest for certainty about how new technologies work from the distinct question of whether the attack or other combat operation an autonomous system executes is in accordance with LOAC.

A. Responsible Command and Command Responsibility

The doctrine of command responsibility is a form of liability that holds an individual in a leadership position accountable for the actions of her subordinates. Command responsibility rests on two fundamental elements: the commander knew or had reason to know that the subordinates committed or were about to commit violations of LOAC and the commander failed to take necessary and reasonable measures to prevent such acts or punish the violations.[59] Although command responsibility overall raises many challenging issues in the context of new weapons technologies, the second element of necessary and reasonable measures highlights key issues in the interplay between reasonableness and certainty.

The obligation to take necessary and reasonable measures—such as training, orders prohibiting unlawful acts, or disciplinary and criminal action—is a fundamental incident of responsible command.[60] The type of measures considered necessary and reasonable is limited by what is possible in the circumstances at the time. As the ICTY held, it is important to recognize "that international law cannot oblige a superior to perform the impossible. Hence, a superior may only be held criminally responsible for failing to take such measures within his powers . . . [or] within his material possibility."[61]

Applying these notions of reasonable measures to the use of new weapons technologies immediately introduces the question of certainty and how it relates to or even supersedes reasonableness. Regarding LAWs, for example, some argue that in order to impose criminal responsibility, whether direct or superior responsibility, "it must be always possible to predict what [LAWS] do; otherwise humans cannot remain responsible for their conduct and only human beings

[59] Trial of General Tomoyaki Yamashita, Case No. 21, Judgment (U.S. Mil. Comm'n, Manila Oct. 8, 1945-Dec. 7, 1945), *reprinted in* 4 U.N. WAR CRIMES COMM'N, LAW REPORTS OF TRIALS OF WAR CRIMINALS 1 (1945); Additional Protocol I, *supra* note 2, arts. 86, 87; Rome Statute of the International Criminal Court art. 28, July 17, 1998, 2187 U.N.T.S. 90; Statute for the International Criminal Tribunal for the Former Yugoslavia art. 7(3) (May 25, 1993); Statute of the International Criminal Tribunal for Rwanda art. 6(3) (Nov. 8, 1994); Statute of the Special Court for Sierra Leone art. 6(3), Jan. 16, 2002, 2178 U.N.T.S. 137; Prosecutor v. Aleksovski, Case No. IT-95-14/1-T, Judgement (Int'l Crim. Trib. for the former Yugoslavia, June 25, 1999); Prosecutor v. Blaškić, Case No. IT-95-14-T, Judgement (Int'l Crim. Trib. for the former Yugoslavia March 3, 2000); Prosecutor v. Kordić and Čerkez, Case No. IT-95-14/2-T, Judgement (Int'l Trib. for the former Yugoslavia Feb 26, 2001); Prosecutor v. Askayesu, Case No. ICTR-96-4-T, Judgment, Int'l Crim. Trib. for Rwanda, Sept. 2, 1998); Prosecutor v. Kayishema and Ruzindana, Case No. ICTR-95-1-T, Judgment (Int'l Crim. Trib. for Rwanda, May 21, 1999); *In re* Yamashita, 327 U.S. 1 (1946).

[60] *See* AP I COMMENTARY, *supra* note 28, ¶¶ 3548-49 ("The first duty of a military commander . . . is to exercise command"; if commanders "refrain from taking the requisite measures [to prevent abuses], or if, having taken them, they do not ensure their constant and effective application, they fail in their duties and incur responsibility").

[61] Prosecutor v. Delalić, Case No. IT_96-21-T, Judgement ¶ 395 (Int'l Crim. Trib. for the former Yugoslavia, Nov. 16, 1998).

are addressees of international humanitarian law."[62] This approach demands a level of certainty regarding how LAWS work, how they make decisions, how they respond to the operational environment, how often and why they malfunction, and how they respond to hacking or other adversarial exploitation, a level of certainty that simply may not be attainable. In the absence of a firm understanding of how LAWS work and clear rules to govern their deployment, and thus to assess the commander's decision to use them, "it will be difficult if not impossible to establish that a commander had sufficient knowledge of the misuse of complex autonomous weapon systems to justify the imposition of criminal liability for his or her failure to prevent or suppress violations."[63] In effect, command responsibility appears to rest on whether a commander took reasonable measures to prevent violations by an autonomous weapon system, an inquiry that depends on the commander's ability to control or predict the system's decisions so as to know when and whether to take such preventive measures.

This inquiry sparks several questions highlighting how the interplay between certainty and reasonableness can create confusion and even detrimental developments in the interpretation and application of LOAC. A primary question is whether the commander, before deploying an autonomous system, must determine if the system will make the *right* decision or if the system will make a *reasonable* decision. The latter approach to assessing decision-making accords most closely with LOAC's basic reliance on objective reasonableness in the application and post-hoc analysis of distinction, proportionality and precautions. However, it depends almost completely on a comfort level and understanding of how LAWS make decisions, a challenge that raises certainty questions of its own, as discussed above. Alternatively, if the obligation is for the commander to determine that the autonomous system will make the right decision, our current understanding of LAWS suggests that it is highly improbable. And yet the nature of our interaction with machines generally is that we expect and want machines to "get it right" every time, so coming to terms with what appears to be a lesser threshold for a commander to be willing to use an autonomous system may be difficult.

Related questions raise similar issues. For example, imagine that an autonomous weapon system makes a faulty decision and targets a civilian or civilian object. If that faulty decision is considered sufficient to demonstrate that the commander was unreasonable in deploying the weapon, then the commander is effectively being held to a strict liability standard, one more stringent than that applied with regard to acts of subordinates. In contrast, if the relevant judgment is whether the commander's decision to deploy the weapon in the circumstances was reasonable, then the actual targeting decision — made by the autonomous system — is not truly assessed and potentially no responsibility is assigned for what may be a violation of the law. One might also ask how much a commander should be required to foresee the unforeseeable if the autonomous system is deployed as provided. This question includes how much a commander should be able to anticipate breakdowns, jamming, spoofing, infiltration or exploitation, and even errors, all of which introduces the question of what level of technological understanding is required, for both the commander and her subordinates deploying LAWS. More important, after an attack leading to

---

[62] Marco Sassòli, *Can Autonomous Weapon Systems Respect the Principles of Distinction, Proportionality and Precaution?*, *in* INT'L COMM. RED CROSS, *supra* note 59, at 41.
[63] Jack M. Beard, *Autonomous Weapons and Human Responsibilities*, 45 GEO. J. INT'L L. 617, 659 (2014).

civilian harm or other indicators of a possible LOAC violation, the difficulty in understanding precisely how LAWS or other new technologies work may interfere with or even eliminate any ability to assign responsibility because of an inability to determine what actually went wrong. At present, it is unclear how the interplay between certainty and reasonableness, and the likely trend towards greater demands for certainty, will affect the application and future development of the doctrine of command responsibility, but the potential for disruption clearly exists.

B. Shifting LOAC to a Certainty Approach

A leading proponent of LAWS argues that one powerful reason to employ autonomous systems is their ability to act conservatively, to risk their own safety so as to ensure a high level of certainty in target identification before engaging the target.[64] The idea is that LAWS could, ideally, perform better than humans in the implementation of distinction, proportionality and precautions. Whether this is attainable remains subject to extensive debate, but nonetheless the discourse already demonstrates that "while autonomous weapons systems cannot be required to be perfect, they will in practice be held to standards that are significantly higher than those posed for humans."[65] These two developments—certainty in targeting decisions and a more stringent standard for decision-making—raise significant concerns about the impact on LOAC going forward.

As Part II explores, discomfort with the uncertainty seemingly inherent in LAWS is a strong impetus either for a total ban on the development and use of LAWS or for measures to impose greater certainty on the circumstances and terms of their use. These efforts at greater certainty appear with respect both to how LAWS function and to how key LOAC norms apply when implemented by an autonomous system. Indeed, finding the threshold of certainty needed is central to the entire enterprise: "[t]he tricky part is developing machines whose behavior is predictable enough that they can be safely deployed, yet flexible enough that they can handle fluid situations."[66] For human actors on the battlefield, training is the primary tool to enhance consistency and capability. For a machine, it is programming that seeks to accomplish a comparable goal, but a goal that most frequently is thought of in terms of result, that is, in quantitative terms, through the idea of an error rating or certainty of result. This partly because

---

[64] Ronald Arkin, *Lethal Autonomous Systems and the Plight of the Non-combatant*, AISB QUARTERLY 1, 3 (2013), http://www.cc.gatech.edu/ai/robot-lab/online-publications/aisbq-137.pdf.

[65] Christof Heyns, *Increasingly Autonomous Weapon Systems: Accountability and Responsibility*, *in* INT'L COMM. RED CROSS, *supra* note 59, at 45, 47. *See also* Robin Geiß, *The International-Law Dimension of Autonomous Weapons Systems* 17, Friedrich-Ebert-Siftung International Policy Analysis (June 2015) ("one can conclude that such systems . . . should have to satisfy a much higher standard. [Regarding distinction, for example], a legal duty could be established for the developers of autonomous weapons systems to program them in such a way that they use force only in the case of unequivocally aggressive and offensive behavior on the part of enemy combatants/fighters. In situations, by contrast, that are not clear-cut in this respect, such systems would have to refrain from the use of lethal force even if human soldiers in an identical situation would be permitted to reach for their weapons.").

[66] Matthew Rosenberg and John Markoff, *The Pentagon's 'Terminator Conundrum': Robots That Could Kill on Their Own*, N.Y. TIMES, Oct. 25, 2016.

"the ability to handle uncertainty and unpredictability remain uniquely human virtues, for now,"[67] although clearing this hurdle lies at the heart of the LAWS enterprise.

A critical consequence of this inherent difference between human and machine is that certainty and quantifiable measures begin to substitute for reasonableness as a measure of success or, in the context of LOAC and armed conflict, as a measure of lawfulness. As an initial concern, judging an autonomous weapon system's targeting decision based on a quantifiable measure of certainty will mean that targeting decisions by machines and targeting decisions by humans are judged on different standards. While this differentiation in standard might make sense at first or be the only way that we can reach a comfort level with the use of LAWS, it raises the specter of the same attack being lawful if undertaken by one type of actor but not if launched by the other.

This result is fundamentally at odds with the underlying notion of equality of arms and the consistent understanding that greater technological capability does not impose higher standards of legal obligation. More problematic, however, is the more likely result: the higher certainty-based standard applied to autonomous systems will steadily bleed over into the analysis of decisions and attacks by human actors, changing the foundational standard of objectively reasonable into one based on certainty at the time of decision or, more likely, on actually being correct.

Substituting certainty, being correct, or some other quantifiable measure for reasonableness is plainly at odds with LOAC. It removes the foundation for operational judgment in combat operations, "wish[ing] away the exercise of judgment and discretion by military decision-makers."[68] It effectively imposes an effects-based or strict liability standard — if the threshold of certainty is not met, or if the decision turns out to be wrong after the fact, the attack is unlawful. Once certainty begins to replace reasonableness in the application of the law, an effects-based analysis is the only way to achieve such certainty.

This approach would require commanders to operate with a standard that allows for no errors. Doing so would run counter to the established legal standard in Additional Protocol I, the ICTY Statute, the Rome Statute and customary international law: that commanders are obligated to make reasonable decisions based on the information available at the time of the attack. This standard applies across the legal principles of distinction, proportionality and precautions, as explained in Part I above. Thus, for example, an attacker "must take all reasonable steps to ensure . . . that the objectives [to be attacked] are identified as military,"[69] and must assess whether the expected civilian casualties, civilian injury or damage to civilian objects are excessive in light of the anticipated military advantage gained. These determinations are based on the circumstances and information available at the time of the attack, not the results and facts that come to light afterwards: the "law does not judge commanders based on the outcome alone, nor does it require commanders to be right in all circumstances."[70]

---

[67] *Id*.
[68] Merriam, *supra* note 30, at 142 ("it is the effort to somehow quantify reasonableness that ought to be controversial. Seeking to set a 'level' or threshold of certainty is a fool's errand, predicated on the false notion that all possible combat scenarios can be foreseen and accounted for.").
[69] FM 27-10, *supra* note 40, at ¶ 41.
[70] OPERATIONAL LAW EXPERTS ROUNDTABLE, *supra* note 47, at 6.

Since the Nuremberg Tribunals, the law has required that "an individual should not be charged or convicted on the basis of hindsight but on the basis of information available to him or information he recklessly failed to obtain at the time in question."[71] The ICTY has consistently taken the same approach, holding that in order "to establish the *mens rea* of a disproportionate attack, the Prosecution must prove . . . that the attack was launched willfully and in knowledge of circumstances giving rise to the expectation of excessive civilian casualties."[72] Certainty or perfection is not the LOAC standard. Rather,

> [t]he reasonableness of [one's] actions is the touchstone for determining compliance with [LOAC]. The law allows for mistakes in the Clausewitzian "fog of war." Intelligence may be incomplete or faulty, technology may fail to function properly, and tactical conditions may change after a targeting decision has been made and beyond the point at which an attack may be abandoned. [LOAC] does not require perfection.[73]

If human actors start to be judged on the basis of a higher or certainty-based standard used for machines, this fundamental framework begins to unravel. Relying on quantifiable measures or a strict liability standard effectively reduces any assessment of a commander's decision to one based on the effects of the attack in question, because that is the easiest information to gather, quantify and measure. In addition to being wrong as a matter of law,[74] it also raises significant concerns about the misapplication and future development of LOAC, ultimately leading to greater danger for the civilians and civilian areas the law seeks to protect.

First, the effects-based approach disregards the notion of targeting as methodology and ignores operational realities that inform both the targeting process and any careful analysis thereof. Although difficult in many circumstances, commanders engage in this methodology and process every time they apply combat power with consequences for civilians, sometimes in a longer, deliberative process and sometimes in the split second available for troops in contact and fleeting targets. The core targeting principles highlight the goal of a balance between military needs and humanitarian concerns that minimizes civilian harm as much as possible, and the methodology provides guidance on how to achieve that goal—by gathering and analyzing information about the identity of the target, its military value, and the consequences to the civilian population and civilian objects in the area, and making choices among various operational alternatives to achieve the mission while minimizing harm to civilians. This methodology functions in tandem with the operational realities of combat operations. Although careful planning for military operations attempts to incorporate as many operational variables as possible, it is an axiom of military operations that "no plan survives first contact with the enemy." All of these variables are integral

---

[71] USA v. List, *supra* note 26, at 57. This principle is known as the Rendulic Rule; *see* note 24, *supra*, and accompanying text.
[72] Prosecutor v. Galić, *supra* note 31, ¶ 59.
[73] Michael N. Schmitt and Eric W. Widmar, *"On Target": Precision and Balancing in the Contemporary Law of Targeting*, 7 J. NAT'L SEC. L. & POL'Y 379, 401 (2014).
[74] *See* Corn, *supra* note 43 at 318 ("This effects-based focus, however, is inconsistent with fundamental tenets of the law, which demand reasonable combat judgments, which must be assessed contextually, and not based on retrospective analysis.").

to any targeting process at the time of the planning and the attack and to assessing the reasonableness of the commander's decision-making process.

In contrast to this sophisticated and reality-based methodology, an effects-based rule is likely to impose liability regardless of process or effort expended to protect civilians and civilian objects, thus undermining the essential value of this methodology by leaving commanders with only the after-the-fact effects to determine right from wrong. It is thus not simply a higher standard, but a qualitatively different standard altogether. However, "[r]easonableness is not a threshold; rather, it is an attribute of decision-making that can be judged only in context."[75] Even if an autonomous system is programmed to make decisions based on all of the operational considerations and the context, it remains likely that such programming will rely more on a quantifiable measure of certainty or error as a tool to reach what would be considered a reasonable judgment. Over time, this may well replace the quality of reasonableness with a more quantitative measure which, when it spreads back to the arena of human decision-making, will strip commanders and soldiers of the tools and methodology that guide lawful and effective decision-making and execution of combat operations.

Second, divorcing the application of the law from operational realities introduces the very real danger that commanders faced with such a rule will disregard the law as irrelevant. Interestingly, the very effort to maximize the collection and analysis of information and to create a higher level of certainty with regard to identification of targets, harm to civilians, and necessary precautions is likely to have a counter effect when these new standards and expectations filter back down to the application of LOAC to human decisions. Thresholds of certainty and a reliance on results after the fact will create a culture of unpredictability and uncertainty regarding the law and the application of legal standards to operational conduct and decisions. The complexity of the operational environment and the effect of both the enemy's tactics and unexpected changes from the myriad of operational variables mean that an attacker cannot know with certainty what the result of an attack will be. If that certainty is the legal standard, however, the law becomes operationally illogical. Commanders will either refrain from engaging in military operations altogether out of an overabundance of caution in the face of an impossible standard, or will simply disregard the law entirely as no longer relevant to their purposes and mission. Under either scenario, innocent civilians are the ultimate victims—a result directly at cross-purposes with a central goal of LOAC.

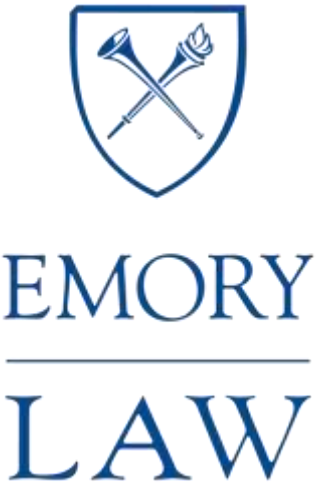
Finally, the most direct and evident consequence of the effects-based approach is that it opens the door to a grave danger: the exploitation of the law by the defending party for its own defensive and propaganda purposes. If the results of an attack determine the lawfulness of that attack, the defending party's precautionary obligations are emasculated because they no longer factor into the legal assessment of who bears responsibility for the harm to civilians. "When parties face no legal consequences, and a potential operational advantage, for co-mingling civilian and military objects, every apartment will be a command center as militaries and armed groups embed

[75] Merriam, *supra* note 30, at 129 (noting that a "targeting decision based on a particular degree of certainty about a target may be entirely reasonable in one context but unreasonable in another" and arguing that "assigning a percentage to certainty is inherently dangerous").

themselves in cities to use the civilian population as a shield."[76] But these tactical advantages are merely the beginning. These tactics often have a more problematic, strategic purpose: to use the resulting civilian deaths as a broader strategic tool to level accusations of war crimes, diminishing support for the war effort and the overall legitimacy of the military operation. Legal assessments based on effects merely ratify the use of civilians and the civilian population as a shield for military operations and — albeit unintentionally, of course — directly undermine the very purpose of LOAC's core principles of distinction, proportionality and precautions.

LAWS appear to offer significant potential for a variety of uses in combat operations, including perhaps autonomous identification and attack of targets without human involvement at some point in the future. If, as some argue, autonomous systems can achieve more accuracy and a higher level of protection for civilians and civilian objects, that accomplishment will be a positive development. The process of achieving that goal, however, presents unintended challenges and consequences for the application and implementation of LOAC in all other combat scenarios in which humans remain the actors and decision-makers. Understanding how the sensible desire for greater certainty with regard to new technologies can, and in fact is likely to, alter the existing and foundational understanding of the roles of certainty and reasonableness in LOAC, to detrimental effect, is therefore an essential aspect of the discourse going forward.

[76] OPERATIONAL LAW EXPERTS ROUNDTABLE, *supra* note 47, at 11.



The Extent of Self-Defense Against Terrorist Groups: For How Long and How Far?

Laurie R. Blank
Emory University Law School

THE EXTENT OF SELF-DEFENCE AGAINST TERRORIST GROUPS: FOR HOW LONG AND HOW FAR

By Laurie R. Blank[*]

47 ISRAEL YEARBOOK ON HUMAN RIGHTS (forthcoming 2017)

I. INTRODUCTION

State use of military force against terrorist groups has been a defining feature of the post-9/11 world since the United States began bombing al Qaeda and Taliban forces in Afghanistan in the fall of 2001. At a fundamental level, States using military force to protect their territory, their inhabitants and their interests is, of course, nothing new. The right to use force in self-defence is a long-established principle of international law and States have resorted to force in self-defence throughout history, against both State and non-State attacks and threats. Modern international law, including the United Nations Charter and customary international law, provides a comprehensive and well-accepted framework for assessing the legality of a resort to force in self-defence. No less, although States and other actors in the international system may disagree vehemently about the lawfulness of any particular self-defence enterprise, the fact that nearly all States embarking on self-defence actions participate in both the procedural framework for such action through communication with the United Nations Security Council and the international legal discourse demonstrates that the overarching legal infrastructure regarding the use of force in self-defence remains the enduring and appropriate legal framework, regardless of State aggression, transnational terrorism, or other challenges to the international order.

Notwithstanding extensive legal debates over whether a State has a right to use force in self-defence against a non-State group outside its borders, State practice in the aftermath of 9/11 provides firm and increasing support for the existence of a right of self-defence against non-State actors, even if unrelated to any State.[1] Repeated incidents of States responding to attacks by non-

[*] Clinical Professor of Law and Director, International Humanitarian Law Clinic, Emory University School of Law. I would like to thank Matthew Johnson (J.D., Emory Law 2016) for his outstanding research assistance.

[1] The international response to the September 11th attacks on the United States are particularly instructive. Both the United Nations Security Council and the North Atlantic Treaty Organization issued resolutions characterizing the attacks as an armed attack triggering the inherent right of self-defense. S.C. Res. 1368, 1, U.N. Doc. S/RES/1368

State groups with forceful measures, both before and after 9/11, have triggered a rich international legal discourse on the nature of an armed attack,[2] whether attribution to a State is required,[3] the meaning of imminence,[4] and the substantive content of the classic requirements of necessity, proportionality and immediacy.[5] But the post-9/11 environment in which states — the United States in particular — may use self-defence as an ongoing and overarching justification and construct for military operations, whether episodic or sustained in nature, against one or more non-state groups for more than fifteen years and counting poses challenges to the very concept of self-defence anew. In particular, this ongoing reliance on self-defence appears to include locations and groups not contemplated at the time of the initial incident or incidents triggering the right to self-defence. This scenario raises essential questions about the extent of self-defence: how far can a State go when acting in self-defence — both in the geographical sense and in the sense of the legitimate aims of using force — and for how long does this right of self-defence last? In this era of extended campaigns

---

(Sept. 12, 2001); North Atlantic Treaty, art. 5, Apr. 4, 1959, 34 *U.N.T.S.* 243, 246; Press Release, NATO, Statement by the North Atlantic Council (Sept. 12, 2001). The September 11th attack was the only instance in which NATO invoked collective self-defense under Article 5 of the North Atlantic Charter. Australia activated the collective self-defense provisions of the ANZUS Pact; Security Treaty, U.S.-Aust.-N.Z., art. IV, Sept. 1, 1951, 3 U.S.T. 3420, 3423, 131 U.N.T.S. 83, 86; B. Pearson, "PM Commits to Mutual Defence", *Austl. Fin. Rev.*, 15 Sept. 2001; and the Organization of American States responded similarly as well; Inter-American Treaty of Reciprocal Assistance, art. 3.1, Sept. 2, 1947, 21 *U.N.T.S.* 77, 93; Terrorist Threat to the Americas, Res. 1, Twenty-fourth Meeting of Consultation of Ministers of Foreign Affairs, Terrorist Threat to the Americas, OAS Doc. RC.24/RES.1/01 (Sept. 21, 2001).

2 *See* Case Concerning Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, I.C.J. Reports 2005 at 168, ¶¶ 146–47; N. Lubell, *Extraterritorial Use of Force Against Non-State Actors* 30–36 (2010); D. Bethlehem, "Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors", 106 *Am. J. Int'l L.* 1 (2012).

3 S. D. Murphy, "Terrorism and the Concept of "Armed Attack" in Article 51 of the U.N. Charter", 43 *Harv. J. Int'l L.* 41 (2002); K. N. Trapp, "Can Non-State Actors Mount an Armed Attack?", *in The Oxford Handbook on the Use of Force in International Law* (2015) ("The ICJ's decisions in *Nicaragua*, *Palestinian Wall*, and *DRC v. Uganda* might be interpreted as limiting 'armed attacks' to uses of force by or attributable to a State.").

4 *See* W. C. Bradford, "The Duty to Defend Them": A Natural Law Justification for the Bush Doctrine of Preventative War", 79 *Notre Dame L. Rev.* 1365 (2004); N. S. Erakat, "New Imminence in the Time of Obama: The Impact of Targeted Killings on the Law of Self-Defense", 56 *Ariz. L. Rev.* 195 (2014); J. Yoo, "Using Force", 71 *U. Chi. L. Rev.* 729 (2004); "Imminence" in the Legal Adviser's Speech", *Lawfare* (6 Apr. 2016), available at https://www.lawfareblog.com/imminence-legal-advisers-speech.

5 C. J. Tams & J. G. Devaney, "Applying Necessity and Proportionality to Anti-Terrorist Self-Defense", 45 *Isr. L. Rev.* 91 (2012); K. N. Trapp, "Back to Basics: Necessity, Proportionality, and the Right of Self-Defense Against Non-State Terrorist Actors", 56 Int'l & Comp. L. Q. 141 (2007).

against transnational terrorist groups, examination of such questions is essential to an understanding of self-defence and, therefore, an effective assessment of the legality of State action against such groups.

This article explores the extent of self-defence, particularly in the context of a State using force in self-defence against one or more terrorist groups located in one or multiple locations outside the boundaries of the State. Although identifying the ends of self-defence is relevant to situations of self-defence against attacks by another State or by a more conventional insurgent non-State group, perhaps in a spillover of an existing non-international armed conflict, it is in the realm of transnational terrorism and State responses thereto that the questions of duration, extent and degree of force become most challenging. Matching the international law framework to the operational realities becomes more and more difficult, such that "[w]here hostilities with groups such as Al Qaeda, Hezbollah, or the Taliban extend in time and/or scope, it becomes increasingly challenging to apply self-defence principles to regulate a State response in the same way as is suggested for more isolated uses of force."[6]

Part I provides foundation for the analysis, providing background on both the nature of the extended campaign of self-defence against transnational terrorist groups and the international legal framework for the use of force in self-defence. Part II then examines how the differing conceptions of the legitimate aims of self-defence affect the extent of self-defence. First, this section analyzes the operational goals different States have put forth when acting in self-defence against terrorist groups. Examining how these objectives match with the international legal framework provides a useful tool for considering how the self-defence principles of necessity and proportionality play out in this extended self-defence paradigm. Second, this section addresses the notion of counterterrorism operations against transnational terrorist groups as armed conflict and the consequences of a "war" framework for the parameters of self-defence. Finally, Part III raises questions that naturally follow from a State's initial success in countering a terrorist group with armed force and pose new challenges for the self-defence analysis. For example, as a State's military operations damage a group's ability to operate, it will seek new bases from which to operate in different States or regions and it may splinter into multiple groups or reconstitute itself as one or more new groups. These developments, along with the appearance of new groups inspired by or declaring allegiance to the original terrorist group, require further analysis of whether the nature and

6 K. Watkin, *Fighting at the Legal Boundaries: Controlling the Use of Force in Contemporary Conflict,* 67 (2016).

extent of self-defence changes — and how — in light of the dynamic operational environment for counterterrorism.

I. FRAMING THE ISSUE

It is axiomatic today that a terrorist group based thousands of miles away in the remote reaches of a developing nation can pose a significant threat to a powerful industrialized nation such as the United States, France or the United Kingdom. Encrypted communication, internet propaganda, the flow of people, weapons and money across borders — many of the freedoms and advances of the modern world offer countless opportunities for groups intent on launching spectacular attacks on civilians. Indeed, the United Nations Security Council has repeatedly characterized international terrorist attacks as a threat to international peace and security, both after 9/11 and after many other attacks.[7] The international community has seen a rapid evolution in the application of international law to the need to respond to terrorist acts and terrorist groups in self-defence, with "the acceptability of resorting to military force in response to transnational terrorism crystalliz[ing] in the aftermath of 9/11."[8] In examining how far this right to respond extends, in time, space and degree, an initial discussion of both the range of self-defence actions launched and the basic international legal framework is useful.

A. The Use of Self-Defence Against Terrorist Groups

On October 7, 2001, the United States declared, in a letter to the President of the United Nations Security Council, that it had "initiated actions in the exercise of its inherent right of individual and collective self-defence following the armed attacks that were carried out against the United States

7 S.C. Res. 1368, ¶ 1, UN Doc. S/RES/1368 (Sept. 12, 2001) ("Unequivocally condemning in the strongest terms the horrifying terrorist attacks which took place on 11 September 2001 in New York, Washington, D.C. and Pennsylvania and regards such acts, like any act of international terrorism, as a threat to international peace and security"). *See also* S.C. Res. 1373, UN Doc. S/RES/1373 (28 Sept. 2001); S.C. Res 1438, UN Doc. S/RES1438 (14 Oct. 2002); S.C. Res. 1440 (UN Doc. S/RES/1440 (24 Oct. 2002); S.C. Res. 1450, UN Doc. S/RES/1450 (13 Dec. 2002); S.C. Res. 1530, UN Doc. S/RES/1530 (11 Mar. 2004); S.C. Res. 1611, UN Doc. S/RES/1611 (7 Jul. 2005).

8 M. N. Schmitt, "Responding to Transnational Terrorism Under the *Jus ad Bellum*: A Normative Framework," *in Essays on Law and War at the Fault Lines* 49, 57 (M. N. Schmitt ed., 2012).

on 11 September 2001."[9] These military operations were launched against "Al-Qaeda terrorist training camps and military installations of the Taliban regime in Afghanistan."[10] Since that time, the United States has announced countless actions in self-defence, against numerous groups in equally numerous countries around the world. Strikes and other actions against al Qaeda personnel and facilities have been launched in Afghanistan,[11] Pakistan,[12] Yemen,[13] Somalia[14] and other countries. The United States has also used force in self-defence against al Qaeda in the Arabian Peninsula (AQAP), an offshoot of al Qaeda, striking AQAP operatives in Yemen,[15] and

9 Letter dated 7 Oct. 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2001/946, 7 October 2001.

10 *Id*.

11 Operation Enduring Freedom was the primary United States operation against al Qaeda from 2001-2014 and was succeeded by Operation Freedom's Sentinel, which includes a "counterterrorism mission against the remnants of Al-Qaeda to ensure that Afghanistan is never again used to stage attacks against our homeland." U.S. Dep't of Defense, *Obama, Hagel Mark End of Operation Enduring Freedom* (Dec. 28, 2014), available at http://www.defense.gov/News/Article/Article/603860. Actions against al Qaeda militants in Afghanistan continue today. *See* "Al-Qaeda Leader Killed in Drone Strike in Afghanistan", *BBC News* (5 Nov. 2016).

12 "Al-Qaeda Number Three "Killed by CIA Spy Plane" in Pakistan", *The Telegraph*, 4 Dec. 2005, available at http://www.telegraph.co.uk/news/worldnews/asia/pakistan/1504718/Al-Qaeda-number-three-killed-by-CIA-spy-plane-in-Pakistan.html; "Top al-Qaeda Commander Killed", *BBC.Com* (1 Feb. 2008), available at http://news.bbc.co.uk/2/hi/south_asia/7220823.stm; E. Schmitt, "2 Qaeda Leaders Killed in Drone Strike in Pakistan", *N. Y. Times*, (8 Jan. 2009), available at http://www.nytimes.com/2009/01/09/world/asia/09pstan.html.

13 "Sources: U.S. Kills Cole Suspect", *CNN.com/WORLD* (5 Nov. 2002), available at http://archives.cnn.com/2002/WORLD/meast/11/04/yemen.blast/index.html.

14 *See, e.g.*, "US 'Targets al-Qaeda' in Somalia", *BBC News* (9 Jan. 2007), available at http://news.bbc.co.uk/2/hi/africa/6245943.stm ("White House spokesman Tony Snow said the U.S. action was a reminder that there was no safe haven for Islamic militants. 'This administration continues to go after al-Qaeda.'"); J. Gettleman & E. Schmitt, "U.S. Kills Top Qaeda Militant in Southern Somalia", *N. Y. Times* (14 Sept. 2009), available at http://www.nytimes.com/2009/09/15 /world/africa/15raid.html; *see also* J. Gettleman & E. Schmitt, "U.S. Forces Fire Missiles Into Somalia at a Kenyan", *N.Y.Times* (4 Mar. 2008), available at http://www.nytimes.com/2008/03/04/world/africa/04somalia.html (detailing an unsuccessful missile strike aimed at Nabhan launched from Kenya into Somalia).

15 B. Roggio, "AQAP Confirms Death of 2 Commanders in US Airstrike", *Long War Jour*. (21 July 2011), available at http://www.longwarjournal.org/archives/2011/07/aqap_confirms_2_comm.php; B. Roggio, "US Airstrikes in Southern Yemen Kill 30 AQAP Fighters: Report", *Long War Jour*. (1 Sept. 2011), available at http://www.longwarjournal.org/archives/2011/09/us_airstrikes_in_sou.php; E. Schmitt, "U.S. Drones and Yemeni Forces Kill Qaeda-Linked Fighters, Officials Say", *N. Y. Times* (21 Apr. 2014), available at https://www.nytimes.com/2014/04/22/world/middleeast/us-

has used lethal force against al-Shabaab in Somalia[16] and other militant groups inspired by or affiliated with al Qaeda.[17] More recently, the United States has used force in self-defence against al Qaeda operatives in Syria,[18] including the splinter Khorasan group,[19] and began military operations against the Islamic State of Iraq and Syria (ISIS) in Iraq in June 2014 and in Syria in September 2014.[20]

---

drones-and-yemeni-forces-kill-qaeda-linked-fighters-officials-say.html?_r=0; K. Samolsky, "U.S. Drone Strike May Suggest New Strategy to Combat Terrorism", *Center for Secur. Pol'y* (23 Mar. 2016), available at http://www.centerforsecuritypolicy.org/2016/03/23/u-s-drone-strike-may-suggest-new-strategy-to-combat-terrorism/.

16 P. Stewart, "U.S. Strikes al-Shabaab Training Camp in Somalia, More Than 150 Killed", *Reuters* (8 Mar. 2016), available at http://www.reuters.com/article/us-usa-somalia-dronestrike-idUSKCN0W91XW; L. C. Baldor, "U.S. Drone Strike Targets Al-Shabab Commander in Somalia", *Military.com* (1 June 2016), available at http://www.military.com/daily-news/2016/06/01/us-drone-strike-targets-al-shabab-commander-somalia.html; Reuters, "Leader of Al-Shabab is Killed in U.S. Drone Strike in Somalia . . . As Experts Warn the Group May Now Join Forces with ISIS", *Daily Mail* (5 Sept. 2014), available at http://www.dailymail.co.uk/news/article-2745255/U-S-confirms-death-al-Shabaab-leader-Godane-Somalia-air-strike.html.

17 For example, on 15 June 2015, a U.S. air strike killed Mokhtar Belmokhtar, formerly a senior figure in al Qaeda in the Islamic Maghreb (AQIM) and by then the leader of al-Murabitoun, an al-Qaeda-associated organization in north-west Africa and "a threat to Western interests." "Mokhtar Belmokhtar: Top Islamist "Killed" in US Strike", *BBC News* (June 15, 2015), available at http://www.bbc.com/news/world-us-canada-33129838.

18 "The White House, Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations" 17 (Dec. 2016) (hereinafter "Legal and Policy Frameworks"), available at https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Legal_Policy_Report.pdf (providing the Obama Administration's view that the United States' collective right to self-defence justifies Syrian airstrikes under international law).

19 J. E. Barnes & S. Dagher, "Syria Strikes: U.S. Reports Significant Damage in Attacks on Islamic States, Khorasan", *Wall St. J.* (Sept. 24, 2014), available at http://www.wsj.com/articles/syria-strikes-u-s-reports-significant-damage-in-attacks-on-islamic-state-khorasan-1411486035; "U.S. Bombs ISIS Sites in Syria and Targets Khorasan Group", *NBC News* (Sept. 23, 2014), available at http://www.nbcnews.com/storyline/isis-terror/u-s-bombs-isis-sites-syria-targets-khorasan-group-n209421 (reporting that the U.S. "mounted eight separate strikes overnight 'to disrupt the imminent attack plotting against the United States and Western interests conducted by a network of seasoned al Qaeda veterans,' also known as 'the Khorasan group.'); Letter, dated 23 Sept. 2014, from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, U.N. Doc. S/2014/695, 23 Sept. 2014 ("In addition, the United States has initiated military actions in Syria against al-Qaida elements in Syria known as the Khorasan Group to address terrorist threats that they pose to the United States and our partners and allies").

20 *See* Letter from Hoshyar Zebari, Minister for Foreign Affairs of the Republic of Iraq, to the Secretary General of the United Nations, S/2014/440, June 25, 2014; Letter from Ibrahim al-Ushayqir al-Ja'fari, Minister for Foreign Affairs of Iraq, to the Secretary General of the United Nations, S/2014/691, Sept. 22, 2014; Letter dated 23 Sept. 2014

Throughout the past fifteen-plus years since the 9/11 attacks, the United States has relied on self-defence as the overarching justification for military action against these various terrorist groups, alongside the broad assertion of an armed conflict against al Qaeda and associated forces. Notably, even when reporting on strikes against al Qaeda operatives, which would ostensibly fall squarely within this armed conflict paradigm, the United States has typically asserted both an armed conflict and a self-defence justification for such strikes and for operations against al Qaeda generally. For example, the U.S. State Department Legal Advisor explained in a well-known speech in 2010 that the United States uses force against al Qaeda either because it "is engaged in an armed conflict or in legitimate self-defence."[21] Similarly, in a brief submitted to the U.S. District Court for the District of Columbia, the Government asserted that it had legal authority to target Anwar al-Awlaki either in the context of the armed conflict with al Qaeda and associated forces as authorized in the 2001 Authorization to Use Military Force (AUMF) or under "the inherent right to national self-defence recognized in international law."[22] And, as noted above, the *raison d'être* for the armed conflict with al Qaeda is, of course, self-defence. As the United States has extended its self-defence campaign for over fifteen years, across at least seven countries, and against multiple terrorist groups — most of which did not exist at the time of the initial response to the 9/11 attacks, the question of how far self-defence extends becomes increasingly relevant and challenging.

B. The International Law of Self-Defence: Jus ad Bellum Basics

Jus ad bellum is the Latin term for the law governing the resort to force, that is when a State may use force within the constraints of the United Nations Charter framework and traditional legal principles. Modern *jus ad bellum* has its origins in the 1919 Covenant of the League of Nations, the

---

from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, U.N. Doc. S/2014/695, 23 Sept. 2014.

21 Harold Koh, Legal Adviser, U.S. Dep't of State, Address at Annual Meeting of American Society of International Law (Mar. 25, 2010), available at https://www.state.gov/s/l/releases/remarks/139119.htm. *See also* Attorney General Holder's Speech on Targeted Killing, Mar. 2012, Northwestern Law School, 5 Mar. 2012, available at http://www.cfr.org/terrorism-and-the-law/attorney-general-holders-speech-targeted-killing-march-2012/p27562 ("Because the United States is in an armed conflict, we are authorized to take action against enemy belligerents under international law. . . And international law recognizes the inherent right of national self-defense.").

22 *Al-Aulaqi v. Obama*, 727 F. Supp. 2d 1 (D.D.C. 2010) (Opposition to Plaintiff's Motion for Preliminary Injunction & Memorandum in Support of Defendants' Motion to Dismiss at 4–5, (No.10-cv-1469(JDB), 2010 WL 3863135).

1928 Kellogg-Briand Pact, and the United Nations Charter.[23] In particular, the United Nations Charter prohibits the use of force by one State against another in Article 2(4): "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[24] This article, in many ways, is the foundation of the U.N.'s goal of "sav[ing] succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind,"[25] through severe restrictions and prohibitions on the use of force.

International law provides only three justifications that rebut this presumption against the use of force; therefore, any use of force not falling within one of these three justifications violates Article 2(4) and the fundamental prohibition of the use of force across State boundaries. These exceptions to the prohibition on the use of force balance two key international law principles: respect for state sovereignty and the collective interests of the international community, including the right to use force in self-defence. Thus, a State's sovereignty and territorial integrity is foundational to international law and the international system. At the same time, however, States have an inherent right to protect their territory, nationals and interests from attack.

The first exception is customary in nature: a State may use force in the territory of another state with the consent of that State. For example, a State engaged in an internal conflict with a rebel group may seek assistance from other States in defeating the rebels and restoring order and security. For example, NATO operations in Afghanistan through the International Security Assistance Force (ISAF) fall within this category of consent,[26] as do individual interventions like the U.S. role in support of the Republic of Vietnam.[27] In a different variation, a State may also consent to another State using force in counterterrorism operations, such as Yemen's consent to United States drone strikes against al Qaeda and AQAP operatives in that country.[28] In such cases, however, the territorial State can only consent to

23 M. N. Shaw, *International Law*, 780–81 (4th ed. 1997).
24 U.N. Charter, art. 2, para. 4.
25 *Id*. (preamble)
26 Koh Address, *supra* note 21 ("[I]n Afghanistan, we work as partners with a consenting host government.").
27 B. K. Landsberg, "The United States in Vietnam: A Case Study in the Law of Intervention", 50 *Cal. L. Rev*. 515, 523 (1962).
28 G. Miller, "Yemeni President Acknowledges Approving U.S. Drone Strikes", *Wash. Post* (Sept. 29, 2012), available at https://www.washingtonpost.com/world/national-security/yemeni-president-acknowledges-approving-us-dronestrikes/2012/09/29/09bec2ae-0a56-11e2-afffd6c7f20a83bf_story.html?utm_term=. f024b7926a13.

such assistance and uses of force in which it could legally engage — no State can consent to actions by another State that would violate international law if undertaken on its own. This means that the intervening State may not use the request as the means for engaging in an act of aggression against a neighboring State.

The United Nations Charter provides the second and third exceptions to the prohibition on the use of force: the multinational use of force authorized by the Security Council under Chapter VII in Article 42, and the inherent right of self-defence in response to an armed attack under Article 51. Article 42 authorizes the Security Council to "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security . . . [including] operations by air, sea, or land forces of Members of the United Nations."[29] The multinational military operation to protect civilians in Libya in the spring and summer of 2011 is an example of the Security Council authorizing the use of force in accordance with Article 42.

Self-defence, the most commonly relied upon justification for the use of force, builds on and establishes the basic framework of *jus ad bellum*. States may use force as an act of individual or collective self-defence in response to an armed attack in accordance with Article 51 of the United Nations Charter. Article 51 states:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.[30]

This provision recognizes the pre-existing right of States to use force — and to use force in response to another State's request for assistance — in self-defence against an attack.

The prerequisite for any use of force in self-defence is the existence of an armed attack. Note that an armed attack is more severe and significant than a use of force, meaning that a State can be the victim of a use of force without being the victim of an armed attack that triggers the right of self-defence. Although the United Nations Charter does not define "armed attack," customary international law and, in particular, the jurisprudence of the

29 U.N. Charter, art. 42.
30 *Id*., art 51.

International Court of Justice (ICJ) focuses on the "scale and effects"[31] of any particular hostile action directed at a State to determine whether it rises to the level of an armed attack. For example, the deployment of a State's regular armed forces across a border will generally constitute an armed attack, as will a State's sending irregular militias or other armed groups to accomplish the same purposes. In contrast, providing assistance, such as weapons or other support, to rebels or other armed groups across State borders will not reach the threshold of an armed attack.[32]

Directly related to the analysis of self-defence against attacks by terrorist groups or other non-State actors, is a key *jus ad bellum* question whether only States can launch an armed attack. Nothing in Article 51 specifies that the right of self-defence is only available in response to a threat or use of force by another State. Nonetheless, the precise contours of what type of actor can trigger the right of self-defence remains controversial. Some argue that only States can be the source of an armed attack — or imminent threat of an armed attack — that can justify the use of force in self-defence.[33] The ICJ has continued to limit the right in this manner in a series of cases.[34] However, State practice in the aftermath of the 9/11 attacks provides firm support for the existence of a right of self-defence against non-State actors, even if unrelated to any State.[35] Indeed, the *Caroline* incident, which forms

31 Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. US*), I.C.J. Reports 1986, 14, ¶ 195.

32 *Id.*, ¶ 191.

33 *See, e.g.*, A. Cassese, "The International Community's "Legal" Response to Terrorism", 38 *Int'l & Comp. L. Q.* 589, 597 (1989); E. Myjer & N. White, "The Twin Towers Attack: An Unlimited Right to Self-Defense", 7 *J. Conflict & Sec. L.* 5, 7 (2002) ("Self-defense, traditionally speaking, applies to an armed response to an attack by a state.").

34 *See, e.g.,* Military and Paramilitary Activities, *supra* note 31; Oil Platforms (*Iran v. U.S.*), I.C.J. Reports 2003, 161; Armed Activities on the Territory of the Congo (*Dem. Rep. Congo v. Uganda*), I.C.J. Reports 2005, 168; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, 136, 215.

35 *See, e.g.,* Y. Dinstein, *War, Aggression and Self-Defence,* 224-30 (5th ed. 2011); C. Greenwood, "International Law and the Preemptive Use of Force: Afghanistan, al Qaeda, and Iraq", 4 *S. D. Int'l L. J.* 7, 17 (2003) (discussing the effects of attacks made by non-State actors); S. D. Murphy, "The International Legality of US Military Cross-Border Operations from Afghanistan into Pakistan", *in The War in Afghanistan: A Legal Analysis* 109, 126 (M. N. Schmitt ed., 2009) (Vol. 85, U.S. Naval War College Int'l Law Studies) ("While this area of the law remains somewhat uncertain, the dominant trend in contemporary interstate relations seems to favor the view that States accept or at least tolerate acts of self-defense against a non-State actor."); R. van Steenberghe, "Self-Defence in Response to Attacks by Non-state Actors in the Light of Recent State Practice: A Step Forward?", 23 *Leiden J. Int'l L.* 183, 184 (2010) (concluding

the historical foundation of the right to self- defence, involved an armed attack by non-State actors. United Nations Security Council Resolution 1368, for example, recognized the inherent right of individual and collective self-defence against the September 11th attacks[36] and the North Atlantic Council activated the collective self-defence provision in Article 5 of the North Atlantic Treaty for the first time in its history.[37] Several other States have asserted the same right, including Turkey, Israel, Colombia, and Russia, for example.[38] Over the past decade, the challenge of responding to transnational terrorism has helped drive State practice and debate regarding the lawfulness of self-defence in response to armed attacks by non-State actors. Although the question of when and whether terrorist acts constitute armed attacks is essential to the analysis of self-defence against such groups, the instant discussion focuses on the extent of self-defence once the right to use force in self-defence has been triggered, and therefore further examination of the initial question of what constitutes an armed attack is outside the scope of this article.

Once an armed attack triggers a State's right to use force in self-defence, that use of force must comply with three requirements derived from the *Caroline* incident in the nineteenth century: necessity, proportionality and immediacy. In the *Caroline* incident, British troops crossed the Niagara River to the United States side and attacked the steamer *Caroline*, which had been running arms and materiel to insurgents on the Canadian side.[39] The attack set fire to the *Caroline* and killed one American. The British claimed that they were acting in self-defence in response to the insurgents' provocations.[40] In a letter to Lord Ashburton, his British counterpart, U.S. Secretary of State Daniel Webster declared that the use of force in self-defence should be limited to "cases in which the necessity of that self-defence is instant, over-whelming, and leaving no choice of means, and no

---

that recent State practice suggests that attacks committed by non-State actors alone constitute armed attacks under Article 51).

36 S.C. Res. 1368, ¶ 1, U.N. Doc. S/RES/1368 (Sept. 12, 2001) (emphasis added).

37 North Atlantic Treaty, art. 5, Apr. 4, 1949, 34 *U.N.T.S.* 243, 246; Press Release, NATO, Statement by the North Atlantic Council (Sept. 12, 2001).

38 For an extensive treatment and discussion of the use of force in self-defense and the unwilling or unable test with regard to state consent to the use of force, *see* A. S. Deeks, ""Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense", 52 *Va. J. Int'l L.* 483 (2012).

39 H. Miller, "British-American Diplomacy: The Caroline Case", *The Avalon Project*, available at http://avalon.law.yale.edu/19th_century/br-1842d.asp.

40 *Id.* ("[T]he destruction of the Caroline was an act of necessary self-defense." (quoting a letter from Mr. Fox, the British minister at Washington, to Mr. Forsyth, U.S. Secretary of State)).

moment for deliberation."[41] Furthermore, the force used must not be "unreasonable or excessive; since the act, justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it."[42] As a result, the central features of the right to self-defence, reaffirmed repeatedly by the ICJ and other courts, are that the force used is necessary and proportionate to the goal of repelling the attack or ending the grievance.[43]

The requirements of necessity and proportionality are the essential ingredients for the analysis here of how long, how far, and for what purposes self-defence can be used. Parts II and III examine how necessity and proportionality match with the operational goals that States seek to achieve in combatting terrorist groups and explore how our understanding of necessity and proportionality does or should change over time and in response to changing facts and circumstances. A preliminary discussion here of both requirements and the particularities of their application in the counterterrorism context provides useful foundation and context for the more in-depth analysis below. The third criterion of immediacy, which imposes a temporal limitation on the resort to self-defence, does not affect the extent of self-defence but rather highlights on the question of when the right to self-defence matures — in the case of an imminent attack — and how soon after an attack the victim State must act.[44]

1) Necessity

Overall, the requirements of necessity and proportionality focus on whether the defensive act is appropriate in relation to the ends sought. Necessity addresses whether there are adequate non-forceful options to deter or defeat the attack, such as diplomatic avenues, defensive measures to halt any further attacks or reparations for injuries caused. To this end, "acts done in self-defence must not exceed in manner or aim the necessity provoking them."[45] The *Caroline* formula of "no choice of means" guides the application of necessity with an underlying goal of minimizing or prohibiting the resort to force except in situations where it is unavoidable to

41 Letter from Daniel Webster, U.S. Secretary of State, to Lord Ashburton, Special British Minister (Aug. 6, 1842), *reprinted in* 2 *J. Moore, Dig. of Int'l Law* sec. 217 at 409 (1906).

42 *Id*.

43 Legality of the Threat and Use of Nuclear Weapons in Armed Conflict, Advisory Opinion, I.C.J. Reports 1996, 226, 245 (hereinafter Nuclear Weapons); Military and Paramilitary Activities, *supra* note 31, para. 237; Oil Platforms *supra* note 34, paras. 43, 73-74, 76; Jus ad Bellum (*Ethiopia v. Eritrea*), Ethiopia's Claims 1–8, Partial Award (Dec. 19, 2005), available at http://www.pca-cpa.org.

44 *See* Schmitt, *supra* note 8 at 63-66.

45 O. Schachter, "In Defense of International Rules on the Use of Force", 53 *U. Chi. L. Rev.* 113, 132 (1986).

protect the State's essential interests, such as sovereignty, territorial integrity, and nationals. If a State has an alternative to force available to it, *i.e.*, if it had been able "to achieve the same result by measures not involving the use of armed force, it would have no justification for adopting conduct which contravened the general prohibition against the use of armed force."[46] Necessity thus operates to enforce the ban on using force.

Crucially, however, necessity centers on the absence of reasonable alternatives, and thus "does not require victim States to exhaust *all* non-forcible responses before resorting to self-defence, but only those that are likely to be effective."[47] Thus, for example, as the then-United States State Department Legal Advisor explained with respect to the United States' exercise of self-defence in 2001,

> if [the United States] did not have the right to use force against al Qaida and the Taliban, then we would have had no acceptable way to defend our citizens after the most devastating attack against the United States in history. Given the Taliban's unwillingness to cooperate with the international community to bring the perpetrators of the September 11th attack to justice, it cannot reasonably be argued that the only recourse the United States had was to file diplomatic protests or extradition requests with Mullah Omar.[48]

Similarly, the fact that an extensive law enforcement operation was underway against al Qaeda after 9/11 did not affirmatively rule out the use of force in self-defence. Notwithstanding "the most intensive international law enforcement operations in history, . . . al Qaeda remained active, launching numerous spectacular attacks in the wake of 9/11."[49] The United States' use of force thus clearly met the necessity criterion.

In the case of attacks by non-State actors, States seeking to act in self-defence must first explore whether the territorial State can take action to stop the non-State actors from launching further attacks, including, potentially, detention of those responsible, as part of determining whether there are any

46 R. Ago, "Addendum to Eighth Report on State Responsibility", 2 *Y.B. Int'l L. Comm'n,* 13 para. 120 (1980), U.N. Doc. A/CN.4/318/ADD.5-7.

47 Tams & Devaney, *supra* note 5 at 96.

48 J. B. Bellinger III, *Legal Issues in the War on Terrorism* (2006). The justification for the use of force against the Taliban rests on shakier footing given the lack of evidence that al Qaeda's attack could be attributed to the Taliban. Lubell, *supra* note 2, at 47-48.

49 Schmitt, *supra* note 8 at 63.

non-forceful alternatives available. Unlike the State-on-State context, when self-defence is contemplated against a non-State group, there are two States with potential capability to respond to the terrorist attack or threat: the victim State and the host State. To the extent they are effective, non-forceful repressive measures by the host State are the preferred response in comparison to the victim State's extraterritorial use of force, simply due to the international system's fundamental distaste for the use of force. Therefore, "for self-defence to be considered necessary [against a non-State group], the victim State has to make an attempt to have the host State suppress the terrorist threat[,] attempt to cooperate with the host state against terrorists . . ., or seek the host State's consent to extraterritorial anti-terrorist measures."[50] To target a terrorist operative in self-defence, the State must have "credible evidence that the targeted persons are actively involved in planning or preparing further terrorist attacks against the victim State and no other operational means of stopping those attacks are available."[51] Particularly with regard to terrorist groups, the intransigence of the group and the practice of seeking operational space and safe haven in remote areas with little, if any, effective government authority will often mean that the necessity criterion will be satisfied for a state seeking to respond in self-defence to an armed attack or imminent armed attack.

2) Proportionality

The requirement of proportionality measures the extent of the use of force against the overall military goals, such as fending off an attack or subordinating the enemy. Rather than addressing whether force may be used at all — which is the main focus of the necessity requirement — proportionality looks at how much force may be used. The underlying goal is "the minimization of the disruption of international peace and security."[52] Historically, scholars have presented numerous formulas or descriptions of

50 Tams & Devaney, *supra* note 5 at 98; *see also* Dinstein, *supra* note 35 at 275 ("It must be clearly demonstrated by Utopia that the attacks by the organized armed group or terrorists cannot be defeated through recourse to alternative measures that are less intrusive in their effects on the territorial sovereignty of Arcadia.").

51 D. Kretzmer, "Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?", 16 *Eur. J. Int'l L.* 171, 203 (2005). *See also* M. N. Schmitt, "Counter-Terrorism and the Use of Force in International Law" 5 Marshall Center Papers 20 (2002), available at http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/mcPapers/mc-paper_5-en.pdf. ("Similarly, if a State in which the terrorists are located conducts military operations with a high probability of success, there would be no necessity basis for self-defense by the victim State.").

52 C. Greenwood, "Self-Defence and the Conduct of International Armed Conflict", in *International Law at a Time of Perplexity: Essays in Honor of Shabtai Rosenne*, 273, 278 (Y. Dinstein ed., 1989).

proportionality in *jus ad bellum*, including the idea that the response must be proportionate to the danger posed,[53] that the force used must be "what is required for achieving the object,"[54] or that the self-defence action "is proportionate, in nature and degree, to the prior illegality or the imminent attack."[55] Ultimately, proportionality focuses not on some measure of symmetry between the original attack and the use of force in response, but on whether the measure of counterforce used is proportionate to the needs and goals of *repelling* or *deterring* the original attack.[56]

Israel's response to Hezbollah's cross border raid in July 2006 highlights this focus on the objective of stopping the attack and further attacks rather than the nature of the original attack. Once Hezbollah had captured the Israeli soldiers, Israel needed to take action to recover the hostages, including by preventing their movement deeper into Lebanon, and to stop Hezbollah's rocket attacks on northern Israel. In the end, "[a]lthough the IDF response exceeded the scope and scale of the Hezbollah kidnappings and rocket attacks manyfold, the only way effectively to have prevented movement of the hostages was to either destroy or control lines of communication [and] the best tactic for preventing Hezbollah rocket attacks, especially from mobile launchers, was through control of the territory from which they were being launched."[57] In assessing proportionality, therefore, the force used may indeed be significantly greater than that used in the attack that triggered the right to self-defence — what matters is the result sought, not the equivalence between attack and response. As a report to the International Law Commission explains,

> it would be mistaken . . . to think that there must be proportionality between the conduct constituting the armed attack and the opposing conduct. The action needed to halt and repulse the attack may well have to

53 D. Bowett, *Self-Defence in International Law,* 269 (1958).

54 H. Waldock, "The Regulation of the Use of Force by Individual States in International Law", 81 *Receuil des Cours* 455, 463-64 (1952).

55 R. Higgins, *The Development of International Law Through the Political Organs of the United Nations* 201 (1963).

56 Dinstein, *supra* note 35, at 275.

57 M. N. Schmitt, "Change Direction‖ 2006: Israeli Operations in Lebanon and the International Law of Self-Defense", 29 *Mich. J. Int'l L.* 127, 153 (2007–2008). Although Israel's operations against Hezbollah in 2006 engendered significant international criticism, including on the question of proportionality, the predominant issue was extension of military operations to infrastructure beyond southern Lebanon, including the roads and airfields in and around Beirut, and the air and sea blockade of southern Lebanon, which were seen as extending beyond that which was needed to respond effectively to the attack. *Id*. at 154–55.

> assume dimensions disproportionate to those of the attack suffered. What matters in this respect is the result to be achieved by the "defensive action" and not the forms, substance and strength of the action itself.[58]

One question that arises in the context of self-defence against terrorist groups is whether the geographical location of attacks and the force used in response has any bearing on the proportionality analysis. Historically, some have argued that any force in self-defence must be limited to the area of the attack they seek to repel, and that, as a result, any coercive action that occurs far from the initial attack is likely to constitute a disproportionate use of force.[59] The notion of geography ultimately serves merely as a proxy for examining the objective of the victim State in using force. The issue is whether self-defence actions at the location of the attack can accomplish the goal of repelling or deterring the attack, or whether action against the attacker beyond that immediate locale is necessary. For example, in the 1990-1991 Persian Gulf conflict, the United States and its coalition partners "took the view that tactically, in light of Iraq's military capability, the response could not be restricted to Kuwaiti territory"[60] and therefore attacking targets in Iraq was not disproportionate. In contrast, the ICJ in *Armed Activities on the Territory of the Congo* held that Uganda's extensive and extended forays into Congolese territory exceeded the limits of the proportionality requirement, because Ugandan operations capturing "airports and towns many hundreds of kilometres from Uganda's border would not seem proportionate to the series of transborder attacks it claimed had given rise to the right of self-defence."[61] However, it was not the fact of

58 Ago, *supra* note 46 at 69. *See also* J. G. Gardam, *Necessity, Proportionality and the Use of Force by States*, 160-161 (2004) ("an assessment of what will achieve the end result of self-defence, 'that of halting and repelling the attack', consists neither merely of a comparison of weapons or the scale of force used nor, as Ago puts it, 'the forms, substance and strength of the action itself'. Indeed, the action needed to halt and repulse an attack may well have to assume dimensions that would be disproportionate using such a comparison").

59 Greenwood, *supra* note 52 at 277. *See also* S. Etezazian, "Air Strikes in Syria—Questions Surrounding the Necessity and Proportionality Requirements in the Exercise of Self-Defense", *OpinioJuris*, (14 October 2015), available at http://opiniojuris.org/2015/10/14/guest-post-air-strikes-in-syria-questions-surrounding-the-necessity-and-proportionality-requirements-in-the-exercise-of-self-defense/.

60 Gardam, *supra* note 58 at 164.

61 Armed Activities on the Territory of the Congo *supra* note 34, para. 147. *See also* Military and Paramilitary Activities, *supra* note 31, para. 237; Gardam, *supra* note 58 at 158 (explaining that in the Nicaragua case, the Court held that "the approach is not to focus on the nature of the attack itself and ask what is a proportionate response but rather to determine what is proportionate to achieving the legitimate goal under the Charter, the repulsion of the attack").

geographical distance but rather the relationship between those extended operations and the legitimate self-defence objective of repelling the attack that drove the Court's analysis.

Terrorist attacks, of course, usually occur on the territory of the victim state while the action in response takes place where the terrorists or terrorist group has found safe haven, often halfway around the world. Al Qaeda's attacks or attempted attacks against the United States have predominantly been on United States territory or aircraft, such as the 9/11 attacks, the shoe-bomber, the underwear bomber, or the attempted bombing in Times Square in May 2010. The United States has launched military force in response where it finds al Qaeda operatives and facilities: Afghanistan, Pakistan, and Yemen, for example. The geography of self-defence does pose challenging questions for the extent of self-defence, as discussed in Part III.A, below. However, as an initial question of proportionality,

> recent practice suggests that geographical factors that may be considered relevant to the proportionality of inter-state self-defence are of limited relevance [in the terrorism context]: hence states hit by terrorist attacks on their home soil have asserted a right to respond against terrorists at their base — and even where their conduct was not generally accepted, this fact that the self-defence operation had carried the fight against terrorism into far-away, remote countries seemed to be a factor of limited relevance.[62]

Finally, and particularly relevant to counterterrorism operations, the necessity and proportionality criteria can account not only for action taken to halt and defeat an initial attack, but also for broader action to eliminate a continuing threat. In the State-on-State context, a victim State is not constrained to respond separately to each intrusion from the attacking State, but can respond appropriately where the only means available to end the attacks is a more comprehensive and large-scale response. With regard to the acceptable degree or amount of force, if "a [S]tate suffers a series of successful and different acts of armed attack from another [S]tate, the requirement of proportionality will certainly not mean that the victim [S]tate is not free to undertake a single armed action on a much larger scale in order to put an end to this escalating succession of attacks."[63] Terrorist groups rarely capture and hold territory — ISIS being the current exception of a terrorist group operating more akin to conventional forces in Iraq and

62 Tams & Devaney, *supra* note 5 at 104.
63 Ago, *supra* note 46, ¶ 121.

Syria.[64] Rather, they launch attacks, often dispersed by time and geographical distance, and a victim state's small-scale response to one such attack may not have any utility in stopping the attacks. As with any other armed attack and considered response in self-defence, the nature of the attacker, the attacks themselves, the effects on the victim State, and the anticipated effects, or lack thereof, of potential actions in response will all drive the necessity and proportionality analysis.

II. LEGITIMATE AIMS AND THE EXTENT OF SELF-DEFENCE

As the discussion of necessity and proportionality shows, any assessment of self-defence must start with the victim State's aim or objective in using force in response to the armed attack or imminent armed attack. Necessity focuses on whether force is the only means available to achieve that objective; proportionality looks to the relationship between the force used and the objective sought. Decision-makers in the victim State therefore "should ideally define the aims of [self-defence] force and assess the scope of the force and the means necessary to achieve those aims."[65] The terminology of *jus ad bellum* and self-defence comport with the basic concepts of a State's aggression and the victim State's response, including notions of "deterring" or "repelling" an attack. One can certainly envision one state's army massing at the border, invading the other State's territory, and then the victim State marshalling its forces to push the invading forces back across the border and to accomplish any further objectives necessary to ensure that the aggressor state does not continue the attack or try again. How we analogize this conventional image to the current environment of terrorist attacks, terrorist groups and State action in response and to preempt is much more complicated.

After a brief explication of the legitimate aims of self-defence, this Part explores two questions in depth with an eye to furthering our understanding of the extent of self-defence. The first sub-section seeks to match the operational goals of contemporary counterterrorism operations with the international law framework and terminology, to examine whether the framework of necessity and proportionality can help determine how far and

64 A. Kurth Cronin, "ISIS is Not A Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat", *For. Aff.* (Mar./Apr. 2015), available at https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group ("ISIS, on the other hand, boasts some 30,000 fighters holds territory in both Iraq and Syria, maintains extensive military capabilities, controls lines of communications, commands infrastructure, funds itself, and engages in sophisticated military operations.").

65 D. Kretzmer, "The Inherent Right to Self-Defence and Proportionality in *Jus Ad Bellum*", 24 *Eur. J. Int'l L.* 235, 267 (2013).

how long self-defence extends in such contexts. Second, the characterization of counterterrorism operations as armed conflict — such as the United States' campaign against al Qaeda — raises separate questions regarding the impact on self-defence, namely whether armed conflict paradigm expands the reach of self-defence to include complete defeat of the terrorist group or groups.

The fundamental premise of self-defence is that a State is not rendered helpless when faced with an attack, but rather can respond to protect its territory, sovereignty, nationals and interests. The most basic and widely-supported aim of self-defence, therefore, is to halt or repel an attack. "In the case of self-defence against an armed attack that has already occurred, it is the repulsing of the attack giving rise to the right that is the criterion against which the response is measured."[66] If, for example, one State attacks another, repelling the attack would naturally include military operations not only to halt the aggressor, but also to push it back across the border. The challenge in the terrorism context is that attacks tend to be singular events causing mass civilian casualties rather than military operations to gain territory or achieve other conventional strategic objectives, such that the very idea of halting or repelling an attack does not translate well into the counterterrorism scenario.

Where the armed attack is imminent but has not yet occurred, there is general acceptance — with significant disagreement about what specifically constitutes an imminent attack and when the right of self-defence is triggered in such situations — that a State may act in anticipatory self-defence to prevent an attack from occurring. Prevention of imminent attacks is a common theme of strikes against terrorists and terrorist groups, such as the United States strikes against the Khorasan Group in Syria in 2014, a group that had not launched any attacks against the United States at the time but was believed to be actively planning attacks.[67] One useful description of when the use of force in self-defence is acceptable against terrorist groups to prevent anticipated attacks is the idea of the "last window of opportunity." Given that a terrorist group may put an attack in operation well in advance and then "go underground" to avoid detection before the attack, a State may have its only opportunity to prevent the attack and defend itself when it can find the terrorist operatives, even if that opportunity is long before the attack ultimately takes place. Accordingly, "self-defence against terrorists is appropriate and lawful when a terrorist group harbors both the intent and

66 Gardam, *supra* note 58 at 156.

67 R. Kaplan, "Khorasan Was 'Nearing the Execution Phase of an Attack': Pentagon", *CBS News* (23 Sept. 2014), available at http://www.cbsnews.com/news/khorasan-was-nearing-the-execution-phase-of-an-attack-pentagon/.

means to carry out attacks, there is no effective alternative for preventing them, and the State must act now or risk missing the opportunity to thwart the attacks."[68] The United States government takes this approach, arguing that a rule forcing a State to wait until specific preparations are concluded and the attack is temporally imminent is impractical and operationally not feasible in the counterterrorism context. The very nature of al Qaeda and other terrorist groups is such that "defensive options available to the United States may be reduced or eliminated if al-Qa'ida operatives disappear and cannot be found when the time of their attack approaches."[69]

Even in the State-on-State context, however, it is unclear to what extent self-defence allows a State to use force to go beyond merely repelling the attack and to also prevent further attacks in the future. More conservative theorists resist this more comprehensive view of self-defence, positing that any use of force "must necessarily be commensurate with the concrete need to repel the current attack, and not with the need to produce the level of security sought by the attacked State."[70] However, this limited concept of the legitimate aims of self-defence does not comport with the realities of the international system, where the United Nations Security Council is often not effective at maintaining international peace and security, or provide sufficient protection for victim states if an aggressor state faces no consequences beyond a repulsed attack. These disconnects are only magnified in the case of terrorist attacks, where the terrorist attackers either escape before the attack or die in the course of the attack and the leaders are far from the point of attack at all times, so there is no one for the state to repel at the moment of attack. For these reasons, States responding to attacks that have been completed will commonly point to the need to defend against future attacks and future threats, even if undefined, in justifying action in self-defence. President Clinton presented this argument in announcing U.S. strikes in response to the 1998 Embassy bombings. After explaining that law enforcement and diplomatic tools were not sufficient to protect U.S. national security, he stated that "[w]ith compelling evidence that

68 Schmitt, *supra* note 8 at 66. *See also* M. N. Schmitt, "Preemptive Strategies in International Law", 24 *Mich. J. Int'l L.* 513, 535 (2003).

69 "Dep't of Justice, White Paper: Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who is a Senior Operational Leader of Al-Qa'ida or an Associated Force 7" (8 Nov. 2011), available at http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf.

70 E. Cannizzaro, "Contextualizing Proportionality: Jus ad Bellum and Jus in Bello in the Lebanese War", 88 *Int'l Rev. Red Cross* 779, 785 (2006) (arguing that "the forcible removal of threatening situations and the creation of permanent conditions of security seem to have been reserved by the international community as tasks to be performed collectively"). *See also* A. Cassese, *International Law* 355 (2d ed. 2005) ("self-defence must limit itself to rejecting the armed attack; it must not go beyond this purpose").

the bin Ladin network of terrorist groups was planning to mount further attacks against Americans and other freedom-loving people, I decided America must act."[71]

The precise parameters of such action remain uncertain, however, leaving open key questions about whether and to what extent a State can take action to destroy the attacking entity as a way to prevent future attacks or whether proportionality precludes action to remove a continuing threat, beyond that needed to prevent an immediate future attack. In effect, the issue is twofold. First, if halting or repelling the attack is a legitimate objective, "is it proportionate to take action that is designed to prevent such an attack occurring again and restore the security of the State,"[72] including the total defeat of the attacking entity's forces if necessary? This approach looks at the broader range of action to defeat the enemy not as a more robust objective of self-defence, but as a question of proportionality and how elastic the degree of force allowed can be for achieving the more conservative objective of halting or repelling. Alternatively, the second possibility is to ask whether the destruction of the attacking force's capability is a legitimate objective of force in self-defence. An evolution in thinking about how terrorist groups operate offers support for this approach. There is a growing recognition that rather than looking at each terrorist attack or potential attack as an armed attack in isolation, and examining the necessity, proportionality and immediacy criteria for each such attack separately, terrorist groups now should be "viewed as conducting campaigns."[73] Thus, "once it is established that an ongoing campaign is underway, acts of self-defence are acceptable throughout its course, so long as the purpose is actually to defeat the campaign."[74] If so, the proportionality inquiry and analysis would be based on that objective in assessing the amount of force appropriate to achieving the goal of self-defence.

Assessing the extent of self-defence is difficult in the face of vague or shifting objectives for the use of force in self-defence. Both necessity and proportionality depend, fundamentally, on the objective of the self-defence, and both effectively determine how extensive or constrained the use of force

71 W. J. Clinton, Address to the Nation on Military Action against Terrorist Sites in Afghanistan and Sudan, (20 Aug. 1998), available at https://www.gpo.gov/fdsys/pkg/WCPD-1998-08-24/pdf/WCPD-1998-08-24-Pg1642.pdf. Indeed, the requirement of necessity suggests that "there must be a sound basis for believing that further attacks will be mounted and that the use of armed forces is needed to counter them." Schmitt, *supra* note 51 at 64.

72 Gardam, *supra* note 58 at 165.

73 Schmitt, *supra* note 51 at 66.

74 *Id*.

can or must be in any given situation. One international scholar summarized the difficulties of analysis and interpretation thus:

> For example, where a [S]tate is faced with an ongoing pattern of attacks by a non[-S]tate group acting from a territory across its border, the [S]tate is entitled to take defensive action, but with what objective? Is the [S]tate only entitled to act to stop the threat of immediate future attacks, or may it take action to prevent these attacks over the long run? The answer to that question will determine whether, for example, the [S]tate is only entitled to go across the border to destroy rocket launchers used to initiate the attacks, to destroy the base where the non[-S]tate groups are camped, or, instead, to seek to change the government of the host state to prevent the territory from being used for future attacks.[75]

These questions and other related questions present even more complex challenges when the non-State group is a transnational terrorist group without a fixed territorial home base, or any other group operating in a manner that similarly negates the effectiveness of the victim state using force to clear and hold territory and to disabuse the group from further attacks through the direct application of force. The following two sub-sections examine these questions thoroughly by looking at whether and how the stated operational goals of current and recent counterterrorism operations comport with or perhaps even illuminate the necessity and proportionality analysis.

A. Matching Operational Goals and the International Legal Framework

Preventing future attacks is the common underlying theme or goal when States use force against terrorist groups. Indeed, the very nature of terrorist attacks as singular attacks on civilian sites or events, where the attackers are far away or die as planned in the attack, renders it improbable, if not impossible, for a State to repel an attack while it is underway. But preventing future attacks is a remarkably elastic concept, particularly in the contemporary world where the ease of movement across borders and communication makes it possible for terrorist groups to strike at targets notwithstanding extraordinary distance from their seeming base of operations. As a result, the *justification* of preventing future attacks does not

[75] D. Akande, "Note and Comment: Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense", 107 *Am. J. Int'l L.* 563, 569 (2013).

necessarily provide any useful guidance on understanding the extent to which a State may act in self-defence, because the justification stems from the existence of the armed attack or imminent armed attack as the trigger for the right to act in self-defence. Rather, necessity and proportionality, which determine how much force a state can use, depend on the *goal* of acting in self-defence, the objective the state seeks to achieve. In the absence of clear parameters for the appropriate objectives for self-defence action, a look at the stated operational and strategic goals States have declared in using force in self-defence against terrorist groups can help advance our analysis of the extent of self-defence.

1) What States Seek to Achieve

These stated operational goals fall along a spectrum from ending ongoing attacks and preventing future attacks to what appear to be a more wide-ranging objective of defeating or destroying the terrorist group. The former goals match the language of the international legal frameworks discussed above more closely. With regard to military operations in Gaza in 2008-2009, for example, Israel explained that it had "both a right and an obligation to take military action against Hamas in Gaza to stop Hamas' almost incessant rocket and mortar attacks upon thousands of Israeli civilians and its other acts of terrorism."[76] The rocket attacks were ongoing and military operations in response were the only method of stopping them. The stated goal of ending ongoing attacks falls squarely within the classic objectives of self-defence to halt or repel attacks. Similarly, the United States response to the 1998 Embassy attacks focused on preventing future attacks[77] and did not present any broader or more comprehensive goals. On that particular occasion, the United States launched a single series of strikes against two targets and that was the full extent of the action in self-defence, eliminating any real question regarding how far the right of self-defence would extend for the operational goal of preventing future attacks.

That question, of course, drives further analysis into how much force a State can use to protect itself from terrorist attacks. In particular, since the very nature of terrorism means that preventing future attacks must be a legitimate aim in self-defence — a State cannot exercise its inherent right of self-defence if it must always absorb a terrorist attack rather than seek to prevent it — then the essential question is what is allowed to achieve this goal of preventing future attacks. Indeed, the United States declared in

[76] State of Isr., The Operation in Gaza 27 December 2008 - 18 January 2009: Factual and Legal Aspects 1 (2009).

[77] Clinton, Address to the Nation, *supra* note 71.

October 2001 that it was using force against al Qaeda to "prevent and deter further attacks on the United States."[78] In the AUMF, Congress authorized the President to

> use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.[79]

Over fifteen years later, the United States continues to rely on that original claim of self-defence. However, without greater granularity on the meaning of preventing future attacks as a general self-defence objective and what it could or should encompass, the concept remains elusive, highly elastic and perpetually subject to manipulation.

As a preliminary point, preventing future attacks can include both action to eliminate or degrade the terrorist group's capability to attack and action to deter future attacks, that is, to weaken the group's will to launch attacks. Self-defence can, therefore, include a degree of force "sufficient to cause the terrorist to change his expectations about the costs and benefits so that he would cease terrorist activity."[80] This framing tracks how we conceive of self-defence against another State as well and underlies the basic understanding that force used in self-defence may well be significantly greater than the force used in the initial attack. With regard to preventing attacks, "it is clear that the more damage done to [the enemy's] military capacity the less chance there will be of a further attack by the same enemy."[81] Where terrorist groups have significant military capacity and infrastructure, States have declared operational goals that focus on destroying or substantially weakening the terrorist group's capabilities. For example, Turkey launched Operation Sun against the Kurdistan Worker's Party (PKK) in 2008 to "destroy PKK camps and hunt rebels of the PKK,"[82] an objective that was generally justified and accepted by the international

78 Letter, dated 7 Oct. 2001, from the Permanent Representative of the United States of America to the United Nations Security Council, *supra* note 9.

79 Pub. L. No. 107-40, 115 Stat. 224 (2001).

80 O. Schachter, "The Extraterritorial Use of Force against Terrorist Bases", 11 *Hous. Int'l L. J.* 309, 315 (1988-89).

81 Kretzmer, *supra* note 65, at 268.

82 P. de Bendern, "Turkey Launches Major Land Offensive into Northern Iraq", *Reuters* (22 Feb. 2008), available at http://www.reuters.com/article/us-turkey-iraq-idUSANK00037420080222.

community "as a broad response that would finally weaken [the] PKK for good."[83] After immediate actions in response to Hezbollah's attack and kidnapping of two Israeli soldiers in 2006, as Hezbollah rocket attacks accelerated in frequency and range, Israel ultimately sought to end the threat Hezbollah posed to Israel by weakening Hezbollah decisively. Prime Minister Ehud Olmert declared that they would "not stop until we can tell the Israeli people that the threat hanging over it has been removed,"[84] effectively aiming for "Hezbollah neutralization."[85]

Over time, the United States has begun to add further texture to its objective of preventing future attacks by al Qaeda. To achieve this broad self-defence objective, the United States seeks to "disrupt, dismantle, and ensure a lasting defeat of al Qaeda and violent extremist affiliates."[86] Although this formulation provides greater detail about what the United States believes is necessary to prevent future attacks, it could easily be interpreted as a broadening of the authority to use force overall, both to what end and against whom or what groups. Finally, most recently, the United States has stated that the goal of its military operations against ISIS are to "degrade and ultimately destroy"[87] the terrorist group. Its allies have presented a range of objectives in joining forces against ISIS as well. Belgium, Germany and Norway simply refer to "necessary measures of self-defence" in their respective letters to the United Nations Security Council regarding their actions in collective self-defence.[88] The United Kingdom has progressed through multiple objectives, beginning with the collective self-defence of Iraq to "end the continuing attack on Iraq, to protect Iraqi citizens and to enable Iraqi forces to regain control of Iraq's borders by striking ISIL sites and military strongholds in Syria, as necessary and proportionate

83 Tams & Devaney, *supra* note 5, at 103.

84 Israel Ministry of Foreign Affairs, Cabinet Communique, 16 July 2006, available at http://www.mfa.gov.il/mfa/pressroom/2006/pages/cabinet%20communique%2016-jul-2006.aspx.

85 R. Wright, "Strikes Are Called Part of Broad Strategy: U.S., Israel Aim to Weaken Hezbollah, Region's Militants", *Wash. Post* (16 July 2006).

86 J. C. Johnson, "The Conflict Against Al Qaeda and its Affiliates: How Will it End?", Speech at the Oxford Union, Oxford University (30 Nov. 2012), available at www.lawfareblog.com/2012/11/jeh-johnson-speech-at-the-oxford-union/#_ftn11.

87 The White House, *Statement by the President on ISIL* (10 Sept. 2014), available at https://www.whitehouse.gov/the-press-office/2014/09/10/statement-president-isil-1.

88 Letter, dated 7 Jun. 2016, from the Permanent Representative of Belgium to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2016/523, June 9, 2016; Letter, dated 10 Dec. 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2015/946, Dec. 10, 2015; Letter dated 3 Jun. 2016 from the Permanent Representative of Norway to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2016/513, 3 Jun. 2016.

measures."[89] Several months later, the United Kingdom notified the Security Council that it had launched a precision air strike against an ISIS vehicle in individual self-defence against a "target known to be actively engaged in planning and directing imminent armed attacks against the United Kingdom"[90] — focusing here on the classic objective of preventing immediate attacks. Finally, as discussed further below, by the end of 2015, the United Kingdom had broadened its stated objective to degrading and defeating ISIS.[91]

2) Military Doctrine

Military doctrine is instructive here in understanding what these stated goals mean and could mean, particularly with respect to how necessity and proportionality apply. The terms defeat, disrupt, and destroy have specific meanings in military doctrine that offer guidance for further analysis and examination of the operational goals states pronounce for these self-defence actions against terrorist groups. According to Army Field Manual 3-90-1, defeat

> is a tactical mission task that occurs when an enemy force has temporarily or permanently lost the physical means or the will to fight. The defeated force's commander is unwilling or unable to pursue that individual's adopted course of action, thereby yielding to the friendly commander's will and can no longer interfere to a significant degree with the actions of friendly forces. Defeat can result from the use of force or the threat of its use.[92]

The two primary components of defeat are physical defeat, when the enemy no longer has the military capability, including equipment and personnel, to continue fighting; and psychological defeat, when the enemy

89 Identical Letters, dated 25 Nov. 2014, from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the Secretary-General and the President of the Security Council, U.N. Doc. S/2014/851, 26 Nov. 2014.

90 Letter, dated 7 Sept. 2015, from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2015/688, Sept. 8, 2015.

91 Remarks by Prime Minister David Cameron, House of Commons, November 26, 2015, available at http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm151126/debtext/151126-0001.htm.

92 Headquarters, Department of the Army, Field Manual 3-90-1, Appendix B, Tactical Mission Tasks B-11 (4 July 2001).

loses the will to fight because of low morale or mental exhaustion that renders them no longer able to accomplish their mission.[93] In theory, the notion of defeat can extend to a State's struggle with a terrorist group. A State acting in self-defence is permitted to take action necessary to repel or end ongoing attacks and, just as with a State enemy, it is possible that defeating the terrorist group is the only way — that is, necessary — to accomplish that goal. For example, although the United States originally formulated its self-defence actions against al Qaeda as "preventing future attacks," that objective quickly morphed into defeat of al Qaeda as the means to accomplish that original goal. U.S. strategy and planning in the immediate aftermath of 9/11 and the launch of Operation Enduring Freedom in Afghanistan, therefore, "was that the elimination of al Qaida would bring the war on terrorism . . . to an end."[94]

The doctrinal meaning of defeat, however, is one based on collective action, resting on the understanding that the opposing forces have a commander who makes decisions for the entire entity and personnel who abide by the decision of the commander. This corporate notion of defeat begins to fray in the context of highly decentralized terrorist groups driven by ideology rather than allegiance to a sovereign entity. Structurally, the decentralization and non-hierarchical nature of decision-making and execution impedes the State's ability to conceptualize defeat and actually accomplish the objective. Al Qaeda and other current groups demonstrate that "cells that operate independently are much more difficult to eliminate."[95] More important, terrorists "may be fanatical devotees willing to die for their cause; this makes it extremely difficult to meaningfully affect their cost-benefit calculations."[96] These characteristics pose two primary challenges to any necessity and proportionality analysis.

First, it is unclear what defeat of a terrorist group looks like. Army doctrine explains that defeat "manifests itself in some sort of physical action, such as mass surrenders, abandonment of significant quantities of equipment and supplies, or retrograde operations."[97] In a geographically confined conflict with a terrorist group, such as the Tamil Tigers in Sri Lanka, the organization may well be "sufficiently coherent and could eventually be defeated in some meaningful sense (or its military capacity sufficiently

93 *Id*. at B-11-12.
94 A. Kurth Cronin, "How al Qaida Ends: The Decline and Demise of Terrorist Groups", 31 *Int'l Sec*. 7, 7 (Summer 2006).
95 *Id*. at 13.
96 Schmitt, *supra* note 51, at 22.
97 Field Manual 3-90-1, *supra* note 92, at B-12.

degraded to declare its defeat)."[98] However, even a cursory familiarity with al Qaeda and its derivative or affiliated groups demonstrates that these conventional physical manifestations of defeat simply do not exist or make sense in the transnational terrorism environment. Indeed, when a terrorist group withdraws in some way that is more likely to mean that they are regrouping for another day than that they are giving up the fight.

One Obama administration counterterrorism official explained that he would "define the strategic defeat of Al Qaeda as 'ending the threat that Al Qaeda and all of its affiliates pose to the United States and its interests around the world.'"[99] This definition comports with the international legal framework as a legitimate aim of self-defence but does not provide any detail to help understand what "ending the threat" al Qaeda and affiliates pose actually looks like. Different conceptions of "defeat" or "ending the threat" lead to vastly different conclusions about the success of the self-defence endeavor in this case. For example, the defeat of al Qaeda could be "defined as no terrorist attacks or attempted attacks on the US and its interests at all,"[100] or it could be understood as "no major terrorist attacks on US soil of the kind orchestrated by al-Qaeda on 9/11."[101] As one top terrorism analyst explains, "if closer to the former, it is a standard that has not existed for the United States since 1970, when it began to keep decent records. If closer to the latter, the US may already be there."[102]

The way one defines defeat, or winning, against a terrorist group then controls the way in which one analyzes the permissible extent of force in self-defence against that group. If defeat of al Qaeda means that "the US and its allies have eliminated the al-Qaida that attacked the United States, and prevented it from resurging,"[103] then self-defence would end once the achievement of that objective can be identified. Although identifying when that objective has been attained is difficult, because terrorist groups operate in the shadows, the issue is one of intelligence gathering and analysis rather than a more basic conceptual challenge. In contrast, if the defeat of al Qaeda

98 M. C. Waxman, "The Structure of Terrorism Threats and the Laws of War", 20 *Duke J. Comp. & Int'l L.* 429, 452-453 (2010).

99 E. Schmitt, "Ex-counterterrorism Aide Warns Against Complacency on Al Qaeda", *N. Y. Times*, 28 July 2011, available at http://www.nytimes.com/2011/07/29/world/29leiter.html (quoting statement by Matthew Olson made during confirmation hearings for the post of Director of the National Counterterrorism Center).

100 A. Kurth Cronin, "The 'War on Terrorism': What Does it Mean to Win?", 37 *J. Strat. Stud.* 174, 191 (2014).

101 *Id.*

102 *Id.*

103 *Id.* (noting that such a scenario "may shortly be achieved").

means that "no al-Qaida 'associate' is attacking anyone, anywhere,"[104] then the United States and its allies would be entitled to continue acting in self-defence until that objective could be achieved. The nature of terrorism, of course, means that such an objective is unlikely, if not impossible, to ever be achieved, let alone verified.[105] As a result, this broader conception of defeat renders the necessity and proportionality criteria for lawful self-defence effectively toothless without some more specific metrics to guide the analysis.

Second, there is an equal lack of clarity as to what actions are necessary or effective in defeating a terrorist group, a challenge that significantly handicaps any attempt to analyze when a state's choice of particular actions against a terrorist group go beyond what is necessary and proportionate in self-defence. There are few, if any, examples of international commentary, whether approval or condemnation, regarding the type of acts taken to defeat a terrorist entity, simply because few State actions against terrorist groups have been characterized as designed to defeat the terrorist group rather than prevent further attacks. The international community and individual States did remark on the nature and extent of specific acts taken by Turkey in Operation Sun in 2008 and by Israel in 2006 against Hezbollah, but neither of those self-defence operations aimed to defeat the terrorist entity. Rather, they focused on the objective of weakening the enemy decisively such that the enemy could not continue its attacks against the state, an objective short of defeating the group. Comments regarding the proportionate or disproportionate nature of the actions taken by Turkey or Israel,[106] therefore, do not provide any useful guidance regarding the extent of force that is or

[104] *Id*. (noting that if defeat is so characterized, "the US will be forced into a perpetually tactical, reactive mode").

[105] Department of Defense General Counsel Jeh Johnson affirmed as much in a 2012 speech, reminding us that the United States and its allies cannot "capture or kill every last terrorist who claims an affiliation with al Qaeda"). Johnson Oxford Union Speech, *supra* note 86.

[106] For example, States generally seemed to accept Turkey's actions, noting that they were "restricted to specific actions against PKK targets in the border area of northern Iraq." T. Ruys, "Quo Vadit Jus ad Bellum?: A Legal Analysis of Turkey's Military Operations Against the PKK in Northern Iraq", 9 *Melb. J. Int'l L.* 334 (2008), citing Maxime Verhagen, Dutch Minister of Foreign Affairs, "Beantwoording vragen van het lid Van Bommel over een Turkse invasie in Noord-Irak" (Ministerial Statement, 3 Mar. 2008). Initial reactions to Israel's operations against Hezbollah were cautiously supportive when Israel's operations focused on eliminating Hezbollah's rocket launchers and containing the kidnappers' escape routes and lines of communication, but as Israel expanded its operations to include acts perceived to be against the host state, the international community turned towards characterization and criticism of the operation as disproportionate. *See* Tams & Devaney, *supra* note 5, at 104; Watkin, *supra* note 2, at 86; Schmitt, *supra* note 57.

should be allowed if defeat of the terrorist group is the legitimate objective necessary to end the attack or threat of attacks.

A primary tactic for the United States in achieving the objective of defeating al Qaeda has been the elimination of al Qaeda's senior and mid-level leadership. The successful raid against Osama bin Laden in May 2011 is but the most well-known example; and as President Obama's top counterterrorism advisor explained later that year, "[i]f we hit Al Qaeda hard enough and often enough, there will come a time when they simply can no longer replenish their ranks with the skilled leaders that they need to sustain their operations."[107] Targeting a group's leaders appears to be a reasonable and proportionate measure in pursuing the defeat of a terrorist group. In particular, if conventional understandings of defeat — as discussed above — that rest on a commander's determination that he is unable or unwilling to continue the fight lose their traction in the terrorism context, then killing or capturing the leaders is a natural option to achieve that goal in an alternative fashion.[108]

Similarly, existing understandings of necessity and proportionality surely encompass actions to destroy, capture or neutralize a terrorist group's main bases, training camps or other facilities. United Kingdom Prime Minister David Cameron used this formulation as part of his description of his government's objectives in joining the fight against ISIS. He stated, "we want to defeat the terrorists, by dismantling their networks, stopping their funding, targeting their training camps and taking out those plotting terrorist attacks against the United Kingdom."[109] But how far do these notions of killing terrorist operatives and destroying terrorist facilities extend? One might argue that defeating a terrorist group requires that the State kill or capture every member of the group, however one defines membership in the group, no matter where located around the world and regardless of whether the person was a member of the group at the time of the attack or joined the group after the state began its self-defence operations. This argument carries

[107] E. Schmitt & M. Mazzetti, "Obama Advisor Outlines Plans to Defeat Al Qaeda", *N. Y. Times* (29 June 2001), available at http://www.nytimes.com/2011/06/30/world/30terror.html?action=click&contentCollection=World&module=RelatedCoverage&region=Marginalia&pgtype=article.

[108] There is growing research and debate about the effectiveness of this so-called "decapitation" strategy. *See e.g.*, J. Jordan, "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation", 18 *J. Strat. Stud.* 719-755 (2009); Cronin, *supra* note 78; B. C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism", 36 *Int'l Sec.* 9-46 (Spring 2012); J. Jordan, "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes", 38 *Int'l Sec.* 7-38 (Spring 2014).

[109] Remarks by Prime Minister David Cameron, *supra* note 91.

some weight, particularly when each leader killed is quickly replaced, ideological fanaticism drives individuals to join and fight for the terrorist group, and the decentralized framework of the terrorist network belies any potential leadership ability or desire to call a halt to attacks from any and all adherents.

However, if defeating the terrorist group is a legitimate aim of self-defence and this expansive interpretation of defeating the group were to be accepted, the State's right to use force in self-defence could be boundless. As with the very meaning of defeat above, such a result is fundamentally inconsistent with the very purpose of the necessity and proportionality criteria. Although the State surely has a methodology or framework for determining if and when the terrorist group is so decimated as to no longer pose any threat, any such framework rests on significant uncertainty given the nature of terrorist groups. In addition, because this analysis is entirely intelligence-driven, there is no way for outside observers to comment in a productive manner, thus emasculating any broader effort at constraint — without access to the intelligence, another state, an advocacy group or an international organization is hard pressed to compete with the State's presentation and characterization of the relevant information as justification for continued action in self-defence.

"Degrade and destroy" is the current catch phrase for operations against ISIS, the objective President Obama set forth in September 2014. The United Kingdom uses similar justifications for acting in both individual and collective self-defence against ISIS: Prime Minister David Cameron declared that "the initial objective is to damage [ISIS] and reduce its capacity to do us harm" and further explained that dismantling — destroying — the "so-called caliphate" is essential to protecting the United Kingdom's security.[110] In these statements, destroying the group appears to mean to completely eliminate the group altogether. However, it is not clear whether that is a rhetorical statement used to garner popular support for the military operations or whether destroying the group is the actual intention, and if not, what the consequences of a disconnect between the rhetoric and the intent are for understanding the legal parameters for acting in self-defence.

In contrast, military doctrine defines destroy as a "tactical mission task that physically renders an enemy force combat-ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition

[110] *Id*. (noting that "For as long as [ISIS] can pedal the myth of a so-called caliphate in Iraq and Syria . . . it will be a rallying cry for Islamist extremists all around the world, and that makes us less safe").

without being entirely rebuilt."[111] Destroy as such is more a component of or tactic for defeating a group than an overarching objective, leaving little guidance for understanding exactly what "destroy" means with regard to a terrorist group and raising the same questions that "defeat" engenders about the outer boundaries of self-defence. If destroying the group is a legitimate aim in self-defence, how do we determine when force is still necessary and how do we measure how much force is needed and for how long to achieve the goal, especially when we are not certain what destroying a terrorist group actually looks like. In addition, if it is the doctrinal definition of "destroy" that is to guide decision-makers and international law analysis, the definition's utility is limited with respect to terrorist groups — a terrorist group can be "combat-effective" with very little (as the use of box cutters on 9/11 demonstrated) and can often reconstitute much more quickly than conventional forces. If the extent of self-defence were to be limited to this doctrinal conception of "destroy," states would likely consider the parameters for self-defence to be too restrictive, because the necessity and proportionality paradigm would prevent states from taking action beyond short-term dismantling of terrorist capabilities.

B. Counterterrorism as Armed Conflict

A related issue is whether, once a State is engaged in ongoing military operations against a terrorist group in self-defence after being attacked, characterizing those hostilities as an armed conflict will change the extent to which the State is allowed to act in self-defence. Throughout most of the post-9/11 period, the United States has maintained that it is engaged in an armed conflict with al Qaeda[112] and, notwithstanding continued resistance to the notion of an armed conflict between a State and a transnational terrorist group in certain quarters, there is general acceptance that the scope of armed

[111] Field Manual 3-90-1, *supra* note 91, at B-12.

[112] All three branches of the U.S. government have demonstrated that they view the situation as an armed conflict. *See* Authorization to Use Military Force ("AUMF"), Pub. L. No. 107-40, 115 Stat. 224(a) (2001); *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006); Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57833 (Nov. 13, 2001) (stating that the 9/11 attacks "created a state of armed conflict that requires the use of the United States Armed Forces"); Dept of Def. Military Commission Order No. 1, Procedures for Trials by Military Commissions of Certain Non-United States Citizens in the War Against Terrorism (21 Mar. 2002); *see also* Koh Address, *supra* note 21 (stating that the United States is "in an armed conflict with Al Qaeda, as well as the Taliban and associated forces"); Reply of the Government of the United States of America to the Report of the Five UNHCR Special Rapporteurs on Detainees in Guantanamo Bay, Cuba 4 (2006), available at http://www.asil.org/pdfs/ilib0603212.pdf ("[T]he United States is engaged in a continuing armed conflict against Al Qaeda, the Taliban and other terrorist organizations supporting them, with troops on the ground in several places engaged in combat operations.").

conflict can indeed encompass such a State versus non-State conflict. At the most basic level, the armed conflict paradigm raises the question of whether victory in war supplants self-defence against an attack or imminent attack as the analytical structure for assessing the lawfulness of state action. The law of armed conflict (LOAC) will, of course, govern the conduct of hostilities between the two parties and the protection of persons to minimize suffering during armed conflict.[113] However, the key issue for the instant discussion is whether the characterization as armed conflict removes the necessity and proportionality criteria from consideration and leaves the extent of self-defence — how much force against what groups and for how long — to be determined solely by the idea of victory in war.

1) Transition from Self-Defence to Victory?

Historically, a State's right to act in self-defence against an armed attack by another State was, in certain situations, "a right to resort to war."[114] Some argue that, in such a situation, necessity and proportionality are relevant at the onset of war to determine whether the victim State may respond in self-defence to the attack, but would not continue to determine the extent and parameters of the State's use of force thereafter. The attack triggers the necessity for force, but the constraint placed by the need to repel or deter the attack then fades away. As a result, a State "may prosecute its war to final victory even after the point at which this is no longer necessary to reverse or frustrate the initial use of force which provided the justification for the war."[115] Similarly, proportionality is determinative when self-defence is triggered, but only with respect to whether the decision to resort to war is proportionate to the nature and gravity of the armed attack suffered by the State.[116] Once the armed conflict is underway, the analysis changes: "[t]here is no support in the practice of States for the notion that proportionality remains relevant — and has to be constantly assessed — throughout the

[113] For an analysis of the consequences of blurring the armed conflict and self-defense justifications for targeted strikes against terrorist groups, *see* L. R. Blank, "Targeted Strikes: The Consequences of Blurring the Armed Conflict and Self-Defense Justifications", 38 *Wm. Mitchell L. Rev*. 1655-1700 (2012).

[114] J. L. Kunz, "Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations", 41 *Am. J. Int'l L.* 872, 877 (1947).

[115] D. Rodin, *War and Self-Defense*, 112 (2002). Others continue to rely on the self-defense framework and necessity, arguing that "as long as necessity of self-defence continues to exist in the sense of an ongoing attack, which can include occupation of (part of) a state's territory or ongoing military operations aimed at facilitating an attack, or clear evidence of threat of attack in the proximate future persists, the right of self-defence will remain operative." T.D. Gill, "When Does Self-Defence End?", *in The Oxford Handbook of the Use of Force in International Law* 738, 745 (M. Weller ed., 2015).

[116] Dinstein, *supra* note 35, at 263.

hostilities in the course of war."[117] Based on this understanding of conflict, this transition from self-defence to war, from repelling an armed attack to victory, therefore means that a "[w]ar of self-defence, if warranted as a response to an armed attack, need not be terminated when and because the aggressor is driven back: rather, it may be carried on by the defending State until final victory."[118]

Taking this analytical approach from the State-on-State context to the counterterrorism arena triggers the immediate question of whether the conception of a transition from self-defence to victory only applies in the traditional environment of States going to war with other States, or whether we can conceptualize a conflict with a non-State group in the same comprehensive manner. The growing acceptance of the idea of an armed conflict between a state and a transnational terrorist group suggests that this framework can be applied to such a conflict. At the same time, the international community has pushed back against the U.S.'s expansive view of the conflict, evincing a general reluctance to accept a global or even transnational battlefield.[119] Perhaps, therefore, the idea of a transition from self-defence to victory is more conditional in the counterterrorism as armed conflict context, although we lack a set of guiding principles to determine how and on what it would be conditioned. One such example is the application of the criterion of proportionality. In the context of conflict with a transnational terrorist group, for example, it is worth considering whether the traditional argument that *jus ad bellum* proportionality no longer needs to be assessed once a conflict is underway remains reasonable. Proportionality seeks to minimize the disruption to international peace and security; as a result, one possible accommodation is that proportionality should continue to apply after a State's self-defence operations launch conflict with a terrorist group with respect to where and against which groups the conflict can or should extend. Because conflict with a transnational terrorist group is likely

117 *Id*. at 262.

118 *Id*. at 266. *See also* Kretzmer, *supra* note 65, at 258 ("under traditional laws of war, once a war had started each party could carry on fighting until victory (whatever that may mean) was achieved").

119 Int'l Comm. of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, at 16, 32IC/15/11 (Oct. 2015) (hereinafter "ICRC Challenges Report") ("The ICRC considers that [international humanitarian law (IHL)] would begin to apply in the territory of such a State if and when the conditions necessary to establish the factual existence of a separate NIAC in its territory have been fulfilled. In other words, if persons located in a non-belligerent State acquire the requisite level of organization to constitute a non-State armed group as required by IHL, and if the violence between such a group and a third State may be deemed to reach the requisite level of intensity, that situation could be classified as a NIAC. Thus, IHL rules on the conduct of hostilities would come into effect between the parties").

to expand in time and geography, proportionality would thus help to maintain the balance between sovereignty, territorial integrity and order in the international system, and the State's inherent right of self-defence.

2) Identifying the End of Conflict

Even if victory does displace necessity and proportionality as the determinant of the extent of force when a State is in armed conflict with a transnational terrorist group, it is unclear what victory against a transnational terrorist group looks like. As one terrorism expert has noted, "[i]n this war, no one seems to know what winning is."[120] At present, neither international law nor strategic studies analysis offers effective guidance for understanding how an armed conflict against a terrorist group ends. Without tools for identifying when a conflict ends or, put another way, victory is achieved, it is difficult to delineate metrics for when a State has exceeded the parameters for the use of force against a terrorist group. For this reason, it would be wise to consider if and how necessity and proportionality can continue to play a role in assessing the reasonableness of the use and extent of the use of force.

LOAC references the end of armed conflict in international armed conflict with phrases in the Geneva Conventions such as "cessation of active hostilities"[121] and "general close of military operations."[122] At the time the Conventions were drafted, the "general close of military operations" was considered to be "when the last shot has been fired."[123] The Commentary to the Fourth Geneva Convention then provides further explanation:

> When the struggle takes place between two States the date of the close of hostilities is fairly easy to decide: it will depend either on an armistice, a capitulation or simply on *deballatio*. On the other hand, when there are

[120] Cronin, *supra* note 100, at 176.

[121] Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, art. 118, 75 *U.N.T.S.* 135 (entered into force Oct. 21, 1950) (referring to the release and repatriation of prisoners of war).

[122] Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, art. 6, 75 *U.N.T.S.* 287 (entered into force Oct. 21, 1950) (denoting the end of application of the Fourth Geneva Convention in the territory of parties to the conflict upon the general close of military operations, or in occupied territory, one year after the general close of military operations); *see also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), *adopted by Conference* June 8, 1977, 1125 *U.N.T.S.* 3, art. 3(b) ("The application of the Conventions and of this Protocol shall cease, in the territory of Parties to the conflict, on the general close of military operations . . . .").

[123] Final Record of the Diplomatic Conference of Geneva of 1949, Vol. II-A, at 815.

> several States on one or both of the sides, the question is harder to settle. It must be agreed that in most cases the general close of military operations will be the final end of all fighting between all those concerned.[124]

In non-international armed conflict — the relevant framework for any conflict between a State and a non-State group — treaty law provides no real methodology for identifying the end of a conflict. Common Article 3 of the Geneva Conventions does not reference the end of armed conflict and Additional Protocol II's mentions of the end of armed conflict[125] do not define or elucidate any further meaning of the concept. In one of the only judicial pronouncements addressing the end of non-international armed conflict, the International Criminal Tribunal for the former Yugoslavia (ICTY) declared that the application of LOAC — which applies only during armed conflicts — "extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved."[126]

In many conflicts, including non-international armed conflicts, these notions of "end of active hostilities," the "general close of military operations," or "peaceful settlement" are useful in demarcating the end of conflict. Armistices and peace treaties feature as the conflict-ending mechanism in most inter-State conflicts and it is not uncommon to see peace treaties or settlements bring an end to an internal conflict as well — Colombia being the most recent example.[127] In general, however, the nature of terrorism and counterterrorism is that States are not going to defeat terrorism; rather, terrorism is something to be managed, minimized, and defended against.[128] At the most basic level, "[a] war against groups of

[124] Int'l Comm. Red Cross, Commentary on the Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War 62 (1958) (footnotes omitted). *See also* W. Heintschel von Heinegg, "Factors in War to Peace Transitions", 27 *Harv. J.L. & Pub. Pol'y* 843, 845-46 (2004).

[125] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), arts. 2(2), 6, 25, (adopted by Conference June 8, 1977), 1125 *U.N.T.S.* 609.

[126] *Prosecutor v. Tadić*, Case No. IT-94-1, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction para. 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[127] E. Lopez & S. Capelouto, "Colombia Signs Peace Deal with FARC", *CNN* (Nov. 13, 2016), available at http://www.cnn.com/2016/11/12/world/colombia-farc-peace/.

[128] C. Vance, "A War to Be Won, to Be Won", *Oped News* (27 May 2010), available at http://www.opednews.com/articles/A-War-to-Be-Won-to-be-Wo-by-carrie-vance-100524- 408.html ("All terrorist groups end, but terrorism, like crime, never ends." (quoting Seth G. Jones)); S. G. Jones & M. C. Libicki, How Terrorist Groups End: Lessons for Countering Al Qa'ida, xii, xvi-xvii (2008).

transnational terrorists, by its very nature, lacks a well delineated timeline."[129] Not only is it difficult to envision an end to the hostilities, but more problematic, there is at present no way of identifying what that end might look like.

Terrorist groups morph, splinter, and reconfigure, making it difficult to determine if, let alone when, they have been defeated.[130] Furthermore, the diffuse geographical nature of most conflicts with terrorist groups and the decentralized nature of such groups generally makes traditional temporal concepts unlikely to apply effectively to such conflicts. A conflict with transnational terrorist groups will not produce a surrender ceremony, the equivalent of V-E Day, or any other identifiable moment marking the end of the conflict.[131] No less, terrorist groups may launch attacks or take other action not because they are in a position of strength, but precisely because they are at a moment of existential danger. A group like al Qaeda or one of its ideological brethren may "have an innate compulsion to act — for example, it may be driven to engage in terrorist attacks to maintain support, to shore up its organizational integrity, or even to foster its continued existence."[132] Signs that might generally be understood to mean an enemy is getting stronger can thus actually be signals that it is significantly weakened; in the same way, a lack of attacks or overt action does not mean that a terrorist group is in decline.

Interestingly, the ICTY's holding that the temporal and geographic limits of LOAC range beyond the exact time and place of hostilities, a broad protective approach to the application of LOAC, can easily lead to a definition paralysis in a conflict with a terrorist group because it is unlikely that a "peaceful settlement" or "general conclusion of peace" will be achieved in any foreseeable period of time, if ever, in this type of conflict. The United States might defeat al-Qaeda in some meaningful way, ending their ability to launch any effective attacks against the United States or its allies. For example, some U.S. courts have thus talked of a time "when operations against al Qaeda fighters end, or the operational capacity of al

129 N. Balendra, "Defining Armed Conflict", 29 *Cardozo L. Rev*. 2461, 2467 (2008).

130 *See* Part II.A. *supra* & Part III.B. *infra*.

131 *See* Johnson Oxford Union Speech, *supra* note 86 ("We cannot and should not expect al Qaeda and its associated forces to all surrender, all lay down their weapons in an open field, or to sign a peace treaty with us"); Amos N. Guiora, *American Counterterrorism: The Triangle of Detention, Interrogation and Trial, Keynote Address at the Magna Carta Institute's Symposium, Towards a Global Legal Counterterrorism Model: Transatlantic Perspectives* 6 (23 Dec. 2009), *available at* http://ssrn.com/abstract=1527314 ("Precisely because there is no defined end to terrorism, a ceremony reminiscent of General MacArthur receiving Japan's surrender on the 'USS Missouri' will not take place.").

132 Cronin, *supra* note 94 at 11.

Qaeda is effectively destroyed."[133] As noted above, many analysts suggest that the United States is steadily approaching that time, if it is not already here. But other terrorist groups have already taken up the same fight and it is easy to see how the United States will still consider that it is engaged in an armed conflict with terrorist groups. The 2001 AUMF leaves open that very scenario: unlike the declarations of war against Germany and Japan in 1941, which directed the President not only to "carry on war against the Government of Germany" or the Imperial Government of Japan, but also to "bring the conflict to a successful termination,"[134] the AUMF provides no specified end.

In fact, although the United States government's latest pronouncement on legal and policy issues offers extensive and thoughtful explanations about the legal framework and reasoning behind current and anticipated U.S. counterterrorism operations, it nonetheless raises the specter of a conflict easily redefined to persist after al Qaeda's disintegration. In explaining how the government conceptualizes the end of the conflict with al Qaeda and associate forces, the report states that

> [a]t a certain point, the United States will degrade and dismantle the operational capacity and supporting networks of terrorist organizations like al-Qa'ida to such an extent that they will have been effectively destroyed and will no longer be able to attempt or launch a strategic attack against the United States. At that point, there will no longer be an ongoing armed conflict between the United States and those forces.[135]

Note that the conceptual framework of who the United States needs to defeat (or "degrade and dismantle") is no longer "al Qaeda and associated forces," but rather "terrorist organizations like al-Qaeda," which is far more sweeping than even the already broad notion of conflict with al Qaeda. The focused nature of the tactical and operational definition of effectively destroying an enemy by dismantling and degrading their operational capacities is thus lost in the highly elastic delineation of the enemy — "terrorist organizations like al-Qaeda" offer no inherent boundaries but could simply be expanded to incorporate each new terrorist organization that appears if the State so desires.

[133] *Padilla v. Bush*, 233 F. Supp. 2d 564, 590 (S.D.N.Y. 2002).

[134] 77th U.S. Congress. "Joint Resolution 119 of December 11, 1941, declaration of war on Germany." *U.S. National Archives and Records Administration*. Pub. L. 77-331, 55 Stat. 796, enacted December 11, 1941.

[135] Legal and Policy Frameworks, *supra* note 18, at 11.

If the extent of acceptable force in self-defence against the original terrorist attack or series of attacks is determined by the end of conflict or victory, an effective application of any such constraints depends on both a viable means for distinguishing between conflicts with different terrorist groups, and a recognized requirement that States cannot simply combine campaigns against terrorist groups into one seemingly never-ending conflict. More than fifteen years in, the United States has killed or captured hundreds of al Qaeda operatives, including Osama bin Laden and substantial portions of the group's leadership.

Yet, the more the United States fights, the longer the war's trajectory seems to grow. Twelve years after 9/11, [a] senior US Defense official . . . told Congress that the war with al-Qaeda would continue 'for 10 or 20 years' more. How could that be? Clearly Al-Qaeda is not the same organization it was a decade ago. What does success mean?[136]

These questions have enormous strategic and operational consequence. At the same time, they present telling concerns about how we can and should conceive of the extent of self-defence. One useful and thoughtful approach appears in a speech by then-Department of Defense General Counsel Jeh Johnson in late 2012:

> I do believe that on the present course, there will come a tipping point – a tipping point at which so many of the leaders and operatives of al Qaeda and its affiliates have been killed or captured, and the group is no longer able to attempt or launch a strategic attack against the United States, such that al Qaeda as we know it, the organization that our Congress authorized the military to pursue in 2001, has been effectively destroyed.
>
> At that point, we must be able to say to ourselves that our efforts should no longer be considered an "armed conflict" against al Qaeda and its associated forces; rather, a counterterrorism effort against *individuals* who are the scattered remnants of al Qaeda, or are parts of groups unaffiliated with al Qaeda, for which the law enforcement and intelligence resources of our government are principally responsible, in cooperation with the international community – with our military

[136] Cronin, *supra* note 100, at 178.

> assets available in reserve to address continuing and imminent terrorist threats.[137]

The difference between these two operational scenarios — armed conflict with al Qaeda as an organization or periodic reliance on military force to address imminent terrorist threats — is central to parsing out how necessity and proportionality apply to cabin or guide the use of force in self-defence. Once that tipping point, or transition from conflict to law enforcement, is reached, the right of self-defence would not encompass force to the extent needed to defeat or destroy al Qaeda or any other associated group. Instead, necessity and proportionality would limit the extent of the force allowed in self-defence only to that aimed at preventing imminent terrorist attacks and threats.

As the previous sub-section discusses, the State's strategic and operational goals provide useful guidance for framing the international law parameters of self-defence against terrorist groups. Allowing a State to characterize operations against a terrorist group as armed conflict can potentially give that State *carte blanche* to set perpetually expanding aims in self-defence, a dangerous scenario. At the same time, this risk should not lead to a rejection of the notion of armed conflict with terrorist groups; rather, it should be the impetus for a more deliberate examination of what it means to be in a conflict with a terrorist group and what success looks like in such a conflict. Just as LOAC mandates that the determination of the existence of armed conflict must be based on an objective analysis of the situation of violence, not the claims or goals of the parties to the conflict, so it is essential that the extent of force allowed in self-defence be tethered to an objective analysis of legitimate aims of self-defence and how such aims should be understood. Otherwise, the self-defence to armed conflict to victory progression will lead to unfettered state discretion in the amount, degree and duration of force allowed.

III. INITIAL SUCCESS AND THE CHANGING FACE OF SELF-DEFENCE

Beyond the challenges of assessing the extent of force in self-defence that is allowed in pursuit of the various possible legitimate objectives of self-defence, several particular characteristics of transnational terrorist groups and military operations against such groups introduce another set of questions as well. These questions derive from the shifting nature of the military operations and of the terrorist group as the State enjoys initial

[137] Johnson Oxford Union Speech, *supra* note 86.

success in its forceful responses to the terrorist group's attack or series of attacks. As a preliminary point, several factors can alter how necessity and proportionality apply to the use of force in self-defence. Some offer little useful application in the context of counterterrorism, such as if an attacking State accepts a United Nations Security Council-mandated ceasefire and provides guarantees of repetition.[138] In contrast, if, for example, the host State reversed its prior intransigence about repressing terrorist attacks from its territory and took action itself to arrest and prosecute or forcefully stop the terrorists, then the necessity for forceful action by the victim State would be significantly less and its "right of self-defence will diminish accordingly."[139] Finally, while a State would no longer have a right to continue acting in self-defence if the attacking state or group no longer poses a threat, that assessment is extraordinarily difficult to make with regard to a terrorist group, because it is part of their *modus operandi* to remain out of sight and then launch attacks without warning.

As a State takes forceful action in response to terrorist attacks and to prevent future attacks, the calculus with respect to the threat of those future attacks can change. If necessity and proportionality continue to apply throughout the use of force in self-defence (either because the situation is not an armed conflict or if one discounts the argument that necessity and proportionality no longer govern once a war of self-defence begins), then as the threat of future attacks diminishes, the scope of self-defence should contract accordingly because the necessity for action has lessened and the amount of force needed to attain the objective is lower. Operationally, however, this approach proves counterintuitive. If a State's initial success causes the threat of future attacks to decrease, and therefore the right of self-defence diminishes, the state would have less room for action — and the terrorist group would then likely have more space to reconstitute, maneuver and launch attacks, then re-triggering the State's right to act in self-defence. The result: a circular argument and a legal framework divorced from the operational reality of how States respond to threats, which will reduce the willingness of States to abide by the international legal parameters for action in self-defence. However, if necessity and proportionality do not continually operate to constrain or guide the extent of the use of force, then any terrorist attack would automatically trigger the State's right to use any force necessary to defeat or destroy the group, even if much less force was all that was needed to prevent further attacks. A related question arises if a State's

[138] *See* Gill, *supra* note 115, at 747 (noting that not every "measure the Council may choose to take will have that effect, but if the Council's action results in removing the necessity for the exercise of self-defence, there would be no legal basis for continuing its exercise").

[139] Schmitt, *supra* note 51, at 33.

actions in self-defence stop or forestall immediate further terrorist attacks, but the group still has the capability and intent to attack the State and is simply waiting until it has another viable opportunity, even if that might be a year or more in the future. According to classical threat analysis, the threat a group poses is based on its capabilities combined with its intent.[140] The State will make such determinations and the sources, analysis and substance of the determinations will remain classified, making any useful objective judgment of the necessity for continued forceful measures and how far those measures must go to eliminate the threat difficult, if not impossible.

Three features of the contemporary counterterrorism environment are emblematic of the need to consider how initial success and the responsive acts or maneuvers of the terrorist group affects how we consider the extent of self-defence against terrorist groups. The following sub-sections address these developments: the terrorist group finds safe haven in another State or area; the terrorist group splinters or reconstitutes as one or more new and related groups; and the terrorist group's attacks and propaganda inspire the creation of new groups or vows of allegiance from other existing groups.

A. New Territory: The Geography of Necessity and Proportionality

The story of al Qaeda is, in part, the story of how a terrorist group seeks and secures new safe havens and space to operate as it faces either law enforcement or forceful action to contain it. First operating in Afghanistan during the Soviet occupation and the corresponding armed conflict in the 1980s, al Qaeda was then based in Sudan in the early and mid-1990s before being expelled from Sudan and reestablishing its main base of operations in Afghanistan in the late 1990s. After 9/11 and the launch of Operation Enduring Freedom in Afghanistan, al Qaeda has maneuvered accordingly, seeking safe haven over the border in Pakistan and then in remote areas of Yemen. Most recently, al Qaeda's core leadership has reportedly decided "that the terror group's future lies in Syria and has secretly dispatched more than a dozen of its most seasoned veterans there . . . to start the process of creating an alternate headquarters in Syria."[141] Given that terrorist groups

[140] C. B. King, *Alternative Threat Methodology*, 4 *J. Strat. Sec.* 57, 58 (spring 2011) ("the 'traditional' method to estimate terrorist threat is to decompose threat into two components, 'intent' and 'capability,' estimate the two variables independently, and then combine them (usually, but far from always, multiplicatively) to generate a non-dimensional threat score").

[141] E. Schmitt, "Al Qaeda Turns to Syria, With a Plan to Challenge ISIS", *N.Y. Times* (May 15, 2016), available at http://www.nytimes.com/2016/05/16/world/middleeast/al-qaeda-turns-to-syria-with-a-plan-to-challenge-isis.html.

rarely have the ability to confront military forces,[142] finding new territory in which to operate is the natural response to aggressive State action against the group in the original geographical locale. As a result, regardless of "the effects of the use of repressive military force" in the immediate location, in some cases "it may result in the export of the problem to another country."[143]

The effect of this spread to another country on the State's right to use force in self-defence and the extent of that force that is, how far it reaches geographically, or whether geography is relevant at all, is unclear. Returning to the fundamental purpose of *jus ad bellum* and the United Nations Charter framework, the international legal framework prohibits the use of force in the territory of another State in order to "end the scourge of war"[144] and minimize the spiraling of violence and resort to force in the international system. It is generally understood that any time a State uses force in the territory of another State, it must do so within one of the three exceptions to the prohibition: consent, United Nations authorization, or self-defence. A terrorist group's relocation to another country therefore raises the question of whether the existing self-defence justification is sufficient to get the State across the border, so to speak, or whether the introduction of a new state's territory into the equation demands a new *jus ad bellum* analysis.

There are three possible interpretations: first, one could argue that as long as the State continues to have the right to act in self-defence against the particular group, that right extends to wherever that group or its operatives are located. Operationally, this approach has merit — if the group continues to launch attacks or present a threat of future attacks such that the State can use force in self-defence to repel or prevent such attacks, then the State should not have to wait for an attack emanating from this new territory to be able to take repressive action against the group's operatives or infrastructure there. This analysis tracks with the generally accepted argument that preventing future attacks is a legitimate objective of using force in self-defence.[145] Second, if the violence between the State and the terrorist group

[142] *See e.g.* Cronin, *supra* note 64 ("Terrorist networks, such as al Qaeda, generally have only dozens or hundreds of members, attack civilians, do not hold territory, and cannot directly confront military forces").

[143] Cronin, *supra* note 94, at 30.

[144] U.N. Charter, Preamble.

[145] *See e.g.*, Schmitt, *supra* note 451, at 25 ("unless one is willing to deny victim States a consequential right of self-defense against terrorists, it is reasonable to interpret self-defense as permitting the use of force against terrorists who intend, and have the capability, to conduct future attacks against the victim"); Ago, *supra* note 39 at para. 121 (including preventing attacks from occurring as a legitimate aim of self-defense). For the views of states engaged in self-defense against terrorist groups, *see* Clinton, Address to the Nation, *supra* note 71; D. Vidalon, "France Carries Out First Air Strikes on Islamic

constitutes an armed conflict, one could argue that the existence of the armed conflict is the sole justification needed to use force in this new location. This claim is highly contested and lies at the center of the ongoing debate about the geography of the battlefield, a complex and challenging issue.[146] These first two theories place no constraints on the extent of self-defence when a terrorist group seeks a new home in another State's territory and actually permit an expansive conception of the extent of self-defence by eliminating the need to take geography into consideration in assessing necessity and proportionality.

The third possible argument produces the opposite result. According to this interpretation, when the terrorist group seeks safe haven in a new State, necessity as a criterion of lawful self-defence would require that the State face an armed attack or imminent armed attack from the group in that location before it can take action in self-defence there against the group or its operatives. This interpretation of the impact of geographical expansion on self-defence appears to offer the greatest adherence to the prohibition on the use of force, by restricting the State's ability to resort to force. However, it consequently provides greater space for terrorist groups and other non-State groups to escalate attacks against States without the same consequences, thus undermining the overarching goal of reducing violence and also interfering with a State's basic right to protect its people and territory from attacks. Ultimately, any parameters for the extent of force in self-defence against a group scattered in different countries must weigh the authority to use force in self-defence against the general goal of minimizing the resort to force and preventing a spiraling of violence.

B. Splintering and Reconstituting Groups

In June 2002, only eight months into what is now a fifteen-plus year conflict with al Qaeda, a news report stated the following about al Qaeda:

> Al Qaeda trainees are no longer in Afghanistan learning by the thousands to build bombs or hijack planes. Osama bin Laden, if alive, is incommunicado, hampered from

State", *Sydney Morning Herald* (27 Sept. 2015) (French Prime Minister Manuel Valls stated that France is "hitting Daesh because this terrorist organization prepares its attacks against France from Syria").

146 *See* ICRC Challenges Report, *supra* note 119, at 14-16; N. Lubell & N. Derejko, "A Global Battlefield? Drones and the Geographical Scope of Armed Conflict", 11 *J. Int'l Crim. Just.* 65-88 (2011); M. N. Schmitt, "Charting the Legal Geography of Armed Conflict", 90 *Int'l Leg. Stud.* 1 (2014); L. R. Blank, "Debates and Dichotomies: Exploring the Presumptions Underlying Contentions About the Geography of Armed Conflict", 16 *Y. B. Int'l Human. L.* 297-318 (2013).

> plotting new attacks. His operations czar, Abu Zubaydah, is in US custody, and talking. His military chief, Mohammed Atef, is presumed dead.
>
> In short, Al Qaeda Central is no more. Its home turf is gone. Its command structure is broken. Its brazen freedom to recruit, communicate, and plan and to raise funds has been sharply curtailed.
>
> There's just one problem: Al Qaeda is reinventing itself. Just as a frail mother spider sends hundreds of young creeping to the far reaches of her web, Al Qaeda's core mission to wage jihad on Americans and their allies lives on through its cells and links to radical Islamic groups already dispersed around the globe.[147]

Al Qaeda has continued to be "a moving target, with experts arguing that it has changed structure and form numerous times."[148] Faced with pressure from law enforcement or State military action, terrorist groups may go underground, splinter into two or more successor groups, or reconstitute into a new group after the main leadership scatters or goes into hiding to avoid capture or death. Al Qaeda is a prime example with many such offshoots — to name but two, AQAP is the most well-known "spinoff" of what is now called "core al Qaeda," and the Khorasan Group, a target of United States strikes in Syria in 2014, is a group of "seasoned al Qaeda operatives who . . . established a safe haven to plot attacks on the West."[149] And although there is debate about ISIS's origins, the United States and many others trace ISIS back to al Qaeda, arguing that al Qaeda in Iraq, one of the original al Qaeda offshoots, reconstituted itself as ISIS after being driven underground and drastically weakened during the United States counterterrorism surge and continued presence in Iraq through 2011.[150]

147 A. Scott Tyson, "Al Qaeda Broken, But Dangerous", *Christ. Sci. Mon.* (24 June 2002).

148 Cronin, *supra* note 94, at 7. Cronin explains that "[n]o previous terrorist organization has exhibited the complexity, agility and global reach of al-Qaeda, with its fluid operational style based increasingly on a common mission statement and objectives, rather than on standard operating procedures and an organizational structure." *Id.* at 33.

149 "What is the Khorasan Group?", *BBC News* (24 Sept. 2014), available at http://www.bbc.com/news/world-middle-east-29350271.

150 "What is 'Islamic State'?", *BBC News* (2 Dec. 2015), available at http://www.bbc.com/news/world-middle-east-29052144; Remarks of Stephen W. Preston, "The Legal Framework for the United States' Use of Military Force Since 9/11", American Society of International Law Annual Meeting, April 10, 2015, available at https://www.defense.gov/News/Speeches/Speech-View/Article/606662/the-legal-framework-for-the-united-states-use-of-military-force-since-911.

As groups like al Qaeda or ISIS split off members to form new affiliated groups or reconstitute themselves under a new name, these changes can have ramifications for the authority of the State to act in self-defence. Is a successor group or offshoot automatically included within the State's authority to use force in self-defence, in essence as a carryover from the initial authority to respond to the original group in self-defence? Such an approach would place few, if any, limits on the breadth of the force a State can use in self-defence with respect to the groups it can attack. Alternatively, one might argue that once the potential target of State force is different in any way — by name, by composition, by location — from the original or core group, the self-defence analysis and justification needs to start anew, placing constraints on the extent of self-defence. Even if these groups "are seen as essentially pursuing a common strategy and engaging in a coordinated series of attacks originating from different locations, but forming a whole, [such that they can be treated] as a single actor and source of threat," the authority to act would then "depend upon whether in each case the requirements of necessity, proportionality, an immediacy had been met."[151]

The nascent State practice of U.S. acts and statements in the current conflict with al Qaeda and associated forces offers some fodder for analysis. The United States generally appears to take a case-by-case approach, looking for direct linkage between the successor or splinter group and core al Qaeda, but then applying the full extent of its self-defence authority once it identifies that linkage. With respect to AQAP, the United States argues that the 2001 AUMF applies to AQAP either as part of al Qaeda or as an associated force,[152] but without any further clarification or delineation. For other groups, such as al Qaeda in the Islamic Maghreb or al Shabaab, the United States has asserted self-defence authority but has not explained whether that self-defence authority is the same as that justifying operations against al Qaeda or is a separate set of authorities.[153] A speech by the then-General Counsel of the Department of Defense offers a window in the United States' thinking in this regard, however. After explaining that the United States' operations against ISIS stem from the same self-defence

[151] Gill, *supra* note 115 at 748.

[152] *See al-Aulaqi v. Obama*, 727 F. Supp. 2d 1 (D.D.C. 2010) (Opposition to Plaintiff's Motion for a Preliminary Injunction and Memorandum of the United States in Support of Defendants' Motion To Dismiss at 1) ("The United States has further determined that AQAP is an organized armed group that is either part of al-Qaeda, or is an associated force, or cobelligerent, of al-Qaeda.").

[153] *See* J. Daskal & S. I. Vladeck, "After the AUMF", 5 *Harv. Nat'l Sec. J.* 115, 123-26 (2014).

authority as those against al Qaeda, because of the original linkages between the two groups, the General Counsel then provided clues as to the limits of self-defence authority passed along to a group's successors or offshoots:

> The name may have changed, but the group we call ISIL today has been an enemy of the United States within the scope of the 2001 AUMF continuously since at least 2004. A power struggle may have broken out within bin Laden's jihadist movement, but this same enemy of the United States continues to plot and carry out violent attacks against us to this day. Viewed in this light, reliance on the AUMF for counter-ISIL operations is hardly an expansion of authority. After all, how many new terrorist groups have, by virtue of this reading of the statute, been determined to be among the groups against which military force may be used? The answer is zero.[154]

In contrast, he noted, it would be a "different conversation if ISIL had emerged out of nowhere a year ago, having no history with bin Laden and no more connection to current al-Qa'ida leadership than it has today."[155]

For the United States, therefore, the constraint for the extent of force in self-defence lies in the identification of which groups qualify as successors or offshoots, as opposed to new groups. This is a constraint that, at least preliminarily, protects against the valid concern that a State's response to one terrorist group's attack can quickly become a "war against terrorism" or "global war on terror" with no limits on where or against whom the state can act. However, the constraint only works to the degree that the analysis of the relevant linkages is discriminating; a State that easily finds a successor or offshoot in every terrorist group is merely paying lip service to the role that necessity and proportionality must play in determining the extent of force it can use against terrorist groups. Furthermore, it is not clear whether the United States treats the successor or offshoot connection as the only inquiry required — meaning that once that connection is made, no new or further necessity and proportionality analysis is necessary — or whether the United States freshly examines the need for forceful measures against each successor or offshoot and the reasonableness of the degree of force used.

The former methodology appears to rest on the determination that force against a successor or offshoot group is included within the self-defence aims of preventing future attacks from the original group or defeating the

[154] Remarks of Stephen Preston, *supra* note 150.
[155] *Id*.

original group, for example. This approach seems to borrow from a more conventional environment — in which military forces, militia and other fighting units belonging to a party to a conflict are presumed to be fighting for and answering to the same sovereign entity and its military leaders — and using it to make sense of the complex, rapidly changing, and uncertain world of transnational terrorism. Viewing self-defence against a terrorist group as an armed conflict makes this association of threat, necessity and proportionality both possible and justifiable, at least from the State's perspective. However, it poses a significant risk of relaxing the foundational requirements both for triggering the right of self-defence and for determining the extent of force the state can then use in carrying out that right, thus weakening the international legal prohibition on the use of force. The better approach, therefore, is to consider necessity and proportionality mandatory requirements for the use of force in self-defence against successors and offshoots, recognizing that the nature of such groups and the intelligence and threat assessments the State has made may well make such analyses quite simple and obvious. Requiring that step preserves the essential international legal infrastructure.

C. New Groups and New Allegiances

Finally, it is now common for the primary terrorist group in conflict with a State to inspire new groups and individuals to join that violent struggle and to motivate existing groups to pledge allegiance to the primary group and its leaders. Although this expanding network, as it were, is partly a response to the group's success in its initial attacks, it is also a direct effect of the State's initial success in countering the group's attacks and threat. The United States 2011 National Strategy for Counterterrorism explains that, "precisely because its leadership is under such pressure in Afghanistan and Pakistan, al Qaeda has increasingly sought to inspire others to commit attacks in its name."[156] As a result, where "al-Qa'ida has had some success in rallying individuals and other militant groups to its cause, . . . the United States faces an evolving threat from groups and individuals that accept al-Qa'ida's agenda, whether through formal alliance, loose affiliation, or mere inspiration."[157] Both al Qaeda and ISIS have sought and secured pledges of allegiance from other terrorist groups, whether for operational or rhetorical effect. Al Shabaab pledged allegiance to al Qaeda in 2009 and remains closely tied to al Qaeda, with its leader receiving training from and fighting

[156] President of the United States, National Strategy for Counterterrorism 4 (June 2011), available at https://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.
[157] *Id*. at 3.

with al Qaeda in Afghanistan[158] and al Qaeda operatives regularly noted as collaborating with al Shabaab in Somalia.[159] Over forty groups are believed to have pledged allegiance to ISIS, including Boko Haram in Nigeria and Abu Sayyaf in the Philippines, for example.[160]

As the original terrorist group secures adherents or affiliates, the parameters of the original self-defence authority are tested. For groups inspired by the main terrorist group, whether al Qaeda or ISIS or any other, but not connected operationally in any way, extending the authority to act in self-defence is a stretch indeed. However, that is not the key question here, because few would argue that a group inspired by al Qaeda but not involved in any attacks on the United States or participating directly with al Qaeda in planning or launching operations meets the test for triggering a right of self-defence. Rather, the question for the instant discussion is whether, in order to defeat al Qaeda or prevent future attacks from al Qaeda, force against these inspired but as yet unconnected groups is necessary and proportionate to *that* goal. On first glance, that appears to be a proposition that is quite difficult to support under any interpretation of necessity and proportionality as set forth above. But to the extent that the United States redefines, or even potentially redefines, its conflict with and basic objectives in combatting al Qaeda, the door opens at least a crack.

Descriptions of the shifting nature of al Qaeda and the changing United States framing of its efforts against al Qaeda offer some insight. First, al Qaeda no longer resembles its 2001 incarnation, but "has evolved into an increasingly diffuse network of affiliated groups, driven by the worldview that al-Qaeda represents."[161] Over time, it has therefore "begun to resemble more closely a 'global jihad movement', increasingly consisting of web-directed and cyber-linked groups and ad hoc cells."[162] As the United States

[158] C. Gaffey, "Why Al-Shabab is Not Joining ISIS", *Newsweek* (22 Jan. 2016), available at http://www.newsweek.com/al-shabab-not-joining-isis-418656.

[159] T. Gibbons-Neff, "Pentagon: Drone Strike Targets Senior al-Shabab Leader in Somalia", *Chi. Trib.* (1 June 2016), available at http://www.chicagotribune.com/news/nationworld/ct-drone-strike-al-shabab-somalia-20160601-story.html.

[160] P. Boghani, "Where the Black Flag of ISIS Flies: A Look at the Nine Countries Where the Terror Groups has Formal Affiliates", *Frontline* (13 May 2016), available at http://apps.frontline.org/isis-affiliates/.

[161] Cronin, *supra* note 94, at 32.

[162] *Id.* at 33 (noting that in the process of its evolution, "al-Qaeda has demonstrated an unusual resilience and international reach"). The U.S. National Strategy for Counterterrorism affixes the label "adherents" to some of these groups: "Individuals who have formed collaborative relationships with, act on behalf of, or are otherwise inspired to take action in furtherance of the goals of al-Qa'ida—the organization and the ideology—including by engaging in violence regardless of whether such violence is targeted at the

shifts its focus accordingly — to preventing the spread of radical Islamic extremism and eliminating opportunities for extremist groups to terrorize local populations as a stepping stone to a more global reach — it is important to consider to what extent force is necessary to achieving these objectives. One former National Security Council official described "winning against al Qaeda" as looking

> very much like victories against other insurgents: the spreading of security for populations in Somalia, Yemen, the Sahel, and elsewhere; the prevention of a return of al-Qaeda to those cleared areas; and the empowerment of legitimate governments that can control and police their own territories. By these standards, we have not yet defeated al Qaeda; in fact, beyond Iraq, Afghanistan, and Somalia, we have hardly engaged the enemy at all.[163]

Here it is essential, in order to preserve the purpose of necessity and proportionality as constraints on the use of force in self-defence, to separate the various components of this strategy against al Qaeda and isolate those that require force rather than law enforcement, education, propaganda or other non-forceful measures. Doing so protects against the danger of the self-defence authority being applied to any efforts at all to "stop al Qaeda" and therefore spreading the authority to use force.

With regard to groups that pledge allegiance to al Qaeda or ISIS, the analysis is more complex. Our traditional understanding of how a third State becomes a party to a conflict does not necessarily translate to the murky world of terrorist groups, and ideological affiliation or allegiance. To the extent that a new group "joins the fight" and actually participates in attacks or other military operations against the state, the inclusion of that group in the State's self-defence authority, or in the armed conflict where the appropriate framework, may well be appropriate. The United States uses the concept of "associated forces" to denote such groups.[164] This extension of self-defence authority under both international law and United States domestic law has been thoroughly debated. However, this debate has not

---

United States, its citizens, or its interests." National Strategy for Counterterrorism, *supra* note 157, at 3.

[163] M. Habeck, "Can We Declare the War on al Qaeda Over?", *For. Pol'y* (27 June 2012).

[164] The United States uses "associated forces" as a "legal term of art that refers to cobelligerents of al-Qa'ida or the Taliban against whom the President is authorized to use force (including the authority to detain) based on the Authorization for the Use of Military Force." National Strategy for Counterterrorism, *supra* note 157, at 3 n.1. Further discussion of the meaning and scope of the term and the debate over the use and application of the concept of associated forces is outside the scope of this article.

necessarily addressed the central question raised by the instant analysis — how much force can the State use against such a group. That is, if a terrorist group pledges allegiance to ISIS and fights with it and the United States has the legitimate objective, as part of a self-defence-driven armed conflict, of defeating or destroying ISIS, does proportionate force in self-defence therefore automatically include the defeat or destruction of this other group? Or, is the extent of force against that group limited to what is necessary and proportionate to the goal of defeating ISIS, which possibly would be achieved before or separately from complete defeat of this group? Given the purpose of necessity and proportionality in preventing the spread of violence, the latter approach seems to accord more closely with these goals and be truer to the fundamental purpose of ensuring that the force used is no greater than that needed to end or prevent attacks on the State. At the same time, it matches appropriately with operational realities by not placing unreasonable or unworkable constraints on the state's ability to define threats and determine the appropriate response.

IV. CONCLUSION

In 2003, then Major General David Petraeus famously said to a reporter interviewing him about the war in Iraq: "Tell me how this ends."[165] Although his quip foretold the complications to come in Iraq and exposed skepticism about U.S. prospects in the absence of long-term planning for after the invasion, the question sums up the challenges of analyzing the execution of the right of self-defence against a terrorist group. Effectively assessing necessity and proportionality to judge the lawfulness of force in self-defence rests on the legitimate objective the State seeks to achieve and how the force used relates to that objective. In turn, the legitimate objective requires — or certainly should require — a firm grasp of what success means and looks like and, equally important, why force is needed to achieve that success and the amount or nature of the force needed to reach that result. Terrorism inherently muddies those waters and, somewhat inevitably, leads to a "we'll know it when we see it" characterization of success — the State's leaders can proclaim that they will have success when they degrade or destroy or dismantle the terrorist group or its operational capacity, but there is no way to quantify or describe what that end result looks like either, even though it sounds more specific.

The current jurisprudence and discourse on the international law of self-defence provides the necessary tools for analyzing when a State may resort to force in self-defence against an armed attack or imminent armed attack by

[165] R. Atkinson, "Iraq Will Be Petraeus's Knot to Untie", *Wash. Post* (7 Jan. 2007).

a terrorist group. Furthermore, it is axiomatic that, to be lawful, that use of force in self-defence must be necessary and proportionate to the objective of ending or repelling the attack. But when matched up against the complexities and particularities of counterterrorism operations, whether purely self-defence or in the context of armed conflict, the international law framework comes up wanting. Greater understanding of and detail about the objectives to be attained by using force in self-defence is essential. In particular, effective application of the law depends on further analysis and exploration of how the classic international law notions of ending or repelling an attack or imminent attack match up with the operational conceptions of degrading, defeating, or destroying a terrorist group. The idiosyncrasies of terrorism and counterterrorism also demonstrate that understanding and analyzing necessity and proportionality must be dynamic, because terrorist groups are fluid and agile and ever-changing and counterterrorism operations must be as well. Ultimately, the extent of the use of force in self-defence against terrorist groups leads to a modification of General Petraeus's question: "Tell me how this ends, so we can see what you need to do and how you can lawfully get there."

ARTICLES

THE FUTURE OF THE LAW OF ARMED CONFLICT: OSTRICHES, BUTTERFLIES, AND NANOBOTS

*Eric Talbot Jensen**

INTRODUCTION

Increasingly, we find ourselves addressing twenty-first century challenges with twentieth-century laws.[1]

As Louise Doswald-Beck correctly stated in her 1998 article, "[a]ny attempt to look into the future is fraught with difficulty and the likelihood

* Associate Professor, Brigham Young University Law School. The author spent twenty years in the U.S. military, including five as a Cavalry officer and the rest as a JAG officer, including deployments to Bosnia, Macedonia, Kosovo, and Iraq. His last job in the U.S. Army was as the Chief of International Law. He would like to thank the faculty of Brigham Young University Law School for their assistance as well as attendees at the Rocky Mountain Junior Scholars Forum. Additionally, Allison Arnold, Matthew Hadfield, Rebecca Hansen, SueAnn Johnson, Rachel LeCheminant, Brigham Udall, and Aaron Worthen provided excellent research and review assistance.

1. Harold Hongju Koh, *The State Department Legal Adviser's Office: Eight Decades in Peace and War*, 100 GEO. L.J. 1747, 1772 (2012); *see also Al-Bihani v. Obama*, 590 F.3d 866, 882 (D.C. Cir. 2010) (Brown, J., concurring) ("War is a challenge to law, and the law must adjust. It must recognize that the old wineskins of international law, domestic criminal procedure, or other prior frameworks are ill-suited to the bitter wine of this new warfare. We can no longer afford diffidence. This war has placed us not just at, but already past the leading edge of a new and frightening paradigm, one that demands new rules be written. Falling back on the comfort of prior practices supplies only illusory comfort.").

that much of it will be wrong."[2] This, in part, accounts for the military axiom that a nation is always preparing to fight the last war. In a study about future war, military historian and theorist Thomas Mackubin writes that research has shown "the United States has suffered a major strategic surprise on the average of once a decade since 1940."[3]

If this inherent lag is true about the tactics and strategy of fighting wars, it is even more true concerning the law governing the fighting of wars. Michael Reisman writes that, "[b]ecause modern specialists in violence constantly seek new and unexpected ways of defeating adversaries, the codified body of the law of armed conflict always lags at least a generation behind."[4] This law lag was recently illustrated by those who have argued for new laws to govern the post–9/11 armed conflict paradigm.[5]

The historical fact that the law of armed conflict (LOAC) has always lagged behind current methods of warfare does not mean that it always must. This Article will argue that the underlying assumption that law must be reactive is not an intrinsic reality inherent in effective armed conflict governance. Rather, just as military practitioners work steadily to predict new threats and defend against them, LOAC practitioners need to focus on the future of armed conflict and attempt to be proactive in evolving the law to meet future needs.

In a recent article in *The Atlantic*, authors Andrew Hessel, Marc Goodman, and Steven Kotler propose a hypothetical in the year 2016 where an anonymous web personality known as Cap'n Capsid posts a competition to deliver a specific virus that, unbeknownst to the competitors, is linked to the DNA of the President of the United States. The virus eventually makes its way to Samantha, a sophomore majoring in govern-

---

2. Louise Doswald-Beck, *Implementation of International Humanitarian Law in Future Wars*, *in* 71 INT'L L. STUD., THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM 39, 39 (1998); Stephen Peter Rosen, *The Future of War and the American Military*, HARV. MAG., May-June 2002, at 29, 29 ("The people who run the American military have to be futurists, whether they want to be or not. The process of developing and building new weapons takes decades, as does the process of recruiting and training new military officers. As a result, when taking such steps, leaders are making statements, implicitly or explicitly, about what they think will be useful many years in the future."). Despite the difficulty, it is a vital requirement of militaries and one in which plenty of people are still willing to engage. *See* Frank Jacobs & Parag Khanna, *The New World*, N.Y. TIMES (Sep. 22, 2012), www.nytimes.com/interactive/2012/09/23/opinion/sunday/the-new-world.html.

3. Mackubin Thomas Owens, *Reflections on Future War*, NAVAL WAR C. REV., Summer 2008, at 61, 64.

4. W. Michael Reisman, Rasul v. Bush*: A Failure to Apply International Law*, 2 J. INT'L CRIM. JUST. 973, 973 (2004).

5. *See* NEW WARS, NEW LAWS? APPLYING THE LAWS OF WAR IN 21ST CENTURY CONFLICTS (David Wippman & Matthew Evangelista eds., 2005); Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675 (2004); Geoffrey S. Corn, *Hamdan, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict*, 40 VAND. J. TRANSNAT'L L. 295 (2007); Roy S. Schondorf, *Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?*, 37 N.Y.U. J. INT'L L. & POL. 1 (2004); Robert D. Sloane, *Prologue to a Voluntarist War Convention*, 106 MICH. L. REV. 443 (2007).

ment at Harvard University, who ingests it and comes down with the flu. Given her symptoms, she quickly spreads billions of virus particles, infecting many of her college friends who also get flu-like symptoms, but nothing very harmful.

> This would change when the virus crossed paths with cells containing a very specific DNA sequence, a sequence that would act as a molecular key to unlock secondary functions that were not so benign. This secondary sequence would trigger a fast-acting neurodestructive disease that produced memory loss and, eventually, death. The only person in the world with this DNA sequence was the president of the United States, who was scheduled to speak at Harvard's Kennedy School of Government later that week. Sure, thousands of people on campus would be sniffling, but the Secret Service probably wouldn't think anything was amiss. It was December, after all—cold-and-flu season.[6]

This scenario may sound more like science fiction than like something you would read in a law review article. However, events like this seem inevitable as the technology of war progresses. Such events raise numerous legal issues both about the law of going to war, or *jus ad bellum*, and the LOAC, or *jus in bello*. Would this be considered a "use of force" in violation of the U.N. Charter?[7] In relation to *jus ad bellum*, would it be considered an "armed attack," giving the United States the right to exercise self-defense?[8] How would these answers be affected if Cap'n Capsid were not a state actor, but a terrorist or an individual acting on his own? With respect to the *jus in bello*, was this an attack, triggering the LOAC? If so, did it violate the principles of distinction or discrimination?[9] Is a genetically coded virus a lawful weapon?

---

6. Andrew Hessel, Marc Goodman & Steven Kotler, *Hacking the President's DNA*, THE ATLANTIC (Oct. 24, 2012, 10:42 AM), http://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/.

7. U.N. Charter art. 2, para. 4. Article 2, paragraph 4 has become the accepted paradigm restricting the use of force among states. Actions that amount to a threat or use of force are considered a violation of international law. However, the international community has very different views on what the language actually means and the Charter contains no definitions.

8. U.N. Charter art. 51. The definition of armed attack is controversial. There is no agreed definition of what equates to an armed attack. Despite this lack of clarity, states seem to agree that not all armed military actions equate to an armed attack. The ICJ confirmed this in the Nicaragua case when it decided that Nicaragua's provision of arms to the opposition in El Salvador was not an armed attack. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 195 (June 27). Additionally, there are unresolved questions about the application of new technologies, such as cyber operations, to armed attack. It is still unclear what level of offensive cyber operations against a state will constitute an armed attack.

9. *See infra*, section II.C.2.b. The principle of distinction requires militaries to distinguish between civilians and combatants in the attack. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

Technological development in each of the areas highlighted in the scenario mentioned above is proceeding quickly, and not just in the United States but also amongst nations throughout the world. While much of the development is currently for peaceful purposes, there is no doubt that many, if not all, of these advances will be weaponized over time. Historically, few technologies throughout history that can be weaponized have not been.[10]

P.W. Singer, known scholar on advancing technologies and the law, has recently written,

> Are we going to let the fact that these [new technologies] look like science fiction, sound like science fiction, feel like science fiction, keep us in denial that these are battlefield reality? Are we going to be like a previous generation that looked at another science fiction-like technology, the atomic bomb? The name "atomic bomb" and the concept come from an H.G. Wells short story. Indeed, the very concept of the nuclear chain reaction also came from that same sci-fi short story. Are we going to be like that past generation that looked at this stuff and said, "We don't have to wrestle with all the moral, social, and ethical issues that come out of it until after Pandora's box is open?"[11]

Pandora's box is opening as new technologies are being developed. They will inevitably shape the future battlefield, affecting where conflicts are fought, by whom they are fought, and the means and methods used to fight.

The premise of this Article is that we are at a point in history where we can see into the future of armed conflict and discern some obvious points where future technologies and developments are going to stress the current LOAC. While the current LOAC will be sufficient to regulate the majority of future conflicts, we must respond to these discernible issues by anticipating how to evolve the LOAC in an effort to bring these future weapons under control of the law, rather than have them used with devastating effect before the lagging law can react.

Part I of this article will argue that the LOAC plays a vital signaling role in warfare that is especially needed at this time of technological innovation. Like these changing technologies, the LOAC must also evolve to face the new challenges of future armed conflict. Part II will project armed conflict into the future in three main categories—places, actors, and means and methods—and analyze how advancing technologies and techniques

---

The principle of discrimination requires each specific attack, including each weapon system, to be able to differentiate in the attack and only attack intended targets. *Id.*, art. 57.

10. John D. Banusiewicz, *Lynn Outlines New Cybersecurity Effort*, U.S. DEP'T OF ST. (June 16, 2011), http://www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/news/newsarticle.aspx?id=64349.

11. P.W. Singer, Ethical Implications of Military Robotics, The 2009 William C. Stutt Ethics Lecture, United States Naval Academy (Mar. 25, 2009), *available at* http://www.au.af.mil/au/awc/awcgate/navy/usna_singer_robot_ethics.pdf.

will call into question the current LOAC's ability to adequately regulate armed conflict. This Part will identify specific principles of the LOAC, the effectiveness of which will wane in the face of state practice, and suggest emerging concepts that will allow the LOAC to evolve and maintain its relevance and virulence in armed conflict. The Article will then conclude.

I. OSTRICHES OR BUTTERFLIES

Warfare has always been an evolving concept. Throughout history, it has constantly been shaped and altered by the exigencies of nations and the moral sentiments of the global community. Yet, the paramount force behind this continual military evolution is not economic, social, or moral; rather, the greatest controlling factor has been the ever-changing limitations of wartime technology. . . . For centuries, nations have searched for and sought ways to utilize technological advancements to overcome material deficiencies.[12]

We have all heard or read about how, when faced with danger or adversity, the ostrich buries its head in the sand, hoping the bad thing will pass and leave it unharmed. While this is a myth,[13] it is also a powerful metaphor to describe a possible reaction to a threat. Compare that mythical reaction of the ostrich with the theory of the "coevolutionary arms race"[14] in plants and animals, where a change in the genetic composition of one species is in response to a genetic change in another.[15] For example, over time, the Heliconius butterfly has co-evolved with the passion vine through a series of changes and counter-changes that now link the two inextricably together. As the passion vine developed toxins to protect itself from overfeeding, the Heliconius developed the ability to internalize the toxin and then use it as a defense against its own predators. Similarly, while the Heliconius feeds on the passion vine, it also fertilizes the vine, ensuring the vine's survival.[16]

The natural phenomenon of the co-evolutionary arms race between species is instructive in considering the LOAC and its relationship with

12. Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 603 (2011).

13. Karl S. Kruszelnicki, *Ostrich Head in Sand*, ABC SCIENCE (Nov. 2, 2006), http://www.abc.net.au/science/articles/2006/11/02/1777947.htm.

14. Richard Dawkins & John R. Krebs, *Arms Races Between and Within Species*, 205 PROC. ROYAL SOC'Y LONDON, SERIES B, BIOLOGICAL SCIENCES 489 (1979); Interview with Charles Riley Nelson, Professor, Department of Biology, Brigham Young University, in Provo, Utah (Dec. 20, 2012).

15. Paul R. Ehrlich & Peter H. Raven, *Butterflies and Plants: A Study in Coevolution*, 18 EVOLUTION 586 (1964); Daniel H. Janzen, *When is it Coevolution?*, 34 EVOLUTION 611 (1980); John N. Thompson, *Concepts of Coevolution*, 4 TRENDS ECOLOGY & EVOLUTION 179 (1989).

16. Interview with Charles Riley Nelson, Professor, Department of Biology, Brigham Young University, in Provo, Utah (Dec. 20, 2012) (explaining coevolutionary analysis using the example of the Heliconius and passion vine); *see also* Lawrence E. Gilbert, *The Coevolution of a Butterfly and a Vine*, 247 SCI. AM., Aug. 1982, at 110 (describing how species of Heliconius and passion vine have influenced each other's evolution).

advancing technology. In response to advancing technologies that will undoubtedly affect the conduct of hostilities on the future battlefield, the LOAC can play the role of the ostrich and stick its head in the sand by saying that the current rules are sufficient and all technologies must mold themselves to current rules or not be used. Alternatively, the LOAC can play the role of the butterfly and respond to future developments (or even anticipate them) and adapt or evolve sufficiently to regulate these developments in a meaningful way.

A. *Evolution*

Predicting the future is very difficult,[17] and fraught with the potential for serious error. Hence, the law of armed conflict has been mostly reactive throughout its history. The Fourth Geneva Convention of 1949[18] concerning the protection of civilians during armed conflicts did not come about until after the devastating attacks on civilians that occurred in World War II.[19] Likewise, the Additional Protocols of 1977[20] did not extend protections to victims of non-international armed conflict until decades of lobbying by the International Committee of the Red Cross (ICRC).[21]

The ICRC is engaged in a similar work now. During the recent sixty-year commemoration of the 1949 Geneva Conventions, the ICRC reported on a number of concerns looking at current and future armed conflicts where the law may need to evolve in order to address the needs of victims of armed conflict.[22] Most of these suggestions are based on reactions to current conflicts, but they clearly denote that the international community cannot take the "ostrich's" approach to impending problems. If the law is going to maintain its relevance and ability to adequately regu-

17. Katie Drummond, *Defense Whiz to Pentagon: Your Predictions are Destined to Fail*, WIRED (Oct. 28, 2011, 2:54 PM), http://www.wired.com/dangerroom/2011/10/danzig-military-predictions/ ("The U.S. government has a perfectly awful track record of predicting future events. And there's a good reason why, says the chairman of an influential think tank: it's friggin' impossible.").

18. Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention].

19. See *Civilians protected under international humanitarian law*, INT'L COMM. RED CROSS (Oct. 29, 2010), http://www.icrc.org/eng/war-and-law/protected-persons/civilians/overview-civilians-protected.htm.

20. Protocol I, *supra* note 9, art. 43, para. 2; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Protocol II].

21. Eric Talbot Jensen, *Applying a Sovereign Agency Theory of the Law of Armed Conflict*, 12 CHI. J. INT'L L. 685, 693–94 (2012).

22. Jakob Kellenberger, President, Int'l Comm. Red Cross, Sixty Years of the Geneva Conventions: Learning from the Past to Better Face the Future, Address at Ceremony to celebrate the 60th anniversary of the Geneva Conventions, (Aug. 12, 2009), *available at* http://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-president-120809.htm.

late armed conflict, it must take the "butterfly's" approach and be adaptive and able to evolve in the face of difficulties.[23]

Employing the ostrich's approach and failing to infuse flexibility and adaptability into the LOAC will lead to an increase in the recent phenomenon known as lawfare, or "the use of law as a weapon of war."[24] Recent examples of this phenomenon abound[25] and many LOAC scholars argue that the current LOAC regime in fact encourages non-compliance and incentivizes fighters to use the LOAC as a shield to give them an advantage when fighting LOAC-compliant forces.[26]

---

23. *See* Kenneth Anderson & Matthew Waxman, *Law and Ethics for Robot Soldiers*, POL'Y REV. (Dec. 1, 2012), http://www.hoover.org/publications/policy-review/article/135336 (making a similar argument very effectively with respect to autonomous weapon systems); Louise Arbour, *10 Conflicts to Watch in 2013*, FOREIGN POLICY (Dec. 27, 2012), http://www.foreignpolicy.com/articles/2012/12/27/10_conflicts_to_watch_in_2013 (pointing to the principles of distinction between civilians and combatants and collateral damage from advanced technology as two pressures on the LOAC). *But see* Brad Allenby & Carolyn Mattick, *Why We Need New Rules of War*, SLATE (Nov. 12, 2012), http://www.slate.com/articles/technology/future_tense/2012/11/drones_cyberconflict_and_other_military_technologies_require_we_rewrite.html.

24. *See* Charles J. Dunlap, Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts*, HARVARD PROGRAM ON NATIONAL SECURITY AND HUMAN RIGHTS, WORKSHOP PAPERS: "HUMANITARIAN CHALLENGES IN MILITARY INTERVENTION" 4, 5 (2001), *available at* http://www.ksg.harvard.edu/cchrp/Web%20Working%20Papers/Use%20of%20Force/Dunlap2001.pdf; MICHAEL N. SCHMITT, THE IMPACT OF HIGH AND LOW-TECH WARFARE ON THE PRINCIPLE OF DISTINCTION, HARVARD PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, INT'L HUMANITARIAN LAW RESEARCH INITIATIVE BRIEFING PAPER, 1, 7 (November 2003), *reprinted in* INTERNATIONAL HUMANITARIAN LAW AND THE 21ST CENTURY'S CONFLICTS: CHANGES AND CHALLENGES (Roberta Arnold & Pierre-Antoine Hildbrand eds., 2005).

25. The recent war in Iraq illustrates many examples. Tony Perry & Rick Loomis, *Mosque Targeted in Fallouja Fighting*, L.A. TIMES (Apr. 27, 2004), http://articles.latimes.com/print/2004/apr/27/world/fg-fallouja27 (attacking from protected places and using them as weapons storage sites); *Coalition Forces Continue Advance Toward Baghdad*, CNN (Mar. 24, 2003), http://transcripts.cnn.com/TRANSCRIPTS/0303/24/se.17.html (fighting without wearing a proper uniform); *The Rules of War are Foreign to Saddam*, OTTAWA CITIZEN, Mar. 25, 2003, *available at* LEXIS, Nexis Library, CURNWS File (using human shields to protect military targets); David Blair, *Human Shields Disillusioned with Saddam, Leave Iraq after Dubious Postings*, NATIONAL POST (Canada), Mar. 4, 2003, at A1, *available at* LEXIS, Nexis Library, CURNWS File (same); David B. Rivkin, Jr. & Lee A. Casey, *Leashing the Dogs of War*, NAT'L INT. (Sept. 1, 2003), http://nationalinterest.org/article/leashing-the-dogs-of-war-1120) (using protected symbols to gain military advantage); *South Korean Hostage Beheaded in Iraq*, TORONTO STAR, June 23, 2004, *available at* LEXIS, Nexis Library, CURNWS File (murdering prisoners or others who deserve protection); *see also* Michael Sirak, *Legal Armed Conflict*, JANE'S DEF. WKLY, Jan. 14, 2004, at 27 (listing a number of violations of the law of war committed by Iraqi military and paramilitary forces). In each of these cases, an inferior force used the superior force's commitment to adhere to the law of war to their tactical advantage.

26. *See, e.g.*, Dunlap, *supra* note 24, at 6 ("[T]here is disturbing evidence that the rule of law is being hijacked into just another way of fighting (lawfare), to the detriment of humanitarian values as well as the law itself."); Owens, *supra* note 3, at 70 ("Thus these enemies will try to leverage 'lawfare,' the use of the rules of warfare against the United States (while ignoring these rules themselves), by, for example, taking refuge among the civilian population in an attempt to maximize civilian casualties. In turn, adversaries employing complex

Much of the recent lawfare discussion has centered on backward military opponents or non-state actors who need to use lawfare to overcome asymmetric disadvantages.[27] However, a static and inflexible LOAC will incentivize even developed and powerful nations to use the law as a tool, rather than as a regulator. The Chinese already write of "three warfares" including "legal warfare," which is defined as "arguing that one's own side is obeying the law, criticizing the other side for violating the law, and making arguments for one's own side in cases where there are also violations of the law."[28] This Chinese view portrays the law generally "as a means of enforcing societal (and state) control of the population."[29] Presumably, this would apply to both domestic and international law.

China is, of course, not alone in potentially using lawfare to gain an edge through future technologies. The United States has come under heavy criticism recently for its use of drones in fighting transnational terrorism.[30] Though U.S. and Chinese perspectives on the law may be different,[31] the danger of a static and inflexible approach to the LOAC as future technologies emerge is equally applicable to developed and undeveloped,

---

irregular warfare will take advantage of the fact that such casualties are magnified by the proliferation of media assets on the battlefield."); Jason Vest, *Fourth-Generation Warfare*, THE ATLANTIC (Dec. 1, 2001), http://www.theatlantic.com/magazine/archive/2001/12/fourth-generation-warfare/302368/ (discussing Fourth-generation Warfare which includes a recognition of asymmetric operations "in which a vast mismatch exists between the resources and philosophies of the combatants, and in which the emphasis is on bypassing an opposing military force and striking directly at cultural, political, or population targets").

27. The Council on Foreign Relations has defined lawfare as "a strategy of using or misusing law as a substitute for traditional military means to achieve military objectives." *See* Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F.L. REV. 1, 78 (2005); *Lawfare, the Latest in Assymetries*, COUNCIL ON FOREIGN REL. (Mar. 18, 2003), http://www.cfr.org/publication.html?id=5772.

28. Dean Cheng, *Winning Without Fighting: Chinese Legal Warfare*, HERITAGE FOUND. (May 21, 2012) http://www.heritage.org/research/reports/2012/05/winning-without-fighting-chinese-legal-warfare.

29. *Id.* The report also states "[n]o strong tradition that held the law as a means of constraining authority itself ever developed in China." *Id.* at 3.

30. Chris Jenks, *Law from Above: Unmanned Aerial Systems, Use of Force, and the Law of Armed Conflict*, 85 N.D. L. REV. 649, 651 (2010); Thomas Michael McDonnell, *Sow What You Reap? Using Predator and Reaper Drones to Carry Out Assassinations or Targeted Killings of Suspected Islamic Terrorists*, 44 GEO. WASH. INT'L L. REV. 243, 246–47 (2012); Owen Bowcott, *UN to Examine UK and US Drone Strikes*, GUARDIAN (Jan. 23, 2013), http://www.guardian.co.uk/world/2013/jan/24/un-examine-uk-afghanistan-drone-strikes; Owen Bowcott, *UN to Investigate Civilian Deaths from U.S. Drone Strikes*, GUARDIAN (Oct. 25, 2012), http://www.guardian.co.uk/world/2012/oct/25/un-inquiry-us-drone-strikes; *see* Robert P. Barnidge, Jr., *A Qualified Defense of American Drone Attacks in Northwest Pakistan Under International Humanitarian Law*, 30 B.U. INT'L L.J. 409 (2012).

31. *See* Cheng, *supra* note 28, at 6 ("The most important strategic difference between [the United States and China] is that there is little evidence that Chinese analysts and decision-makers see legal warfare as a misuse of the law. Given the much more instrumentalist view of the law in Chinese history, the idea that the law would be employed toward a given end (in support of higher military and national goals) would be consistent with Chinese culture but problematic, if not antithetical, from the Western perspective.").

Western and non-Western nations. The international community needs to take the butterfly's approach and not that of the ostrich. It is only through being proactive and recognizing the pressures that future developments will have on the LOAC (such as where conflicts are fought, by whom they are fought, and the means and methods used to fight) that the LOAC can evolve to avoid increasing lawfare and maintain its role as regulator on the conduct of armed conflict.

B. *Signaling*

The analogy of the ostrich and the butterfly is useful to illustrate the fate of non-evolving principles in the face of a changing technological environment. Indeed, the fate of organisms is often based on their ability to understand environmental signals that are occurring around them. In this way, the analogy would seem to argue that taking a reactive approach to changing circumstances would be sufficient, especially if the reaction comes quickly. In other words, the law need not be proactive, as this Article argues, but can remain reactive, particularly if the international community decreases the reaction time and makes changes quickly in response to technological developments.

This argument might appear to be especially true in the case of international law generally, and the LOAC specifically, since they are so heavily dependent on state practice and preferences. These areas of the law develop based mainly on consensual agreements between states and also on the activities of states, particularly when done through a sense of legal obligation. These twin sources of international law are complemented by other general principles of law recognized by civilized nations such as equity, judicial decisions, and the teachings of the most highly qualified publicists.[32] As technologies develop, states will have time to consider their potential application to armed conflict and then deliberate on the best way to apply the law to changing circumstances. If nothing else, this approach will certainly maintain the maximum freedom to maneuver for states that are developing new technologies.

This approach would continue millennia of LOAC formulation where custom ripened over time. Increasing the speed with which actions ripen

---

32. See Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993 [hereinafter ICJ Statute], which states:

> 1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
>
> b. international custom, as evidence of a general practice accepted as law;
>
> c. the general principles of law recognized by civilized nations;
>
> d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

into customary international law would also be beneficial. However, relying solely on quick reaction to technological developments ignores the vital signaling role that the LOAC plays in the development of state practice.

The signaling value of the LOAC is clear from the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (GPI). Article 36 of GPI, titled "New weapons," states:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[33]

This article requires every state that is contemplating developing a new technology or weaponizing an existing technology to ensure that such development complies with the LOAC. In other words, the LOAC signals to states what is permissible and what is not even at the stage of study and development of new weapons.[34]

U.S. practice in this area is very clear. Even prior to GPI coming into effect, the United States required such a review,[35] and it is now codified in Department of Defense Directive 5000.01, which states:

> The acquisition and procurement of DoD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements (for arms control agreements, see DoD Directive 2060.1 (Reference (lm), customary international law, and the law of armed conflict (also known as the laws and customs of war). An attorney authorized to conduct such legal reviews in the Department shall conduct the legal review of the intended acquisition of weapons or weapons systems.[36]

Each military service has an attorney designated to do such reviews.[37]

---

33. Protocol I, *supra* note 9, art. 36; *cf.* Duncan Blake & Joseph S. Imburgia, *"Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons"*, 66 A.F. L. REV. 157, 159, 161 (2010) (discussing the application of legal reviews to certain future and developing weapons).

34. Neil Davison, *How International Law Adapts to New Weapons and Technologies of Warfare*, INTERCROSS BLOG (Dec. 4, 2012), http://intercrossblog.icrc.org/blog/how-international-law-adapts-new-weapons-and-technologies-warfare.

35. GEOFFREY S. CORN, ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 203 (2012).

36. Dept. of Def. Directive 5000.01, The Defense Acquisition System ¶ E1.1.15 (D.O.D. 2003) (Certified Current as of Nov. 20, 2007), *available at* http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.

37. For an example of a weapon review, see CORN, ET AL., *supra* note 35, at 228–31 (2012).

This requirement would clearly apply to all new and developing technologies that states may be considering. In such cases, the proposed weapon or means or method of warfare would be reviewed by a legal adviser who would determine its legality under the current law. In many cases, this review might be quite easy. However, it is here that Harold Koh's quote from the beginning of this Article[38] is most relevant. The legal adviser performing the review will look to the current LOAC for signals as to the legality of a proposed weapon, but that may prove difficult if the existing law does not adequately apply to the future weapon. In the absence of apparently applicable law, each legal adviser or nation is left to a discretionary decision that may lead to uneven application of LOAC constraints.

In addition to the legal review at the research and development stage, the law also requires a legal review at the point the weapon is employed. Article 82 of the same Protocol, titled "Legal Advisers in Armed Forces," states:

> The High Contracting Parties at all times, and the Parties to the conflict in time of armed conflict, shall ensure that legal advisers are available, when necessary, to advise military commanders at the appropriate level on the application of the Conventions and this Protocol and on the *appropriate* instruction to be given to the armed forces on this subject.[39]

It is clear from this provision that an otherwise lawful weapon can be employed in an unlawful way. Additionally, advanced technologies might provide tactical options that otherwise do not exist. In each case, the legal adviser must be available to the commander to provide legal advice, but the legal adviser will be looking to the LOAC for signals as to how to apply the LOAC in that specific situation. If the law is not specific to that potential employment or tactic, the legal adviser must be able to extrapolate existing rules to new technologies.

The recent development and deployment of cyber weapons demonstrates that applying existing rules to new technologies will present difficulties. Over the past decade, numerous statements and articles have been written on the application of the law to cyber operations, often coming out with different conclusions. Some have argued that existing law is sufficiently flexible to respond to new technologies such as cyber capabilities,[40]

---

38. Koh, *supra* note 1 ("Increasingly, we find ourselves addressing twenty-first century challenges with twentieth-century laws.").

39. Protocol I, *supra* note 9, art. 86 (emphasis added).

40. Michael N. Schmitt, *IHL Challenges Series—Part III on New Technologies*, INTERCROSS (June 17, 2013), http://intercrossblog.icrc.org/blog/ihl-challenges-series-part-iii-new-technologies; *cf.* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L REV. RED CROSS 533 (2012).

while others argue that a whole new set of rules should be written to provide proper guidance.[41]

In response to this ongoing debate, a group of international LOAC experts embarked on a three-year process to determine how the LOAC applied to cyber operations.[42] Headed by Michael N. Schmitt, a renowned cyber scholar,[43] the experts found that they had to interpret or evolve the law in certain areas for it to sufficiently provide guidance to cyber operators. For example, most of the experts determined that the traditional definition of "attack" was insufficient to determine when the LOAC applied to cyber activities. Instead, a cyber action that affected the functionality of a cyber system might also be considered an attack.[44]

This example is representative of similar difficulties that will occur as new technologies are developed and used. For example, in the scenario quoted from *The Atlantic* at the beginning of this article, would the employing of the virus in the proposed way violate the principle of distinction, even though it was absolutely discriminating in the attack? Similar issues will be raised below.

There is no doubt that legal advisers have been extrapolating rules to new technologies throughout history. But as will be shown below, the kinds of technological advances in weapons and tactics will be unprecedented over the next few decades, applying tremendous stresses on the LOAC. Because of the important signaling role the LOAC plays in providing guidance to states and their legal advisers, particularly during research and development, the international community needs to begin now to analyze these future weapons and tactics and proactively provide guidance on the application of the LOAC to future armed conflict.

II. THE FUTURE OF THE LAW OF ARMED CONFLICT

The nature of armed conflict, and of the causes and consequences of such conflict, is continuing to evolve. IHL must evolve too.[45]

Jakob Kellenberger's statement above, as the president of the ICRC, reflects the fundamental need to evolve IHL to the changing nature of armed conflict. The ICRC's approach is not in disagreement with that of

41. Alireza Miryousefi & Hossein Gharibi, *View from Iran: World Needs Rules on Cyberattacks*, CHRISTIAN SCIENCE MONITOR (Feb. 14, 2013), http://www.csmonitor.com/Commentary/Opinion/2013/0214/View-from-Iran-World-needs-rules-on-cyberattacks-video; Jody R. Westby, *We Need New Rules for Cyber Warfare*, N.Y. TIMES (Mar. 1, 2013), http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/we-need-new-rules-of-engagment-for-cyberwar.

42. THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 1 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. Note that the author was one of the participants in the formulation of the Manual.

43. *Michael N. Schmitt: Faculty Profile*, U.S. NAVAL WAR C., https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx (last visited Mar. 9, 2014).

44. TALLINN MANUAL, *supra* note 42, at 156–159.

45. Kellenberger, *supra* note 22.

the International Court of Justice (ICJ), as stated in the 1996 Nuclear Weapons Advisory Opinion:

> However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present, and those of the future.[46]

The assumption that the "intrinsically humanitarian character of the legal principles" of the LOAC applies to future forms of warfare does not mean that the principles cannot evolve. Rather, the decision by the ICJ that the new technology of nuclear weapons continued to be regulated by the LOAC demonstrates that the ICJ views the law as adaptive to new weapon systems even on LOAC's core fundamental principles.

Many commentators have discussed the need for change in various aspects of the laws applicable to the initiation and continuation of armed conflict,[47] including the division of international law into *jus ad bellum* and

---

46. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 259, ¶ 86 (July 8).

47. *See* Brooks, *supra* note 5, at 684 ("In the long run, the old categories and rules need to be replaced by a radically different system that better reflects the changed nature of twenty-first century conflict and threat."); Interview with Peter W. Singer, Senior Fellow, the Brookings Institute, *available at* http://www.abc.net.au/lateline/content/2012/s3442876.htm ("I think the way to think about this is that when we look at the laws of war that are set for—that are supposed to guide us today, they date from a year when the most important invention was the 45 RPM vinyl record player. We don't listen to music on vinyl record players anymore. I'm guessing a lot of the audience might never have listened to music on a vinyl record player anymore. And yet, the laws of war from that year, we still try and apply today. And so it doesn't mean that the laws of war, you know, you need to throw them out, but it does mean that they're having a real hard time."); *see also* Sylvain Charat, *Three Weapons to Fight Terror*, WASH. TIMES (Sept. 9, 2004), http://www.washingtontimes.com/news/2004/sep/8/20040908-085545-9034r/. Judge George H. Aldrich identified "those aspects of the law that are most in need of further development in the early years of the next century" for international armed conflicts as:

> (1) entitlement of those who take up arms to combatant and prisoner-of-war status;
>
> (2) protection of noncombatants from the effects of hostilities; and
>
> (3) compliance mechanisms, including external scrutiny, repression and punishment of offenses, and the right of reprisal; and
>
> in other armed conflicts—
>
> (1) the extent of regulation by international law when those conflicts are noninternational; and
>
> (2) the applicability of international law when those conflicts are partly international and partly noninternational.

jus in bello,[48] evolution of law to accommodate potential need for preemptive self-defense,[49] the bifurcation of the LOAC between international armed conflicts and non-international armed conflicts,[50] the application of the law to state and non-state actors,[51] and the geographic applicability and limitations of the LOAC to the "active conflict zone,"[52] to name just a few. P.W. Singer framed the question nicely when he asked, "[h]ow do we catch up our twentieth century laws of war that are so old right now they qualify for Medicare to these twenty-first century technologies?"[53]

The prescriptions for solving the current problem include calls for specific adjustments to discrete areas of the current LOAC, but Rosa Brooks has argued for "a radical reconceptualization of national security law and the international law of armed conflict."[54] If catching the law up to current technologies, strategies, and tactics requires a "radical reconceptualization" of the LOAC, it certainly behooves the international community to be proactive in anticipating the future evolution of the LOAC to accommodate changes in future armed conflict.

The next Part of this article will briefly analyze elements of the future battlefield, focusing on "places," or where conflicts are fought; "actors," or by whom they are fought; and "means and methods," or how they are fought. The purpose of the analysis is to highlight areas of the LOAC that will struggle to deal with the future changes that are likely to occur, and to

---

George H. Aldrich, *The Hague Peace Conferences: The Laws of War on Land*, 94 AM. J. INT'L L. 42, 42 (2000).

48. Nathaniel Berman, *Privileging Combat? Contemporary Conflict and the Legal Construction of War*, 43 COLUM. J. TRANSNAT'L L. 1 (2004); Sean D. Murphy, *Protean Jus ad Bellum*, 27 BERKELEY J. INT'L L. 22 (2009); Robert D. Sloane, *The Cost of Conflation: Preserving the Dualism of Jus ad Bellum and Jus in Bello in the Contemporary Law of War*, 34 YALE J. INT'L L. 47 (2009).

49. W. Michael Reisman, *Assessing Claims to Revise the Laws of War*, 97 AM. J. INT'L L. 82 (2003).

50. Brooks, *supra* note 5, at 711–14; Jensen, *supra* note 21; Francisco Forrest Martin, *Using International Human Rights Law for Establishing a Unified Use of Force Rule in the Law of Armed Conflict*, 64 SASK. L. REV. 347 (2001); Gabor Rona, *Legal Frameworks to Combat Terrorism: An Abundant Inventory of Existing Tools*, 5 CHI. J. INT'L L. 499 (2005).

51. Kenneth Watkin, *Canada/United States Military Interoperability and Humanitarian Law Issues: Land Mines, Terrorism, Military Objectives, and Targeted Killing*, 15 DUKE J. COMP. & -INT'L L. 281, 281 (2005) ("The conduct of military operations at the commencement of the 21st century has also shone a bright spotlight on traditional tensions in humanitarian law, such as the application of that law to conflicts between state and non-state actors.").

52. Jennifer C. Daskal, *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the 'Hot' Conflict Zone*, 161 U. PA. L. REV. 1165, 1212; Frédéric Mégret, *War and the Vanishing Battlefield*, 9 LOY. U. CHI. INT'L L. REV. 131 (2011).

53. Singer, *supra* note 11.

54. Brooks, *supra* note 5, at 747. The author further states that "it is becoming more and more difficult to know how to characterize, as a matter of law, the kinds of threats that increasingly face the U.S. and other nations, and it is therefore becoming harder and harder to determine the appropriate legal responses to these threats. The old categories have lost their analytical and moral underpinnings, but we have not yet found alternative paradigms to replace them." *Id.* at 744.

begin a discussion on how the LOAC needs to evolve to maintain its ability to regulate armed conflict in the future.

A. *Places*

The traditional paradigm of armed conflict assumes that at any given time, it will be readily apparent where the armed conflict is taking place, and where it is not. To put it another way, the traditional paradigm assumes clear spatial boundaries between zones of war and zones of peace.[55]

For the entire history of mankind, armed conflict has been confined to breathable air zones—the land, the surface of the ocean, and recently the air above the land in which land-based aircraft can fly. Additionally, the post-Westphalian system was built on the foundation of state sovereignty and the clear demarcation and control of borders.[56] Armed conflicts occurred within specific spatial and temporal limits. As a result, the laws governing armed conflict have been built around certain presumptions about where armed conflict will occur. In the future, these presumptions will no longer be true. The LOAC will have to adjust to account for the emerging factors affecting where armed conflicts take place.

1. Emerging Factors

As technology advances, armed conflict will no longer be restricted to breathable air zones. Instead, it will occur without respect to national borders, underground, on the seabed, in space and on celestial bodies such as the moon, and across the newly recognized domain of cyberspace.[57]

a. Global Conflict

The phenomena of global conflict has already begun to stress the LOAC[58] as the United States has struggled to confront a transnational non-state terrorist actor that does not associate itself with geographic boundaries. As will be discussed in Subsection B, the ability to communicate globally through social media will likely produce organized (armed) groups that will not be bound by geographic boundaries and as such will not see themselves as representing a specific geographic collective. Rather, the boundaries will revolve around affiliations, interests, and ideologies. As Mack Owens has written:

> Thus multidimensional war in the future is likely to be characterized by distributed, weakly connected battlefields; unavoidable urban battles and unavoidable collateral damage exploited by the

55. *Id.* at 720.

56. Jensen, *supra* note 21, at 707–09.

57. *See* David Alexander, *Pentagon to Treat Cyberspace as "Operational Domain"*, REUTERS (Jul. 14, 2011), http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

58. Mégret, *supra* note 52, at 132 (arguing that the "death of the battlefield significantly complicates the waging of war and may well herald the end of the laws of war as a way to regulate violence").

> adversary's strategic communication; and highly vulnerable rear areas. On such battlefields, friends and enemies are commingled, and there is a constant battle for the loyalty of the population.[59]

This issue is amply illustrated through the U.S. practice of drone strikes on terrorists associated with al-Qaeda but not located in Afghanistan.[60] The focused outcry about U.S. reliance on authorities granted by the law of armed conflict even though outside the geographic confines of the recognized battlefield[61] highlights the current paradigm's assumptions about the LOAC's applications to territory. As global communications allow participants in armed conflict to be more widely dispersed across the world, it is unlikely that states will allow themselves to be attacked by transnational actors because they are not located within a specific geographic region that has been designated as the "battlefield."

b. Seabed

Currently the seabed and even non-surface waters have seen very little armed conflict.[62] Submarine vessels have engaged surface vessels but there has been almost no conflict between submarines and none from the seabed. This is likely to change dramatically with technological improvements. For example, China has developed submersibles that can reach 99.8 percent of world's seabed.[63] As more and more underwater vehicles become unmanned, the need for breathable air dissipates. Underwater drones will almost certainly become armed and underwater engagements will quickly follow.

Similarly, the seabed will likely become militarized, once the need for air is erased. Not only could sensors be used to track surface and subsurface traffic, but also armaments will likely soon follow and the seabed will become another area where states will employ weapons systems.

---

59. Owens, *supra* note 3, at 71.

60. Cora Currier, *Everything We Know So Far About Drone Strikes*, PROPUBLICA (Jan. 22, 2013), http://www.propublica.org/article/everything-we-know-so-far-about-drone-strikes.

61. Daskal, *supra* note 52.

62. Two treaties provide limitations on certain military activities on the sea bed. *See* Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space, and Under Water, Aug. 5, 1963, T.I.A.S. No. 5433, 480 U.N.T.S. 43; Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed and the Ocean Floor and in the Subsoil Thereof, Feb. 11, 1971, 23 U.S.T. 701, 955 U.N.T.S. 115 [hereinafter Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed]. These agreements, however, only apply to nuclear weapons and do not limit the transport or use of nuclear weapons in the waters above the seabed.

63. Gordon G. Chang, *China Explores the Seabed Near America*, WORLD AFF. (July 25, 2011), http://www.worldaffairsjournal.org/blog/gordon-g-chang/china-explores-seabed-near-america.

c. Subterranean

Similar to the seabed, the ability to place weapons systems underground and employ them effectively against an enemy is beginning to develop.[64] Not only is it almost certain that underground weapons will attack surface targets, but it is also clear that they could be used to create surface effects through underground explosions and other means of manipulation. This will probably include the creation of earthquakes, tsunamis, and other surface effects that will severely affect an enemy. This portion of the earth is currently not weaponized,[65] but it will be in the future.

d. Space and Celestial Bodies

Space and the free use of space have become vital to the functioning of the modern military. In fact, "[a] Government Accountability Office report . . . showed major Defense space acquisition programs 'have increased by about $11.6 billion'—321 percent—from initial estimates for fiscal years 2011 through 2016."[66]

U.S. Air Force Gen. William Shelton, who is the head of Space Command, recently stated that "[o]ur assured access to space and cyberspace is foundational to today's military operations and to our ability to project power whenever and wherever needed across the planet."[67] Similarly, Army Lt. Gen. Richard Formica stated, "If the Army wants to shoot, move or communicate, it needs space."[68] Formica added that because of the Army's dependency on these systems, they "have to be defended."[69]

These quotes refer mostly to the use of satellites, but despite current legal restrictions, it is very likely that the use of the moon and potentially other celestial bodies will soon follow.[70] Space systems such as satellites

---

64. *See* Geoff Manaugh, *Drone Landscapes, Intelligent Geotextiles, Geographic Countermeasures*, BLDG BLOG (Jan. 11, 2012), http://bldgblog.blogspot.com/2012/01/drone-landscapes-intelligent.html.

65. *See* Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed, *supra* note 62.

66. Walter Pincus, *Hearings Show Our Dependence on Military Space Technology*, WASH. POST (Mar. 26, 2012), http://articles.washingtonpost.com/2012-03-26/world/35448260_1_military-space-space-command-aehf.

67. *Id.*

68. *Id.*

69. *Id.*

70. The 1967 Outer Space Treaty limits military activities in outer space. Article IV states:

> States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.
>
> The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden. The use of military per-

can be defended and attacked both from space and from the ground. Both China and the United States have conducted recent anti-satellite operations and established that both have that capability.[71] Space has already begun to be weaponized[72] and that trend will continue and increase in speed and lethality.

e. Cyberspace

Much has already been written about cyberspace. The Chinese have created a separate department of their military to handle the military aspects of cyberspace.[73] The United States recently created Cyber Command to specifically plan and control U.S. military cyber operations.[74] Army General Keith Alexander not only commands Cyber Command but also heads the National Security Agency.[75] Currently, 140 nations either already have or are actively building cyber capabilities within their military,[76] with Brazil being one of the most recent to make that decision.[77]

---

sonnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the Moon and other celestial bodies shall also not be prohibited.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

71. Amy Chang, *Indigenous Weapons Development in China's Military Modernization*, U.S.-China Econ. & Sec. Rev. Commission (Apr. 5, 2012), http://www.uscc.gov/researchpapers/2012/China-Indigenous-Military-Developments-Final-Draft-03-April2012.pdf; Angela Webb, *Joint Effort Made Satellite Success Possible*, Free Republic (Feb. 26, 2008), http://www.freerepublic.com/focus/f-news/1976747/posts; *Concern Over China's Missile Test*, BBC News (Jan. 19, 2007), http://news.bbc.co.uk/2/hi/asia-pacific/6276543.stm.

72. Blake & Imburgia, *supra* note 33, 173–76; Jameson W. Crockett, *Space Warfare in the Here and Now: The Rules of Engagement for U.S. Weaponized Satellites in the Current Legal Space Regime*, 77 J. Air L. & Com. 671 (2012).

73. Tania Branigan, *Chinese Army to Target Cyber War Threat*, The Guardian (July 22, 2010), http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department.

74. Andrew Gray, *Pentagon Approves Creation of Cyber Command*, Reuters (June 23, 2009), http://www.reuters.com/article/2009/06/24/us-usa-pentagon-cyber-idUSTRE55M78920090624.

75. *Biography: Director of the NSA/CSS*, Nat'l Sec. Agency, http://www.nsa.gov/about/leadership/bio_alexander.shtml (last visited Mar. 9, 2014).

76. Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties*, 13 SMU Sci. & Tech. L. Rev. 249, 249 (2010); Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. Rev. 65, 96 (2009).

77. Pedro Ozores, *Eyeing Major Events, Brazil to Form Body to Fight Cyber Attacks*, BNAmericas (Dec. 28, 2012), http://www.bnamericas.com/news/technology/eyeing-major-events-brazil-to-form-body-to-fight-cyber-attacks.

Recent revelations concerning Stuxnet[78] and Flame[79] make it clear that nations are already using cyberspace to conduct military activities that cause harm similar to kinetic operations. Nations are also stealing technologies and trade secrets through cyber operations.[80] These cyber thefts have not yet been equated with an attack but may be so treated in the future as the seriousness of the thefts continues and increases. Cyberspace has certainly been militarized by states and will continue to be so, and on an increasing basis.[81]

One of the most important aspects of cyberspace is that, unlike the weaponization of space or the seabed, it does not require a nation to conduct "military" activities in cyberspace. There are numerous examples of private hackers, organized groups, and business organizations using the Internet to do great harm to both private and public entities.[82] The accessibility of the militarization of cyberspace makes it somewhat unique in the future of armed conflict, which will be discussed below.

Most important for this discussion is the lack of boundaries in cyberspace. While the computer used to conduct the "attack" must be in one geographic location and work through a server in a specific geographic location, the lethal electrons will traverse many nations in their path to the requested destination. Further, to this point, states have been unwilling to take responsibility for cyber "attacks" that emanate from within their geographic boundaries,[83] leaving only criminal process as the means of seeking redress for non-state-actor-sponsored attacks, a process that has seldom proven successful.[84]

2. Emerging Law

The emerging factors discussed above will create stress on the current underpinnings and general principles of the LOAC. Fundamental ideas, such as territorial sovereignty, upon which the state-centric LOAC is based, will diminish in importance. The current doctrine of neutrality will

78. Amr Thabet, *Stuxnet Malware Analysis Paper,* CODEPROJECT (Sept. 9, 2011), http://www.codeproject.com/Articles/246545/Stuxnet-Malware-Analysis-Paper.

79. *Full Analysis of Flame's Command and Control Servers*, SECURELIST (Sept. 17, 2012, 1:00 PM), http://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers.

80. *See, e.g.*, Peter Foster, *China Chief Suspect in Major Cyber Attack*, DAILY TELEGRAPH (Aug. 3, 2011), http://www.telegraph.co.uk/technology/news/8679658/China-chief-suspect-in-major-cyber-attack.html.

81. Noah Shachtman, *DARPA Looks to Make Cyberwar Routine with Secret "Plan X"*, WIRED, (Aug. 21, 2012), http://www.wired.com/dangerroom/2012/08/plan-x/.

82. Mathew J. Schwartz, *Anonymous Attacks North Korea, Denies Targeting South*, INFO. WEEK (June 25, 2013), http://www.informationweek.com/security/attacks/anonymous-attacks-north-korea-denies-tar/240157253; *Global Network of Hackers Steal $45 Million from ATMs*, CNBC (May 10, 2013), http://www.cnbc.com/id/100726799.

83. *See, e.g.*, *The Cyber Raiders Hitting Estonia*, BBC NEWS, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665195.stm.

84. *See, e.g.*, Clifford J. Levy, *What's Russian for 'Hacker'?*, N.Y. TIMES (Oct. 21, 2007), http://www.nytimes.com/2007/10/21/weekinreview/21levy.html?pagewanted=all&_r=0.

be impossible to apply. Certain specific international agreements that impact the LOAC will likely be ignored or abrogated as technological capabilities increase. As these stresses develop, the LOAC will need to adjust to maintain its relevance to future armed conflicts.

a. Territorial Sovereignty

Since the inauguration of the Westphalian system, one of the indicia of statehood is a designated territory. This was memorialized in the Montevideo Convention[85] and has been part of recent discussions on statehood in both Kosovo[86] and Palestine.[87] Assumed in this attachment of territory to statehood is the authority and obligation to control that territory, including the use of force within designated borders and the use of force from within designated borders that will have effects outside the territory.[88]

It is this assumption that led to the bifurcation of the LOAC into rules governing international armed conflicts (IACs) and separate rules governing non-international armed conflicts (NIACs).[89] When the United States was faced with conducting an armed conflict with a transnational actor after the terrorist attacks of 9/11, it struggled to apply the appropriate rules.[90] It seems clear that applying the NIAC rules to a transnational armed conflict was clearly outside the meaning of the Geneva Conventions as originally signed.[91] Despite this, the U.S. Supreme Court eventually determined that certain LOAC provisions formed a minimum set of rights that applied to all armed conflicts, regardless of unbounded geography.[92]

It is almost certain that armed conflicts in the future will continue to be carried out by organized groups who will be found outside a limited geographic scope. To the extent that the LOAC would prevent the applica-

85. Montevideo Convention on the Rights and Duties of States, Dec. 26, 1933, 49 Stat. 3097, 165 LNTS 19.

86. William Thomas Worster, *Law, Politics, and the Conception of the State in State Recognition Theory*, 27 B.U. INT'L L.J. 115 (2009).

87. JOHN QUIGLEY, THE STATEHOOD OF PALESTINE: INTERNATIONAL LAW IN THE MIDDLE EAST CONFLICT 209–11 (2010).

88. *See* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY 81–90, 96–118 (2002); Frederic Gilles Sourgens, *Positivism, Humanism, and Hegemony: Sovereignty and Security for Our Time*, 25 PENN. ST. INT'L L. REV. 433, 443 (2006) (citing sixteenth-century writer Bodin as defining sovereignty as "the absolute and perpetual power of the commonwealth resting in the hands of the state").

89. *See generally* Jensen, *supra* note 21; James G. Stewart, *Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict*, 85 INT'L REV. RED CROSS 313 (2003), *available at* http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/5PYAXX/$File/irrc_850_Stewart.pdf (describing the history of the development of the Geneva Conventions).

90. Jensen, *supra* note 21, at 685–88.

91. ANTHONY CULLEN, THE CONCEPT OF NON-INTERNATIONAL ARMED CONFLICT IN INTERNATIONAL HUMANITARIAN LAW 36–39 (2010).

92. *See* Hamdan v. Rumsfeld, 548 U.S. 557, 628–32 (2006).

tion of force in accordance with current U.S. practice, a reinterpretation of the LOAC will be necessary. Additionally, the specific application of LOAC provisions, such as non-movement of security detainees,[93] would need to be reinterpreted in light of transnational groups during armed conflict.

Future conflicts will also raise questions about the ability of states to control the use of force from within their territory during armed conflicts in the same way as they currently do. For example, even now, during peacetime, nations have claimed that they cannot be responsible for cyber activities that emanate from within their borders.[94] The obligation to prevent transboundary harm that was clearly articulated in the Trail Smelter Arbitration,[95] and made applicable to situations of armed conflict in the Corfu Channel case,[96] has not prevented states from disclaiming responsibility for cyber actions from within their borders during armed conflict.[97]

As will be discussed below, the globalization of social networking will allow linkages between people of many different nationalities who might take forceful actions during armed conflict. These individuals will be acting not as citizens of any particular country but as members of transnational ideological groupings, and nations will find these individuals difficult to control. While the inability of a state to control all the actions of its individual residents is not new, the capability for those residents to readily harness state-level violence, such as cyber tools, and then direct that state-level violence across boundaries is relatively new and will only become more possible with technological advances.

The transnational nature of fighters and the decreasing ability of states to control the emanation of state-level violence from within their sovereign territory will likely frustrate the current understanding of the application of the LOAC. The idea of a geographically limited conflict is difficult to maintain when organized (social networking) groups are using state-level violence from multiple (neutral) states across the world.[98]

---

93. Geneva Convention, *supra* note 18, art. 49.

94. Shashank Bengali, Ken Dilanian & Alexandra Zavis, *Chinese Cyber Attack Disclosures*, L.A. TIMES (June 5, 2013),http://timelines.latimes.com/la-fg-china-cyber-disclosures-timeline/; *see also*, *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*, INTELLIGENCE & NAT'L SEC. ALLIANCE 8 (Sept. 2011), https://images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf.

95. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1965–66 (1941).

96. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

97. *See* John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

98. *See* Mathew J. Schwartz, *Anonymous Takes Down North Korean Websites*, INFORMATIONWEEK (Apr. 16, 2013), http://www.informationweek.com/security/attacks/anonymous-takes-down-north-korean-websit/240152985 (describing the hacktivist group Anonymous's disruption of North Korean websites).

b. Neutrality

As implied above, the doctrine of neutrality will also come under pressure in future conflicts where the geography of the battlefield is less confined. States that are not participants in armed conflict and that wish to maintain their neutrality will find it difficult to effectively do so when individuals' actions from within their geographic borders will involve state-level violence. For example, assume a citizen of a neutral country decides to conduct a cyber attack against one of the belligerent countries. To maintain its neutrality, the neutral country must prevent such attacks.[99] Alternatively, the attacked country may use self-help to stop the attacks. This is not new.[100] However, what is new is the level of violence that individuals can readily muster and the global scale of organization and reach of these individual participants.

When individuals from eighty neutral countries can organize themselves to attack simultaneously and instantaneously with state-level violence at different targets in the belligerent state, the doctrine of neutrality and a belligerent's ability to respond become almost meaningless. The belligerent state may not have time to determine the neutral state's willingness or ability to intervene or stop the attack. Under the current LOAC doctrine of neutrality, such activities would likely lead to the belligerent declaring the neutral as a hostile party to the conflict.[101]

Additionally, when an individual launches a cyber attack, the malware will inevitably flow through the infrastructure of neutral states. Under Article 8 of Hague V, "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[102] This provision is one of the very few codified provisions in the LOAC that refer to neutrality and electronic communications. Yet, when considering Article 8 specifically, the group of experts who wrote the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) could not agree on its specific applicability to cyber operations.[103] The experts did agree that the provisions of the LOAC applicable to neutrality were difficult to apply in the context of cyber war and "need to be interpreted."[104] This approach by the Tallinn

---

99. Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land art. 5, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention (V)].

100. *See* U.S. DEP'T OF THE NAVY, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, ch. 7.3 (2007) [hereinafter COMMANDER'S HANDBOOK]; R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AM. J. INT'L L. 82, 89 (1938); Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825 (2012).

101. *See* COMMANDER'S HANDBOOK, *supra* note 100, at ch. 7.2.

102. Hague Convention (V), *supra* note 99, art. 8.

103. TALLINN MANUAL, *supra* note 42.

104. *Id.*; *see generally* Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L. J. 815 (2012).

Manual should signal to the international community the need to look more closely at the LOAC, at least within the context of cyberspace, and acknowledge that review and revision is necessary.

c. International Agreements

Finally, though not strictly a matter of the LOAC, there are numerous international agreements that affect the militarization of specific areas and the application of the LOAC to activities in these areas. For example, the Outer Space Treaty limits some military activities in space but has no specific provision prohibiting the use of conventional weapons (or for example, lasers) in outer space that may be used against targets in orbit, on celestial bodies, or on the Earth.[105]

Other treaties[106] also limit or affect the use of Earth's "places" for military purposes. However, these agreements, to the extent that states will continue to follow them in the future, serve only to limit states. As will be discussed below, the actors of armed conflict are going to dramatically change and increase, including a significant variety of non-state entities that will have no legal obligations under these international agreements and may or may not be effectively constrained by states. As emphasized below, the LOAC will have to reach out to these other actors to regulate Earth's "places" during future armed conflict.

B. *Actors*

The potential range of 'new actors' whose actions have repercussions at the international level is of course vast. While many of these 'new actors' have in fact been around for some time, they have called into question—and will continue to call into question—some of the more traditional assumptions on which the international legal system is based.[107]

From the very beginnings of human conflict, fighters have created rules to govern their war-like conduct.[108] As argued by Krauss and Lacey,

---

105. *See* Ricky J. Lee, *The Jus Ad Bellum In Spatialis: The Exact Content and Practical Implications of the Law on the Use of Force in Outer Space*, 29 J. SPACE L. 93, 95–98 (2003); *see also* P.J. Blount, *Limits on Space Weapons: Incorporating the Law of War into the Corpus Juris Spatialis*, Int'l Austronautical Fed'n, IAC-08.E8.3.5 (2008); Deborah Housen-Couriel, *Disruption of Satellites ad Bellum and in Bello: Launching a New Paradigm of Convergence*, 45 ISR. L. REV. 431 (2012).

106. *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3; Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed, *supra* note 62.

107. Kellenberger, *supra* note 22.

108. *See* William C. Bradford, *Barbarians at the Gates: A Post-September 11th Proposal to Rationalize the Laws of War*, 73 MISS. L.J. 639, 641 n.12, 697–710 (2004); Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II*, 47 NAVAL L. REV. 176, 182–85 (2000); Thomas C. Wingfield, *Chivalry in the Use of Force*, 32 U. TOL. L. REV. 111, 114 (2001).

these were rules "written by the utilitarians for the warriors."[109] While the quality and content of these rules ebbed and flowed over time, this progression resulted in a definition of a combatant as an agent for a state that provided authorities for individuals to take part in otherwise illegal conduct (such as killing others) so long as that conduct was in compliance with rules established by the state.[110] Because these rules were initially based on reciprocal application, they established strict qualifications for who could act with this impunity—rules that were codified in the 1899/1907 Hague Convention[111] and in greater detail in the 1949 Geneva Convention for the Protection of Prisoners of War.[112]

Concurrently, the LOAC has developed rules for the treatment of those not acting as fighters but as the victims of armed conflict. The treatment has moved from a point where non-fighters were treated as the spoils of war,[113] to a time when non-fighters were considered part of the targetable enemy,[114] to the current paradigm where militaries are strictly prohibited from targeting civilians,[115] so long as they do not "take a direct part in hostilities."[116]

As a result of these provisions, actors on the battlefield are divided into either combatants or civilians and, in fact, are defined in relation to each other. As Article 50 of GPI states, "A civilian is any person who does not belong to one of the categories of persons referred to in Article 4A(1), (2), (3), and (6) of the Third Convention and in Article 43 of this Protocol."[117] This clean division between two types of battlefield actors is among the current LOAC principles that will be stressed in future armed conflict.

1. Emerging Factors

The seemingly clear bifurcation between combatants and civilians that was established in 1949 was already eroding in the armed conflicts leading up to the 1970s, causing the ICRC to recommend relaxing the require-

109. Eric S. Krauss & Michael O. Lacey, *Utilitarian vs. Humanitarian: The Battle Over the Law of War*, PARAMETERS, Summer 2002, at 73, 73.

110. Jensen, *supra* note 21, at 710–11.

111. Regulations Concerning the Laws and Customs of War on Land, annex to Convention (IV) Respecting the Laws and Customs of War on Land art. 1, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631, *available at* http://www.icrc.org/ihl.nsf/FULL/195?OpenDocument [hereinafter Hague Regulations].

112. *See* Geneva Convention, *supra* note 18, at art. 4.

113. 3 THE GENEVA CONVENTIONS OF 12 AUGUST 1949: COMMENTARY, GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 45 (Jean S. Pictet ed., 1960), *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-III.pdf [hereinafter Geneva Conventions Commentary].

114. FRANCIS LIEBER, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD arts. 15-25 (1863), *available at* http://www.icrc.org/ihl.nsf/FULL/110?OpenDocument.

115. Protocol I, *supra* note 9, arts. 51.2, 52.1.

116. *Id.* at art. 51.3.

117. *Id.* at art. 50.1.

ments for qualification of a combatant which was then codified in GPI.[118] Recent armed conflicts have demonstrated the difficulty of determining when a civilian takes "a direct part in hostilities."[119]

Future armed conflict will undoubtedly increase the consternation over defining actors on the battlefield. The differentiation between civilians and combatants will become more blurred as global technologies allow linkages and associations among people that were not possible in 1949 or 1977. The following sections analyze emerging factors that will stress LOAC understandings of civilians, organized armed groups, and combatants.

a. Civilians

The current LOAC is clear that "the civilian population as such, as well as individual civilians, shall not be the object of attack . . . unless and for such time as they take a direct part in hostilities."[120] Despite the seeming clarity of the rule, applying the rule to civilians on the future battlefield is surprisingly difficult.[121] This rule will be discussed in two parts below, the first dealing with the prohibition on attacking civilians and the second on the meaning of direct participation in hostilities.

i. Prohibition on Attacking Civilians

Future technologies, such as the virology discussed in the scenario at the beginning of this Article, will be enhanced or facilitated by using the civilian population to either spread or host the eventual weapon. Attackers who use viruses or nanotechnologies or genetic mutators will find their attacks facilitated by using the civilian population to propagate their weapons. The nanobot will be released generally into the population and then trigger its payload based on finding the correct DNA sequence or other similar marker.

Cyber attackers will find the same methodologies useful. They will create malware that spreads broadly throughout civilian systems until it finds the specific computer system it is designed to attack and then conduct its attack. The details on these means and methods will be discussed in greater detail below, but the important aspect of these attacks for this section is that they are facilitated or hosted by civilians or civilian objects.

These types of systems are unlike prior chemical or biological weapons because they do not necessarily have deleterious effects on the host and certainly don't take full effect on the host, but rather save their full

118. *Id.* at art. 44.3. Although there is no official statement on this point, it appears that this provision is one of the reasons that the United States has not ratified Protocol I. *See* Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions,* 2 AM. U. J. INT'L L. & POL'Y 419 (1987).

119. Protocol I, *supra* note 9, art. 51.3.

120. *Id.* at arts. 51.2, 51.3.

121. *See* R. George Wright, *Combating Civilian Casualties: Rules and Balancing in the Developing Law of War*, 38 WAKE FOREST L. REV. 129, 129–36 (2003).

effect for the target. Thus, the civilian or civilian object can facilitate the attack without feeling much, if any, of the effects. This approach to disseminating a weapon system will stress the LOAC as future technologies continue to develop.

ii. Direct Participation in Hostilities

Not all civilians enjoy complete protection from being attacked. As GPI states, civilians forfeit their protection from attack if they take a direct part in hostilities.[122] The actual meaning of these words and their practical application on the battlefield has been a matter of great debate.[123] In response to the debate, the ICRC issued its "Interpretive Guidance on the Notion of Direct Participation in Hostilities"[124] (DPH Guidance), which was intended to provide guidance on what actions by civilians rose to the level of direct participation. While this publication is not without controversy[125] and certainly does not purport to be a statement of the law, it provides an interesting basis for analysis.

The DPH Guidance lays out three cumulative criteria for a civilian to be directly participating.[126] The first is that there must be a certain threshold of harm.[127] The harm should "adversely affect the military operations or military capacity of a party to an armed conflict, or . . . inflict death, injury or destruction on persons or objects protected against direct attack."[128] The second criterion is that there must be direct causation.[129] The act must be designed to directly cause harm, or part of a concrete and coordinated military operation of which the act constitutes an integral part.[130] Finally, there must be a belligerent nexus between the act and the conflict.[131] In other words, the act must be designed to directly cause the required threshold of harm in support of a party to the conflict.[132]

However "direct participation" is defined, future weapons systems and tactics will likely increase the number of civilians who become actors on the battlefield, either intentionally or otherwise. Some examples follow.

---

122. Protocol I, *supra* note 9, art. 51.3.

123. Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 90 INT'L REV. RED CROSS 991, 993–94 (2008), *available at* http://www.icrc.org/eng/assets/files/other/irrc-872-reports-documents.pdf.

124. *Id.* at 1006–09.

125. Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641 (2010).

126. Melzer, *supra* note 123, at 1016.

127. *Id.*

128. *Id.*

129. *Id.* at 1019.

130. *Id.* at 1019–25.

131. *Id.* at 1025.

132. *Id.* at 1026.

a) Tools

In the scenario from *The Atlantic* at the beginning of this Article, Samantha has no idea that she is playing a role in the attack on the President of the United States. She is undoubtedly an innocent instrumentality or tool in the attack plan. Nevertheless, she is a key component of the attack and her ingestion of the virus and subsequent spreading of the virus is vital to the operation. Is she directly participating in hostilities though she has no intention of taking part? Does her lack of intention make targeting her any less vital?

Many other future means and methods of warfare will use civilians as tools in the attack as well, including genomics and nanotechnologies. Cyber operations already struggle with this issue.[133] The use of civilians as tools to facilitate advanced technological attacks requires a reconsideration of the rules on direct participation.

b) Transnational Communities of Interest

The rise of social networking and its ability to instantaneously link together individuals and groups from across the globe is just beginning to be explored as a social phenomenon. Negative aspects of this global linkage are already being felt across various levels of society, including the business world.[134]

Jeffrey Walker has termed these groups "instantaneous transnational communities of interest" and argues that "It's simply no longer necessary to have a state sponsor for an interested group of people to effect changes within the international community."[135] Anthony Lake, former National Security Advisor to President Clinton, described these instantaneous transnational communities of interest as "technology enabling local groups to forge vast alliances across borders, and . . . a whole host of new actors challenging, confronting, and sometimes competing with governments on turf that was once their exclusive domain."[136]

Social networking's effects on armed conflict have also already begun to surface[137] and will only increase over time. As Philip Bobbitt has writ-

---

133. TALLINN MANUAL, *supra* note 42, at 119–20; Collin Allan, *Attribution Issues in Cyberspace*, 13 CHI.-KENT J. INT'L & COMP. L. 55, 57 (2013).

134. BOB HAYES & KATHLEEN KOTWICA, TREND RESEARCH: CRISIS MANAGEMENT AT THE SPEED OF THE INTERNET, SECURITY EXECUTIVE COUNCIL (2013), *available at* https://www.securityexecutivecouncil.com/secstore/index.php?main_page=product_info&cPath=77_66&products_id=361.

135. Jeffrey K. Walker, *Thomas P. Keenan Memorial Lecture: The Demise of the Nation-State, the Dawn of New Paradigm Warfare, and a Future Profession of Arms*, 51 A.F. L. REV. 323, 329–30 (2001).

136. *Id.* at 133, 330 (citing ANTHONY LAKE, 6 NIGHTMARES 281–82 (2000)).

137. *See* George Griffin, *Egypt's Uprising: Tracking the Social Media Factor*, PBS (Apr. 20, 2011), http://www.pbs.org/newshour/updates/middle_east/jan-june11/revsocial_04-19.html.

ten, "The internet enabled the aggregation of dissatisfied and malevolent persons into global networks."[138]

Audrey Kurth Cronin likens social networking to the *levée en masse* and argues that it allows cyber mobilization of people across the entire globe on issues of common ideology.[139] She writes:

> The evolving character of communications today is altering the patterns of popular mobilization, including both the means of participation and the ends for which wars are fought. . . Today's mobilization may not be producing masses of soldiers, sweeping across the European continent, but it is effecting an underground uprising whose remarkable effects are being played out on the battlefield every day.[140]

As social networking continues to embed itself as a societal norm, people will begin to view themselves less as Americans, or Germans, or Iranians, and more as members of global ideologies created, maintained, and mobilized over social media.[141]

Through social media, individuals will be able to recruit, provide financial support, collect intelligence, pass strategies and information, forward ideas and instructions for munitions, create and solidify plans of action, and coordinate attacks. These events will occur far from any existing battlefield but will have profound and immediate effects on hostilities, creating a global group of direct participants who will meet the legal criteria for targeting.

c) Hacktivists

The role of hacktivists has already been demonstrated in conflicts between Russia and Estonia[142] and between Russia and Georgia.[143] Though there has been no evidence to date to attribute these actions to states, David Hoffman argues that "States like China and Russia now encourage groups of freelance hackers to do their dirty work, allowing plausible deniability."[144]

Additionally, other groups of hacktivists, which are clearly not state-sponsored or state-aligned, have been able to apply state-level force and create significant effects in armed conflicts. For example, the global collec-

---

138. Philip C. Bobbitt, Inter Arma Enim Non Silent Leges, 45 SUFFOLK U. L. REV. 253, 259 (2012).

139. *See, e.g.*, Audrey Kurth Cronin, *Cyber-Mobilization: The New* Levée en Masse, PARAMETERS, Summer 2006, at 77, 77.

140. *Id.* at 84–85.

141. *See* Thomas J. Holt & Max Kilger, *Examining Willingness to Attack Critical Infrastructure Online and Offline*, 58 CRIME & DELINQUENCY 798 (2012).

142. Allan, *supra* note 133, at 59.

143. *Id.*

144. David E. Hoffman, *The New Virology: From Stuxnet to Biobombs, the Future of War by Other Means*, FOREIGN POL'Y, Mar.-Apr. 2011, *available at* http://www.foreignpolicy.com/articles/2011/02/22/the_new_virology.

tive "Anonymous" has engaged in activities against states during armed conflict with the intent to influence government behavior.[145]

Because hacktivists participate along a spectrum of activities with varying associations, it is very difficult to determine each individual's level of participation. Unless the collective work of a hacktivist group rises to the level of an organized armed group (see below), it is difficult to treat it as a collective when making targeting determinations. Many individuals, though part of the organization, may just be tools (see above) on any specific operation.

In addition to groups, individuals often act alone in this capacity and can also cause great damage. One of the first monumental "hacks" in the United States was the "solar sunrise," which ended up being the work of three individuals—a man in Israel and two teenagers in California.[146]

Hacktivism is unique to computer operations, but civilian activism is not. As the world progresses toward future armed conflict, activists and activist groups in other areas will certainly coalesce. Genomics and nanotechnology will have their own Cap'n Capsid and the international community will have to figure out how to deal with them under the LOAC.

d) "Arms" Dealers

As is discussed below in Section II(C), a wide variety of new means and methods of warfare will emerge as future technologies develop. Similar to computer malware from the hacktivists of the prior section and bioengineers from the scenario at the beginning of this article, some of these new technologies will not be limited to development by states. Some will be developed and marketed by individuals, organized groups, criminal organizations, and corporations. There is already a large market for cyber "arms" that is very lucrative and is sourced almost exclusively by non-state actors.[147]

Some of these arms dealers may also be users of the arms, which will make their legal classification simpler; but many will not be users, but mere producers. For them, this will be a business opportunity, just as it is for many contemporary arms dealers who deal in traditional arms. However, the spread of technology and the needs of future armed conflict will open this line of work to a much broader and previously innocuous group of individuals. At some point, do these creators of modern arms become

145. *See* Jana Winter & Jeremy A. Kaplan, *Communications Blackout Doesn't Deter Hackers Targeting Syrian Regime*, FOX NEWS (Nov. 30, 2012), http://www.foxnews.com/tech/2012/11/30/hackers-declare-war-on-syria/#ixzz2Ht69GA1J.

146. Kevin Poulsen, *Solar Sunrise Hacker 'Analyzer' Escapes Jail*, THE REGISTER (June 15, 2001), http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/. The FBI made a documentary about the hacks. Fed. Bureau of Investigation, *Solar Sunrise Documentary*, SECURITY TUBE, http://www.securitytube.net/video/189 (last visited Mar. 9, 2014).

147. *See* Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BUSINESS WEEK (July 20, 2011), http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html.

participants in the conflict? If not, can they assume that they can continue to take these actions with relative impunity?

e) Nongovernmental Organizations

Nongovernmental organizations (NGOs) deserve mention here also. Though they are unlikely to become actors on the future battlefield, they are expanding their participation in international governance.[148] One need only look at their efforts in the area of anti-personnel landmines to see how significant an effect NGOs can have in the formulation and alteration of the LOAC.[149] It seems likely that the trend of greater influence by NGOs will increase and that as the international community struggles to evolve the LOAC in response to future places, actors, and means and methods of warfare, NGOs will have a seat at the table. Their involvement in law formulation may provide a vehicle for the incorporation of each NGO's individual agenda, whatever that may be. While this may or may not result in positive effects on LOAC development, the point is that NGOs' role is increasing which is likely to lead to different results than in the past.

b. Organized "Armed" Groups

One of the great clarifications urged by the DPH Guidance is the recognition that civilians often form themselves into organized armed groups and that membership in these groups should result, to varying degrees, in a forfeiture of civilian protections.[150] These groups, in many varieties, are likely to increase in future armed conflict. Some examples are discussed below.

i. Non-traditional "Armed" Groups

One of the most important potential changes to the idea of organized armed groups in the future is what it means to be armed. In the discussion above, transnational communities of interest and hacktivist groups were treated as individuals who might directly participate in hostilities. This was based on a more traditional view of "armed," meaning kinetic, weapons. However, many future technologies will produce, as in the scenario at the beginning of this article, weapons or things that can be used as weapons that are very different than the traditional view of "arms."

For example, is "Anonymous" an organized armed group? It possesses state-level force with its ability to infiltrate and affect governmental (and corporate) computer systems. Would a transnational community of interest that has gathered DNA samples on world leaders and is willing to

148. Steve Charnovitz, *Two Centuries of Participation: NGOs and International Governance*, 18 MICH. J. INT'L L. 183, 183 (1997).

149. Walker, *supra* note 135, at 330.

150. For example, the ICRC's DPH Guidance allows for targeting based on membership in an organized armed group when combined with a continuous combat function within the organization. Melzer, *supra* note 123, at 1006–09.

sell them to the highest bidder be an organized armed group? Or a group of individuals who work together to build a virus that will transport a genomic mutator? Or a transnational group of concerned scientists who publish openly nanotechnology processes or offer their services so everyone can enjoy the benefits of nanotechnology?

The future is likely to present numerous groups of varying composition and intent that do not possess traditional arms, but control or create the means to do great harm. These groups will stress the current application of targeting law, including the determination of lawful targets (as will be discussed below), even with the clarification of organized armed groups.

ii. Traditional "Armed" Groups

In addition to the non-traditional armed groups, the types and activities of more traditional armed groups will also expand. Four examples are discussed briefly below.

a) Private Security Companies

Much has been written recently concerning the use of private contractors, and particularly private security companies (PSC).[151] The use of contractors in current military operations has added pressures to the definition of actors on the battlefield.[152] Private contractors are involved in providing a wide array of services[153] and according to the ICRC, the trend of militaries outsourcing traditional military functions to private contractors is "likely to increase in the years ahead."[154]

---

151. John R. Crook, *Contemporary Practice of the United States Relating to International Law: International Law and non-State Actors: United States Supports Conclusion of Code of Conduct for Security Companies*, 105 AM. J. INT'L L. 156 (2011); Daniel P. Ridlon, *Contractors or Illegal Combatants? The Status of Armed Contractors in Iraq*, 62 A.F. L. REV. 199 (2008).

152. FROM MERCENARIES TO MARKET: THE RISE AND REGULATION OF PRIVATE MILITARY COMPANIES (Simon Chesterman & Chia Lehnardt eds., 2007); Eric Talbot Jensen, *Combatant Status: It is Time for Intermediate Levels of Recognition for Partial Compliance*, 46 VA. J. INT'L L. 214 (2005); Christopher J. Mandernach, *Warrior Without Law: Embracing a Spectrum of Status for Military Actors*, 7 APPALACHIAN J. L. 137 (2007).

153. Greg Miller & Julie Tate, *CIA's Global Response Staff Emerging From the Shadows After Incidents in Libya and Pakistan*, WASH. POST, Dec. 26, 2012, *available at* http://articles.washingtonpost.com/2012-12-26/world/36015677_1_security-for-cia-officers-cia-compound-benghazi; Craig Whitlock, *U.S Expands Secret Intelligence Operations in Africa*, WASH. POST (June 13, 2012), http://articles.washingtonpost.com/2012-06-13/world/35462541_1_burkina-faso-air-bases-sahara.

154. Kellenberger, *supra* note 22.

In response to abuses,[155] good work is already being done in this area[156] and more will continue to be done. However, this work is unlikely to constrain how these groups are used in the future. Governments will continue to hire PSCs to provide security to people and places on the battlefield. Even if not intentionally, the PSCs will continue to find themselves in the midst of situations requiring the use of force. It is quite possible that at some future point, some states will contract out their entire state armed forces and designate them as combatants representing the state. If this occurs, significant businesses will arise whose purpose is to provide state forces for hire. These groups of fighters, though likely compliant with the LOAC, will also be loyal to their paymaster rather than a specific state.

b) Corporate Participation and Armies

In addition to private armies for hire, corporations will do even more to provide their own security, especially in regions of instability. ExxonMobil in Indonesia and Talisman Energy in Sudan have already "hired" and controlled national military forces to protect their business interests.[157] Past corporate involvement in armed conflict includes "unlawful taking of property, forced labor, displacement of populations, severe damage to the environment, and the manufacture and trading of prohibited weapons."[158] Recent events where corporate assets were attacked and employees held hostage[159] would increase and cause corporations to reconsider their protective posture.

---

155. Press Release, Federal Bureau of Investigation, Academi/Blackwater Charged and Enters Deferred Prosecution Agreement (Aug. 7, 2012), *available at* http://www.fbi.gov/charlotte/press-releases/2012/academi-blackwater-charged-and-enters-deferred-prosecution-agreement.

156. *See, e.g.*, JENNIFER K. ELSEA, CONG. RESEARCH SERV., R40991, PRIVATE SECURITY CONTRACTORS IN IRAQ AND AFGHANISTAN: LEGAL ISSUES (2010); Rep. of the Working Group on the Use of Mercenaries As a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, Human Rights Council 15th Sess., U.N. Doc. A/HRC/15/25 (July 2, 2010), *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/151/55/PDF/G1015155.pdf?OpenElement.

157. Jonathan Horlick, Joe Cyr, Scott Reynolds & Andrew Behrman, *American and Canadian Civil Actions Alleging Human Rights Violations Abroad by Oil and Gas Companies*, 45 ALTA. L. REV. 653, 657–58 (2008); *see also* Note, *Corporate Liability for Violations of International Human Rights Law*, 114 HARV. L. REV. 2025 (2001).

158. Regis Bismuth, *Mapping a Responsibility of Corporations for Violations of International Humanitarian Law Sailing Between International and Domestic Legal Orders*, 38 DENV. J. INT'L L. & POL'Y 203, 204 (2010); *see also* ICRC, BUSINESS AND INTERNATIONAL HUMANITARIAN LAW: AN INTRODUCTION TO THE RIGHTS AND OBLIGATIONS OF BUSINESS ENTERPRISES UNDER INTERNATIONAL HUMANITARIAN LAW 24 (2006); Erik Mose, *Corporate Criminal Liability and the Rwandan Genocide*, 6 J. INT'L CRIM. JUST. 973, 974 (2008).

159. Aomar Ouali & Paul Schemm, *Desert Drama: Islamists Take Hostages in Algeria*, ASSOCIATED PRESS (Jan. 16, 2013), http://hosted2.ap.org/APDEFAULT/3d281c11a96b4ad082fe88aa0db04305/Article_2013-01-16-Algeria-Kidnapping/id-1b29673dae1745f686acac504f96c598.

Many corporations have far greater resources than the states in which they operate. The search for profit will drive them to protect their assets in areas where governments cannot control the territory. In many cases, this territory will be contested and in an area already enflamed by internal armed conflict. These corporate armies will be tasked with protecting corporate assets, employees, and resources, but will find themselves involved in the armed conflicts raging about them.

c) Global Criminal Enterprises

Another group that could also be discussed under "Organized Armed Groups" below is global criminal enterprises, such as the various organized narcotics organizations operating in Mexico and other parts of Central and South America. Reports place the number of armed fighters in Mexico alone at over 100,000,[160] a number much larger than in most recent armed conflicts.

In addition to narcotics organizations, global criminal enterprises are involved in counterfeiting, money laundering, arms smuggling, and the sex trade to name just a few.[161] Many of these criminal enterprises have links to armed conflict and even contain factions within their business whose role is to conduct military-type tasks necessary for the business enterprise. However, all of these global organizations are likely to appear on future battlefields in order to conduct their business.

d) State Paramilitaries

The large-scale operation of armed drones by the CIA portends a shift in the use of paramilitary organizations in the future. While the CIA has, from its inception, been involved in covert operations that resulted in military-type activities, the scale and openness of current operations is qualitatively different.[162] There is very little difference between the drone strikes conducted by the U.S. military and those done by the CIA, except perhaps in their regulation by the LOAC.[163]

These activities by the United States will likely set an example for other countries that also have similar agencies and will begin to use them more openly in similar ways. Future armed conflicts will undoubtedly involve intelligence and other paramilitary agencies operating openly and using military weapons and tactics.

---

160. Carina Bergal, *The Mexican Drug War: The Case For A Non-International Armed Conflict Classification*, 34 FORDHAM INT'L L.J. 1042, 1066 (2011).

161. JOHN EVANS, CRIMINAL NETWORKS, CRIMINAL ENTERPRISES 2 (1994) *available at* http://www.icclr.law.ubc.ca/publications/reports/netwks94.pdf.

162. *See* Richard M. Pious, *White House Decisionmaking Involving Paramilitary Forces*, J. NAT'L SEC. L & POL'Y (Jan. 24, 2012), http://jnslp.com/2012/01/24/white-house-decision-making-involving-paramilitary-forces/.

163. *See US: Transfer CIA Drone Strikes to Military Ensure Intelligence Agency Abides by International Law*, HUMAN RIGHTS WATCH (Apr. 20, 2012), http://www.hrw.org/news/2012/04/20/us-transfer-cia-drone-strikes-military.

c. State Forces

Significant changes will occur in future armed conflict even to recognized state forces. The changing methods of warfare will undermine the traditional criteria for combatants, and the incorporation of autonomous weapons into regular armed forces will diminish the role of humans in targeting decisions.

i. Combatant's Traditional Criteria

Article 1 of the Annex to Hague Convention (IV) respecting the Laws and Customs of War on Land states that:

> The laws, rights, and duties of war apply not only to armies, but also to militia and volunteer corps fulfilling the following conditions:
>
> 1. To be commanded by a person responsible for his subordinates;
> 2. To have a fixed distinctive emblem recognizable at a distance;
> 3. To carry arms openly; and
> 4. To conduct their operations in accordance with the laws and customs of war.
>
> In countries where militia or volunteer corps constitute the army, or form part of it, they are included under the denomination "army."[164]

These qualifications for militias are repeated in the GPI.[165] Though textually limited to militias and volunteer corps who are working with a party to

---

164. Hague Regulations, *supra* note 111, art. 1.

165. Article 4 states:

> Art 4. A. Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:
>
> (1) Members of the armed forces of a Party to the conflict, as well as members of militias or volunteer corps forming part of such armed forces.
>
> (2) Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfil the following conditions:
>
> (a) that of being commanded by a person responsible for his subordinates;
>
> (b) that of having a fixed distinctive sign recognizable at a distance;
>
> (c) that of carrying arms openly;
>
> (d) that of conducting their operations in accordance with the laws and customs of war.

See Geneva Convention, *supra* note 18, at art. 4.

the conflict, the common understanding is that state forces will also meet these criteria.[166] The difficulty with "armed groups" and these criteria has been alluded to above, but it also exists with traditional state forces.

States (and other organized groups) are employing weapons from great distances where the uniform of the targeter is indiscernible by the eventual target. The eventual target of malware launched from the National Security Agency in Maryland will be completely unaware of whether the person who launched the malware was wearing a uniform or civilian clothes. The development and employment of viruses or genomic mutators will likely be done far from the active battlefield.

Even if created and employed by uniformed personnel, when the virus, nanobot, or computer malware reaches its intended target, it will contain no marking that notifies the victim of the identity of the attacker. In fact, in many of these future weapons systems, anonymity is vital to the success of the operation. As future technologies develop, the issue of "having a fixed distinctive sign recognizable at a distance [and] . . . carrying arms openly"[167] will pressure the LOAC to account for modern armed conflict practices.

ii. Autonomous Weapon Systems

Autonomous weapons have become a very important discussion in the area of the law governing future weapons systems. They include robots, unarmed and armed unmanned aerial and underwater vehicles,[168] auto-response systems such as armed unmanned sentry stations,[169] and a host of other developing weapon systems. The systems will be discussed in greater detail below as means and methods, but they are raised here because the more autonomous they become, the more like "actors" they appear.

---

166. According to 3 GENEVA CONVENTIONS COMMENTARY, *supra* note 113, at 52:

> The drafters of the 1949 Convention, like those of the Hague Convention, considered that it was unnecessary to specify the sign which members of armed forces should have for purposes of recognition. It is the duty of each State to take steps so that members of its armed forces can be immediately recognized as such and to see to it that they are easily distinguishable from members of the enemy armed forces or from civilians. The Convention does not provide for any reciprocal notification of uniforms or insignia, but merely assumes that such items will be well known and that there can be no room for doubt.

167. Hague Regulations, *supra* note 111, art. 1.

168. Damien Gayle, *Rise of the Machine: Autonomous Killer Robots 'Could Be Developed in 20 Years'*, DAILY MAIL (Nov. 20, 2012), http://www.dailymail.co.uk/sciencetech/article-2235680/Rise-Machines-Autonomous-killer-robots-developed-20-years.html; *Marlin*, LOCKHEED MARTIN, http://www.lockheedmartin.com/us/products/marlin.html (last visited Mar. 9, 2014).

169. Jonathan D. Moreno, *Robot Soldiers Will Be a Reality—And a Threat*, WALL STREET J. (May 11, 2012), http://online.wsj.com/article/SB10001424052702304203604577396282717616136.html.

The military use of robots will sufficiently illustrate the point. It is clear that the general use of robots in armed conflict is increasing.[170] According to Peter Singer, a well-known expert on the issue of robotics and armed conflict,[171] "besides the U.S., there are 43 other nations that are also building, buying and using military robotics today."[172] Remotely controlled armed robots entered action in Iraq in summer of 2007.[173] This is a trend that will clearly continue. A report that the "Joint Forces Command drew up in 2005 . . . suggested autonomous robots on the battlefield will be the norm within 20 years,"[174] and a recent report written by the U.S. Department of Defense (DoD), titled *Unmanned Systems Integrated Roadmap FY2011-2036*, stated that it "envisions unmanned systems seamlessly operating with manned systems while gradually reducing the degree of human control and decision making required for the unmanned portion of the force structure."[175]

It appears the intent is to increase the autonomy with which these weapon systems will function, causing Singer to point out that robotics is "changing not just the 'how' [of warfare] but the 'who.'"[176] Future robots may use "brain-machine interface technologies" or "whole brain emulation."[177] The potentially autonomous nature of robots means that they will become actors on the battlefield, as well as means and methods of warfare.

Singer describes this dramatically changing advance in robotic technology as a revolution:

> Carrying forward, that means that our [robotic] systems . . . will be a billion times more powerful than today within 25 years. I'm not saying a billion in a sort of amorphous, meaningless, Austin-Powers' one billion. I mean literally take the power of those systems and multiply them times 1 with 9 zeros behind it. What that means is that the kind of things people used to talk about only at science

170. John Markoff, *U.S. Aims for Robots to Earn Their Stripes on the Battlefield*, INT'L HERALD TRIBUNE (Nov. 27, 2010), at 1.

171. Singer is currently the director of the 21st Century Security and Intelligence and a senior fellow in foreign policy at Brookings. He has authored numerous articles and books on future weapons, with particular emphasis on robotics. *See* Peter W. Singer, BROOKINGS, http://www.brookings.edu/experts/singerp (last visited Mar. 9, 2014).

172. Steve Kanigher, *Author Talks about Military Robotics and the Changing Face of War*, LAS VEGAS SUN (Mar. 17, 2011), http://www.lasvegassun.com/news/2011/mar/17/military-robotics-and-changing-face-war/.

173. Stew Magnuson, *Gun Toting Robots See Action in Iraq*, NAT'L DEF. MAG. (Sept. 2007), http://www.nationaldefensemagazine.org/archive/2007/September/Pages/RifleToting4435.aspx.

174. P.W. Singer, *In the Loop? Armed Robots and the Future of War*, DEF. INDUSTRY DAILY (Jan. 28, 2009, 20:09), http://www.defenseindustrydaily.com/In-the-Loop-Armed-Robots-and-the-Future-of-War-05267/.

175. U.S. DEP'T OF DEF., UNMANNED SYSTEMS INTEGRATED ROADMAP FY2011-2036, 3 (2011), *available at* http://www.defenseinnovationmarketplace.mil/resources/UnmannedSystemsIntegratedRoadmapFY2011.pdf.

176. Singer, *supra* note 11, at 10.

177. Moreno, *supra* note 169.

> fiction conventions like Comic-Con now need to be talked about by people like us, need to be talked about by people in the halls of power, need to be talked about in the Pentagon. We are experiencing a robots revolution.[178]

In response to these advances, the DoD recently issued a Directive titled "Autonomy in Weapon Systems"[179] that applies to the "design, development, acquisition, testing, fielding, and employment of autonomous and semi-autonomous weapon systems, including guided munitions that can independently select and discriminate targets."[180] The Directive states that "It is DoD policy that . . . [a]utonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[181]

In the same week the DoD Directive was issued, Human Rights Watch issued a report[182] calling for a multilateral treaty that would "prohibit the development, production and use of fully autonomous weapons."[183] The Directive and Report have sparked a great deal of discussion,[184] much of which has revolved around the ability of an autonomous weapon to make decisions as required by the LOAC.[185]

---

178. Singer, *supra* note 11.

179. Dept. of Def., Directive, 3000.09, Autonomy in Weapon Systems (D.O.D. 2012). The Directive followed a DoD Defense Science Board Task Force Report on "The Role of Autonomy in DoD Systems" that was issued in July of 2012. DoD DEFENSE SCIENCE BOARD, THE ROLE OF AUTONOMY IN DOD SYSTEMS (2012), *available at* http://www.fas.org/irp/agency/dod/dsb/autonomy.pdf.

180. Dept. of Def., Directive, 3000.09, Autonomy in Weapon Systems ¶ 2a(2), (D.O.D. 2012). The Directive "[d]oes not apply to autonomous and semi-autonomous cyberspace systems for cyberspace operations; unarmed, unmanned platforms; unguided munitions; munitions manually guided by the operator (e.g. laser- or wire-guided munitions); mines; or unexploded explosive ordnance." *Id.* ¶ 2b.

181. *Id.* ¶ 4a.

182. HUMAN RIGHTS WATCH, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS (2012), *available at* http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf.

183. *Id.* at 46.

184. *See, e.g.*, Kenneth Anderson, *Readings: Autonomous Weapon Systems and Their Regulation*, LAWFARE: HARD NAT'L SEC. CHOICES (Dec. 11, 2012, 6:26 PM), http://www.lawfareblog.com/2012/12/readings-autonomous-weapon-systems-and-their-regulation/; Kenneth Anderson, *Autonomous Weapon Systems and Their Regulation—A Flurry of Activity*, THE VOLOKH CONSPIRACY (Dec. 12, 2012, 9:32 PM), http://www.volokh.com/2012/12/12/autonomous-weapon-systems-and-their-regulation-a-flurry-of-activity/; Jordana Mishory, *Carter: Human Input Required For Autonomous Weapon Systems*, UNMANNED SYSTEMS ALERT (Nov. 28, 2012) http://unmannedsystemsalert.com/Unmanned-Systems-General/Public-Content/carter-human-input-required-for-autonomous-weapon-systems/menu-id-1004.html?S=LI#%21; Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to Critics*, HARV. NAT'L. SEC. J. (Feb. 5, 2013), http://harvardnsj.org/wp-content/uploads/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf.

185. Spencer Ackerman, *Pentagon: A Human Will Always Decide When a Robot Kills You*, WIRED (Nov. 26, 2012, 6:12 PM), www.wired.com/dangerroom/2012/11/human-robot-kill.

Despite the DoD Directive, the international community must recognize that at some point, fully autonomous weapon systems will likely inhabit the battlefield (and may eventually become the predominant players) and will be making decisions that we now think of as requiring human intervention.[186] This will stress our current understanding and application of the LOAC, and force an evolution in how we apply LOAC principles.

2. Emerging Law

The section above has touched only briefly on some of the emerging factors regarding actors on the battlefield that will place stresses on the LOAC in future armed conflicts. Anticipating these emerging factors, the law will need to evolve to respond to technological developments and signal appropriate regulation.

a. Attack

The proscription dealing with civilians is against making them the object of "attack." The meaning of attack is defined in GPI as "acts of violence against the adversary, whether in offence or in defence."[187] The strict reading of this treaty language is that civilians are only protected from acts of violence. As clearly argued by Paul Walker, most cyber activities will not reach the threshold of an attack,[188] meaning they are not proscribed. Cyber (and other) activities that cause mere inconvenience are legitimate, even when directed at the civilian population.[189] This argument will arise again below under means and methods of warfare because there are any number of potential or future weapons that will likely fall under the threshold of an "act of violence." If so, as a matter of targeting, civilians are not protected from these activities that do not amount to an attack.

For example, recalling the scenario from the beginning of the article, it is unclear whether the voluntary ingestion of a pill or even the inhalation of a nanobot would be considered an attack. Likewise, it is unclear that infection with a flu-like virus or even a viral gene alteration that had no effect on an individual would be considered an attack. Therefore, under the current LOAC, such activities may be permitted.

One might argue that Article 51 of GPI requires that "the civilian population and individual civilians shall enjoy general protection against dangers arising from military operations,"[190] and "military operations" is a category much broader than "attacks." However, even Article 51 only pro-

186. Anderson & Waxman, *supra* note 23.

187. Protocol I, *supra* note 9, at art. 49.1.

188. Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NAT'L SEC. L. BRIEF 33 (2011), *available at* http://digitalcommons.wcl.american.edu/nslb/vol1/iss1/3.

189. TALLINN MANUAL, *supra* note 42.

190. Protocol I, *supra* note 9, art. 51.1.

tects civilians against "dangers," a term that is not clearly defined and might not include flu-like symptoms. Similarly, Article 57.1 states that "In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[191] The commentary defines military operations as "any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat,"[192] but does not explain what it means to "spare" the population or define "constant care."[193]

With the future development of weapons that will undoubtedly fit below the attack threshold of "acts of violence," it will be important to clarify the LOAC as it pertains to targeting of civilians as actors in armed conflict. If the LOAC is designed to protect civilians from the effects of armed conflict, more detail is necessary here.

b. Status and Conduct

Targeters justify attacking individuals based on either their status or their conduct. Combatants are targetable simply based on their status. The LOAC also allows targeting of members of the military wing or an organized armed group based on their status as members.[194] Almost all others are targetable based solely on their conduct. In other words, the normal civilian has to do something to bring himself within the crosshairs of a targeter. As discussed above, future technologies will cause us to rethink how we currently understand both status and conduct.

Beginning with civilians, under the current DPH Guidance, it is unlikely that Samantha in the scenario that begins this article would be targetable. She is an unknowing facilitator of a uniquely lethal virus. Perhaps the virus could be targeted with lethal force, effectively amounting to the targeting of Samantha, but one can imagine a different scenario where Samantha might, instead of walking to the place where the U.S. President would be speaking, merely prepare food that was going to be served at a luncheon or package flowers that were going to be delivered to the White House. Does she become targetable once she has ingested the virus and remain targetable for the life of the virus, potentially for the rest of her life? The current LOAC does not seem to contemplate such a reading. One could argue that she does not directly participate at any point in her life (though she carries the virus) until she plans on coming into direct contact with the President, but the burden on targeters to maintain awareness of her until she decides to take direct part is overly burdensome, par-

191. *Id.* art. 57.1.

192. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 680 (Sandoz et al. eds., 1987) [hereinafter RED CROSS COMMENTARY].

193. For a discussion on this issue relative to cyber operations, see TALLINN MANUAL, *supra* note 42; Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L L. STUD. 198, 202 (2013).

194. *See, e.g.*, Melzer, *supra* note 123, at 1036.

ticularly once she has inadvertently passed the virus to others who now also presumably carry the threatening virus.

Similar difficulties arise from social networking and transnational communities of interest. As civilians attach themselves to causes, and then work through social media to forward that cause, do they become targetable? For example, are the tens of thousands of individuals targetable who forward a message trying to garner support for a rebel group? What if they are seeking information that might help the rebel group attack opposing forces?

In a variation on the same theme, can a state mobilize its citizens to accomplish national security goals through social media and not forfeit their protected status? Chris Ford proposes that the federal government use social networking methods to involve U.S. citizens "into a nation-wide program designed to address discrete security issues."[195] Would this make the citizens targetable?

Similarly with hacktivists, could Georgia have targeted the Russian hacktivists who were degrading the government's ability to exercise command and control of their military forces? Whatever response Georgia would have contemplated would certainly be bound by the principle of proportionate response, but even the authority to target the hacktivists is unclear under the current application of the LOAC.

This prospect of using civilians as unwitting tools is an area where the LOAC is not fully developed. Many of the answers to these questions are undoubtedly fact-specific, but the use of these future technologies will force the international community to reconsider its application of LOAC immunity.

The same questions exist concerning civilian property. Collin Allan has highlighted the difficulties of the computer system that has been taken over remotely and acts as part of the attack but whose owner has not made any affirmative decision to participate in the attack.[196] Perhaps that civilian property is transformed into a military objective, but if so, that would potentially implicate hundreds of thousands of computers that have been incorporated into powerful botnets and used for nefarious purposes.[197]

This status and conduct difficulty will also be magnified as new "armed" groups, including PSCs, corporate armies, and paramilitaries, become more prominent on the battlefield. Presumably, the Taliban could target a member of the CIA who was flying an armed drone with the intent of attacking members of the Taliban, based on his conduct. Since the CIA now has a continuing program of targeting with armed drones, is the entire CIA (or even the portion who work with the drones) targetable

195. Christopher M. Ford, *Twitter, Facebook and Ten Red Balloons: Social Network Problem Solving and Homeland Security*, 7 HOMELAND SECURITY AFF. J. 1, 1–2 (2011), *available at* http://www.hsaj.org/?article=7.1.3.

196. Allan, *supra* note 133, at 78–81.

197. *See* Pierre Thomas & Jack Cloherty, *FBI, Facebook Team Up to Fight 'Butterfly Botnet'*, ABC NEWS (Dec. 12, 2012), http://abcnews.go.com/Technology/butterfly-botnet-targets-11-million-including-computer-users/story?id=17947276.

based on status, not conduct? Similar analysis would apply to PSCs or corporate armies.

In addition to the question of lawfully targeting corporate armies or PSCs, there is an issue of how the LOAC should respond to their increasing presence on the battlefield. Many will argue that holding to the current LOAC, which does not authorize them to participate with any status on the battlefield, is the right way to proceed. But the realities of future armed conflict and the prevalence of these actors may lead to a different conclusion.

And finally, in the area of status and conduct there is the traditional requirement of marking or wearing a uniform and carrying arms openly. This is an area that is ripe for LOAC evolution. Both Sean Watts[198] and Rosa Brooks[199] have written convincingly, challenging the value of the traditional requirements that combatants "have a fixed distinctive emblem recognizable at a distance," and "carry arms openly"[200] as being "detach[ed] from reality."[201] In an age where an ever-increasing number of weapons are initiated, launched, or activated from a time and place distant from the victim, wearing uniforms and carrying your weapon openly seems of little value.[202]

Does it really matter to the victim if the individual launching the computer malware from his office in Maryland is wearing a uniform or not? Would it be much more meaningful if the malware itself was "marked" as coming from the United States? When the President collapses from ingesting the virus created in the scenario that begins this Article, would it do more to protect innocent victims of the armed conflict from the United States' retaliation if the virus was somehow marked or if Cap'n Capsid was wearing a uniform while he took his actions in sending the virus to Samantha?

Each cruise missile launched by the United States is marked with a U.S. flag, though it is unlikely that anyone will ever see the flag as it flies toward its target. But the idea of marking the weapon may set the pattern for future "over the horizon" or "shoot and forget" weapons. One of the intents in originally requiring combatants to wear uniforms was to make clear that the attacker represented a sovereign. Accomplishing this with viruses, genomics, nanotechnology, and cyber attacks will force the international community to reexamine the traditional criteria for combatants.

c. "Human" Discretion

Much of the legal consternation over robotics and other autonomous weapons systems is the discomfort with non-human decision making in

198. Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391 (2010).

199. Brooks, *supra* note 5.

200. Hague Regulations, *supra* note 111, art. 1.

201. Watts, *supra* note 198, at 446.

202. Brooks, *supra* note 5, at 756–57.

armed conflict, or the "human-out-of-the-loop" weapons. The Human Rights Watch Report referenced above categorized autonomous weapons into three categories:

- HUMAN-IN-THE-LOOP WEAPONS: Robots that can select targets and deliver force only with a human command;
- HUMAN-ON-THE-LOOP WEAPONS: Robots that can select targets and deliver force under the oversight of a human operator who can override the robots' actions; and
- HUMAN-OUT-OF-THE-LOOP WEAPONS: Robots that are capable of selecting targets and delivering force without any human input or interaction.[203]

Currently, it is unclear what having a human "in the loop" actually means[204] and whether it will result in fewer targeting mistakes.[205] What does seem to be clear is that having a human in the loop just makes the communication link between the robot and human the vulnerability.[206]

Despite this discomfort with a lack of legal precedent, technology continues to push forward, attempting to make robots more and more capable of independent decision making. Dyke Weatherington, DoD Deputy Director of Unmanned Warfare said, "I don't see any program going down that path (yet). There are legal and ethical issues, and I just don't think either the department or the technology is ready to do that."[207] Dr. Arkin, Director of the Mobile Robot Laboratory at Georgia Technical College, says that robots "will not have the full moral reasoning capabilities of humans, but I believe robots can—and this is hypothesis—perform better than humans."[208] There is certainly an argument to be made that a robot that is not subject to the emotions of the situation, dependence on inaccuracies and limitations of human sensory perception, and driven to make decisions based on frail human survivability will "perform better" and be less likely to engage an inappropriate target.

---

203. HUMAN RIGHTS WATCH, *supra* note 182.

204. Singer, *supra* note 174.

205. *See id.*

206. *Id.*

207. Tara McKelvey, *Human Input at an End as Killer Robots do the Thinking*, THE AUSTRALIAN (May 21, 2012) at 1. For a discussion of the ethical issues, see Ken Anderson, *An Ethical Turing Test For Autonomous Artificial Agents*, CONCURRING OPS. (Feb. 17, 2012, 11:47 AM), http://www.concurringopinions.com/archives/2012/02/an-ethical-turing-test-for-autonomous-artificial-agents.html.

208. Gary E. Marchant et al., *International Governance of Autonomous Military Robots*, 12 COLUM. SCI. & TECH. L. REV. 272, 279–80 (2011) (listing several reasons why autonomous robots may be able to outperform humans under combat conditions including: the ability to act conservatively, they can be used in a self-sacrificing manner if needed and appropriate without reservation by a commanding officer, and they can be designed without emotions that cloud their judgment); McKelvey, *supra* note 207; *Cry Havoc, and Let Slip the Highly Ethical Robots of War*, THE AM. PROSPECT (Aug. 9, 2011), http://prospect.org/article/cry-havoc-and-let-slip-highly-ethical-robots-war.

Autonomous weapons on the battlefield will increase and the autonomy of those weapon systems will also increase, raising serious questions about how the LOAC can deal with these issues.[209] As Jonathan Moreno has noted, "The various international agreements about weapons and warfare do not cover the convergence of neuroscience and robotic engineering."[210]

At what point do we determine that we have sufficiently programmed a weapon system such that it can legally respond to external information and stimuli in order to make a lethal decision? If the weapon acts incorrectly and unlawfully kills someone, who is responsible? Do we put the system on trial, its designer, its programmer, the soldier who set it up, or the commander who determined it could be used in that situation? As Vik Kanwar writes when reviewing Singer's *Wired for War*:

> From the point of view of the international lawyer, the concern is not asymmetry of protection, but rather that one side might be shielded from legal consequences. For a series of partially coherent reasons, the "human element" is seen as "indispensible": for providing judgment, restraint, and ultimately responsibility for decisions.[211]

All of these questions, and many more, raise legal issues that are as yet unresolved but will need to be resolved as technology propels us toward the greater use of autonomous weapons. It is unlikely that the international community will respond to Human Rights Watch's call for an international agreement to ban autonomous weapons. History does not support that idea.[212] Therefore, the international community needs to begin now to think of how the LOAC must evolve to respond.[213]

C. *Means and Methods*

"Few weapons in the history of warfare, once created, have gone unused."

U.S. Deputy Defense Secretary William J. Lynn III[214]

The quote above by William Lynn highlights the need to evolve the LOAC to regulate new technologies. Once developed, weaponized technologies almost inevitably find their way onto the battlefield. In the few instances where the technologies have not been used, or at least used in a

209. Anderson & Waxman, *supra* note 23.

210. Moreno, *supra* note 169.

211. Vik Kanwar, *Review Essay: Post-Human Humanitarian Law: The Law of War in the Age of Robotic Weapons*, 2 HARV. NAT'L SEC. J. 616, 620 (2011).

212. *See* Banusiewicz, *supra* note 10.

213. Anderson and Waxman make this argument very effectively concerning autonomous weapons in their article, *Law and Ethics for Robot Soldiers*. Anderson & Waxman, *supra*, note 23.

214. Banusiewicz, *supra* note 10.

limited fashion, it has been largely based on legal restrictions.[215] The means and methods discussed below will also require the international community to consider whether the current LOAC is sufficient to adequately regulate their use, and where not, consider what evolutions to the LOAC are necessary.

1. Emerging Factors

Weapons technology is always advancing. The means of conducting hostilities and the methods for employment of those means will continue to develop at an incredible pace over the next few decades. Many of these future technologies, some of which are discussed below,[216] will spring from peaceful advances that greatly benefit the world at large, but when weaponized, create difficult regulatory and response problems.[217]

a. Means

The means of armed conflict generally refers to the weapon used to engage a target, whether that weapon is a rifle fired by a fighter, an explosive round fired from an artillery tube, or a bomb dropped from an aircraft. Research continues to develop weapons that are more lethal, more accurate, more survivable, and less expensive. Future weapons will develop in response to perceived needs by the military, constrained by the LOAC. This section is certainly not comprehensive, but will discuss some

215. *See, e.g.*, Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161 (entered into force Mar. 5, 1970); Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, S. Treaty Doc. No.103-21, 1974 U.N.T.S. 3 [hereinafter Chemical Weapons Convention].

216. There is no way to adequately describe even a small number of the new technologies that will become a common part of future armed conflicts. *See* Blake & Imburgia, *supra* note 33, at 162–63; David Axe, *Military Must Prep Now for 'Mutant' Future, Researchers Warn*, WIRED (Dec. 31, 2012, 6:30 AM), http://www.wired.com/dangerroom/2012/12/pentagon-prepare-mutant-future/; Patrick Lin, *Could Human Enhancement Turn Soldiers Into Weapons That Violate International Law? Yes*, THE ATLANTIC, (Jan. 4, 2013), http://www.theatlantic.com/technology/print/2013/01/could-human-enhancement-turn-soldiers-into-weapons-that-violate-international-law-yes/266732/; Anna Mulrine, *Unmanned Drone Attacks and Shape-shifting Robots: War's Remote-control Future*, CHRISTIAN SCI. MONITOR (Oct. 22, 2011), http://www.csmonitor.com/USA/Military/2011/1022/Unmanned-drone-attacks-and-shape-shifting-robots-War-s-remote-control-future; Noah Schachtman, *DARPA's Magic Plan: 'Battlefield Illusions' To Mess With Enemy Minds*, WIRED (Feb. 14, 2012), http://www.wired.com/dangerroom/2012/02/darpa-magic/; Noah Schachtman, *Suicide Drones, Mini Blimps and 3D Printers: Inside the New Army Arsenal*, WIRED (Nov. 21, 2012), http://www.wired.com/dangerroom/2012/11/new-army-arsenal/; Mark Tutton, *The Future of War: Far-out Battle Tech*, CNN (Dec. 16, 2011), http://www.cnn.com/2011/12/15/tech/innovation/darpa-future-war/index.html.

217. Hoffman, *supra* note 144, at 78 ("Both cyber and bio threats are embedded in great leaps of technological progress that we would not want to give up, enabling rapid communications, dramatic productivity gains, new drugs and vaccines, richer harvests, and more. But both can also be used to harm and destroy. And both pose a particularly difficult strategic quandary: A hallmark of cyber and bio attacks is their ability to defy deterrence and elude defenses.").

of the new weapons technologies that are being developed or researched to highlight some of the areas where the LOAC will need to evolve.

i. Drones

Drones are a quickly developing technology, and their use has been widely documented.[218] In addition to the armed drones so often the topic of discussion in the media,[219] the United States is using unmanned, unmarked turboprop aircraft in places like Africa to "record full-motion video, track infrared heat patterns, and vacuum up radio and cellphone signals."[220] Drones are now a component of local law enforcement and the U.S. Federal Aviation Administration is going to pass laws regulating the use of domestic airspace for drones,[221] in anticipation of a dramatic increase in drone space requests.

As the technology continues to develop, not only would drone capabilities increase, but also drone size will significantly decrease. The United States is currently designing drones as small as caterpillars and moths that replicate flight mechanics so they can "hide in plain sight."[222] Eventually, drones will be measured in terms of nanometers and be capable of travel through the human body.[223]

In addition to decreasing the size of drones, the technology to arm these microscopic drones continues to increase. Through innovative weapons technologies,[224] genomics,[225] and other miniaturization advances, future nanodrones will be lethal and pervasive, amongst the population generally and continuously transmitting data back to the drone's controllers. Singer describes them as a "game changer" on the level with the atomic bomb.[226]

---

218. Peter Bergen & Katherine Tiedemann, *Washington's Phantom War: The Effects of the U.S. Drone Program in Pakistan*, FOREIGN AFF., July-Aug. 2011, at 12, 13 (2011); *see also*, Tony Rock, *Yesterday's Laws, Tomorrow's Technology: The Laws of War and Unmanned Warfare*, 24 N.Y. INT'L L. REV. 39, 42 (2011) (talking about the use of drones and its legal implications).

219. Bergen & Tiedemann, *supra* note 218, at 17.

220. Whitlock, *supra* note 153.

221. Wells C. Bennett, *Unmanned at Any Speed: Bringing Drones into Our National Airspace*, BROOKINGS (Dec. 14, 2012), http://www.brookings.edu/research/papers/2012/12/14-drones-bennett.

222. Elisabeth Bumiller & Thom Shanker, *War Evolves With Drones, Some Tiny as Bugs*, N.Y. TIMES (June 20, 2011), at A1, *available at* http://www.nytimes.com/2011/06/20/world/20drones.html?pagewanted=all.

223. *See* Blake & Imburgia, *supra* note 33, at 180.

224. Mike Hanlon, *Recoilless Technology Provides Killer App for UAVs*, GIZMAG (Dec. 11, 2006), http://www.gizmag.com/go/6590/.

225. See *infra* Part II.C.1.a.vii.

226. Interview with Peter W. Singer, *supra* note 47 ("I think the way to think about [unmanned drones] is they are a game-changer when it comes to both technology, but also war and the politics that surrounds war. This is an invention that's on the level of gunpowder or the computer or the steam engine, the atomic bomb. It's a game changer.").

Technology will also make drones accessible to many more actors than states. Currently, "for about $1,000, you can build your own version of the Raven drone."[227] General access to miniaturized drones will soon follow. Eventually, a disgruntled adversary or disaffected civilian will not need Samantha to carry the virus to the President, but a microdrone with the ability to inject the virus into the President's system.

ii. Cyber

In recent surveys by *Foreign Policy*, cyber capabilities were viewed as the most dangerous of emerging capabilities.[228] Like drones, cyber operations have been written about extensively,[229] including the new Tallinn Manual, which gives guidance on the application of LOAC to cyber operations in armed conflict.[230] As mentioned above, many nations are developing cyber capabilities,[231] and some speculate that cyber operations will become such a part of future conflict that "eventually, the Cyber Force will need to become a separate military branch because of cyberspace's international use as a battlefield that directly affects households, corporations, universities, governments, military, and critical infrastructures."[232]

The increasing prevalence and complexity of cyber weapons is without dispute. The Stuxnet[233] malware "infected about 100,000 computers worldwide, including more than 60,000 in Iran, more than 10,000 in Indo-

227. Singer, *supra* note 11.

228. Elizabeth Dickinson, *The Future of War*, FOREIGN POL'Y, Mar.-Apr. 2011, at 64, *available at* http://www.foreignpolicy.com/articles/2011/02/22/the_future_of_war (describing that out of sixty-two top professionals, policymakers, and thinkers in the military world, twenty-four reported drones and other unmanned technologies to be the most innovative in the last decade but the highest response for the most dangerous innovation was cyberwarfare). In the 2012 survey, of seventy-six top professionals, policymakers, and thinkers in the military world, twenty-four (the majority by ten) thought that cyber operations was the area where the Chinese were catching up with U.S capabilities the fastest. Margaret Slattery, *The Future of War*, FOREIGN POL'Y, Mar.-Apr. 2012, at 78, *available at* http://www.foreignpolicy.com/articles/2012/02/27/The_Future_of_War?print=yes&hidecomments=yes&page=full.

229. COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian T. O'Donnell, eds., 2002); Eric Talbot Jensen, *Unexpected Consequences From Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145 (2003), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=987553; Michael N. Schmitt, *The Principle of Distinction in 21st Century Warfare*, 2 YALE HUM. RTS. & DEV. L.J. 143 (1999); Watts, *supra* note 198, at 392; Sean Watts, Cyber Perfidy and the Law of War (unpublished manuscript)(on file with author).

230. TALLINN MANUAL *supra* note 42, at 75–202.

231. See *supra* Part II.A.1.e.

232. Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 318 (2008).

233. *See generally* Thabet, *supra* note 78.

nesia and more than 5,000 in India;"[234] the recent Flame malware[235] "exceeds all other known cyber menaces to date" according to Kapersky Lab and CrySys Lab which discovered the malware.[236]

One of the great allures of cyber weapons is their bloodless nature,[237] but ethicists worry about the impact of that on armed conflict. "With cyberweapons, a war theoretically could be waged without casualties or political risk, so their attractiveness is great—maybe so irresistible that nations are tempted to use them before such aggression is justified."[238]

Another aspect of cyber means of armed conflict is its ready access to non-state actors. Individual hackers have been known to develop sophisticated malware and cause great damage.[239] Particularly in cyber operations, one of the great dangers is reengineering or copycats.[240] As reported by David Hoffman,

> Langner [who first discovered the Stuxnet malware] warns that such malware can proliferate in unexpected ways: "Stuxnet's attack code, available on the Internet, provides an excellent blueprint and jump-start for developing a new generation of cyber warfare weapons." He added, "Unlike bombs, missiles, and guns, cyber weapons can be copied. The proliferation of cyber weapons cannot be controlled. Stuxnet-inspired weapons and weapon technology will soon be in the hands of rogue nation states, terrorists, organized crime, and legions of leisure hackers."[241]

---

234. Holger Stark, *Stuxnet Virus Opens New Era of Cyber War*, SPIEGEL ONLINE INT'L (Aug. 8, 2011, 3:04 PM), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html. Admittedly, Stuxnet was governed by the *jus ad bellum*, but similar malware will undoubtedly be used during armed conflict in the future. For an analysis of Stuxnet under the *jus in bello*, see Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842 (2012).

235. *See generally Full Analysis of Flame's Command and Control Servers*, *supra* note 79.

236. *Flame Virus Update: UK Servers Used to Control Malware*, INT'L BUS. TIMES NEWS (June 6, 2012, 1:10 PM), http://www.ibtimes.co.uk/articles/349195/20120606/flame-update-servers-shut-down.htm.

237. Blake & Imburgia, *supra* note 33, at 181–83.

238. Patrick Lin, Fritz Allhoff & Neil Rowe, *Is it Possible to Wage a Just Cyberwar?*, THE ATLANTIC (June 5, 2012, 11:24 AM), http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

239. David Kleinbard & Richard Richtmyer, *U.S. Catches 'Love' Virus: Quickly Spreading Virus Disables Multimedia Files, Spawns Copycats*, CNNMONEY (May 5, 2000, 11:33 PM), http://money.cnn.com/2000/05/05/technology/loveyou/.

240. Mark Clayton, *From the Man Who Discovered Stuxnet, Dire Warnings One Year Later*, CHRISTIAN SCI. MONITOR (Sept. 22, 2011), http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later.

241. Hoffman, *supra* note 144.

iii. Robots

Again, the use of robots has been well documented, along with many of the issues they create.[242] Though the use of robotics has not progressed as far as that of drones and cyber operations, their use is increasing in armed conflict. As noted by Singer,

> When the U.S. military went into Iraq in 2003, it had only a handful of robotic planes, commonly called "drones" but more accurately known as "unmanned aerial systems." Today, we have more than 7,000 of these systems in the air, ranging from 48-foot-long Predators to micro-aerial vehicles that a single soldier can carry in a backpack. The invasion force used zero "unmanned ground vehicles," but now we have more than 12,000, such as the lawnmower-size Packbot and Talon, which help find and defuse deadly roadside bombs.[243]

Singer further argues that "literally thousands of Americans are alive today because of [ground and air robotic systems]. They offer precision on the battlefield never imagined before, as well as remove many dangers to our forces."[244]

Robots will be used for both lethal and less than lethal operations. Bobby Chesney speculates on the potential use of robots in capturing as opposed to killing enemies on the battlefield. He admits this possibility is "far-fetched" now, but says he "would not be surprised to learn that a robotic descent/secure/ascent technology already is in development."[245]

Retired Army Colonel Thomas Adams argues that "Future Robotic weapons 'will be too fast, too small, too numerous and will create an environment too complex for humans to direct.' . . . Innovations with robots 'are rapidly taking us to a place where we may not want to go, but probably are unable to avoid.'"[246] Testing and development continue[247] as robots take a more active role in hostilities.

---

242. *See generally* PETER W. SINGER, WIRED FOR WAR (2009).

243. P. W. Singer, *We. Robot*, SLATE (May 19, 2010), http://www.slate.com/articles/news_and_politics/war_stories/2010/05/we_robot.html; *see also* Bumiller & Shanker, *supra* note 222.

244. Steve Kanigher, *Author Talks About Military Robotics and the Changing Face of War*, LAS VEGAS SUN (Mar. 17, 2011, 2:01 AM), http://www.lasvegassun.com/news/2011/mar/17/military-robotics-and-changing-face-war/ (quoting Singer).

245. Robert Chesney, *Robot Rendition: Will There One Day Be Machines That Capture Rather Than Kill?*, LAWFARE: HARD NAT'L SEC. CHOICES (Aug. 10, 2012, 5:41 PM), http://www.lawfareblog.com/2012/08/robot-rendition-will-there-one-day-be-machines-that-capture-rather-than-kill/.

246. *Robots on Battlefield: Robotic Weapons Might be the Way of the Future, But They Raise Ethical Questions About the Nature of Warfare*, TOWNSVILLE BULL. (Austr.), Sept. 18, 2009, at 210.

247. Peter Finn, *A Future for Drones: Automated Killing*, WASH. POST (Sept. 19, 2011), http://articles.washingtonpost.com/2011-09-19/national/35273383_1_drones-human-target-military-base.

iv. Nanotechnology

Nanotechnology is "the understanding and control of matter at the nanoscale, at dimensions between approximately 1 and 100 nanometers, where unique phenomena enable novel applications."[248] As stated by Lieutenant Commander Thomas Vandermolen, "Nanoscience is in its infancy" and its "true practical potential is still being discovered."[249] It has already "exploded from a relatively obscure and narrow technical field to a scientific, economic and public phenomenon."[250]

The United States has embraced nanotechnology development. The National Nanotechnology Initiative is a federal interagency activity that was established in 2000. It is managed by the National Science and Technology Council and its goal is to "expedite[ ] the discovery, development and deployment of nanoscale science and technology to serve the public good, through a program of coordinated research and development aligned with the missions of the participating agencies."[251] Nanotechnology has already yielded amazing results[252] including "a nanoparticle that has shown 100 percent effectiveness in eradicating the hepatitis C virus in laboratory testing."[253]

Because of its potential and its infancy, the U.S. Government has passed legislation concerning nanotechnology, creating a National Nanotechnology Program (NNP) and a National Nanotechnology Coordination Office (NNCO).[254] The responsibilities of the NNCO are to

> (1) establish the goals, priorities, and metrics for evaluation for federal nanotechnology research, development, and other activities;

---

248. *Frequently Asked Questions*, NAT'L NANOTECHNOLOGY INITIATIVE, http://nano.gov/nanotech-101/nanotechnology-facts (last visited Mar. 9, 2014).

249. Thomas D. Vandermolen, *Molecular Nanotechnology and National Security*, AIR & SPACE POWER J. (Fall 2006), http://www.au.af.mil/au/cadre/aspj/airchronicles/apj/apj06/fal06/vandermolen.html.

250. Kenneth W. Abbot, Douglas S. Sylvester & Gary E. Marchant, *Transnational Regulation of Nanotechnology: Reality or Romanticism?*, *in* INTERNATIONAL HANDBOOK ON REGULATING NANOTECHNOLOGIES (Edward Elgar ed. 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1424697.

251. *NNI Vision, Goals, and Objectives*, NAT'L NANOTECHNOLOGY INITIATIVE, http://www.nano.gov/about-nni/what/vision-goals (last visited Mar. 9, 2014).

252. *See* David Brown, *Making Steam Without Boiling Water, Thanks to Nanoparticles*, WASH. POST (Nov. 19, 2012), http://articles.washingtonpost.com/2012-11-19/national/35505658_1_steam-nanoparticles-water.

253. Dexter Johnson, *Nanoparticle Completely Eradicates Hepatitis C Virus*, SPECTRUM (July 17, 2012), http://spectrum.ieee.org/nanoclast/semiconductors/nanotechnology/nanoparticle-completely-eradicates-hepatitis-c-virus?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IeeeSpectrumSemiconductors+%28IEEE+Spectrum%3A+Semiconductors%29; *accord "Nanorobot" Can be Programmed to Target Different Diseases*, PHYS.ORG (July 16, 2012), http://phys.org/news/2012-07-nanorobot-diseases.html.

254. 15 U.S.C. § 7501 (2006).

(2) invest in federal research and development programs in nanotechnology and related sciences to achieve those goals; and

(3) provide for interagency coordination of federal nanotechnology research, development, and other activities undertaken pursuant to the Program.[255]

The legislation does not mention military uses of nanotechnology, but it does task the NNP with "ensuring that ethical, legal, environmental, and other appropriate societal concerns, including the potential use of nanotechnology in enhancing human intelligence and in developing artificial intelligence which exceeds human capacity, are considered during the development of nanotechnology."[256]

Nanotechnology research is booming. The U.S. Government Accountability Office reports that:

> From fiscal years 2006 to 2010, the National Science and Technology Council reported more than a doubling of National Nanotechnology Initiative member agencies' funding for nanotechnology environmental, health, and safety (EHS) research—from approximately $38 million to $90 million. Reported EHS research funding also rose as a percentage of total na-

---

255. 15 U.S.C. § 7501(a) (2006).

256. 15 U.S.C. § 7501(b)(10) (2006). In response to concerns about the ethics of nanotechnology, the President's Council of Advisors on Science and Technology, in its report of April 2008 on nanotechnology, concluded:

> [T]here are no ethical concerns that are unique to nanotechnology today. That is not to say that nanotechnology does not warrant careful ethical evaluation. As with all new science and technology development, all stakeholders have a shared responsibility to carefully evaluate the ethical, legal, and societal implications raised by novel science and technology developments. However, the[re is] . . . no apparent need at this time to reinvent fundamental ethical principles or fields, or to develop novel approaches to assessing societal impacts with respect to nanotechnology.

PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., NATIONAL NANOTECHNOLOGY INITIATIVE: SECOND ASSESSMENT AND RECOMMENDATIONS OF THE NNAP (2008), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST-NNAP-NNI-Assessment-2008.pdf. Marchant, et al. have written:

> More recently, codes of conduct have emerged at the forefront of discussions to restrict the use of genetic engineering to create new biological weapons. Although there are concerns that unenforceable codes of conduct will not provide strong enough assurances against the creation of new genetically engineered biological weapons, they may play an important bridging role in providing some initial protection and governance until more formal legal instruments can be negotiated and implemented. In the same way, codes of conduct may play a similar transitional role in establishing agreed-upon principles for the military use of robots.

Gary E. Marchant et al., *International Governance of Autonomous Military Robots*, 12 COLUM. SCI. & TECH. L. REV. 272, 307 (2011).

> notechnology funding over the same period, ending at about 5 percent in 2010.[257]

In addition to the United States, countries like China and Russia are also "openly investing significant amounts of money in nanotechnology."[258]

The potential benefits of nanotechnology for military purposes have quickly become apparent. As early as 2006, Forbes reported:

> The Department of Defense has spent over $1.2 billion on nanotechnology research through the National Nanotech Initiative since 2001. The DOD believed in nano long before the term was mainstream. According to Lux Research, the DOD has given grants totaling $195 million to 809 nanotech-based companies starting as early as 1988. Over the past ten years, the number of nanotech grants has increased tenfold.[259]

Blake and Imburgia believe that nanotechnology will have a profound effect on both means and methods of warfare:

> Scientists believe nanotechnology can be used to develop controlled and discriminate biological and nerve agents; invisible, intelligence gathering devices that can be used for covert activities almost anywhere in the world; and artificial viruses that can enter into the human body without the individual's knowledge. So called "nanoweapons" have the potential to create more intense laser technologies as well as self-guiding bullets that can direct themselves to a target based on artificial intelligence. Some experts also believe nanotechnology possesses the potential to attack buildings as a "swarm of nanoscale robots programmed only to disrupt the electrical and chemical systems in a building," thus avoiding the collateral damage a kinetic strike on that same building would cause.[260]

Nanotechnology also has the:

> potential to drastically enhance military operations and safety as well as homeland security. Advances in lightweight, nanoscale-engineered materials will protect soldiers on the battlefield from bullets and shrapnel while giving them extreme mobility. In case of injury, engineered bandages with embedded antimicrobial na-

257. *US Government Accountability Office Releases Report on Nanotechnology EHS Research Performance*, NANOWERK NEWS (June 22, 2012), http://www.nanowerk.com/news2/newsid=25691.php.

258. Blake & Imburgia, *supra* note 33, at 180.

259. Josh Wolfe & Dan van den Bergh, *Nanotech Takes on Homeland Terror*, FORBES (Aug. 14, 2006, 6:00 AM), http://www.forbes.com/2006/08/11/nanotech-terror-cepheid-homeland-in_jw_0811soapbox_inl.html.

260. Blake & Imburgia, *supra* note 33, at 180 (citations omitted).

> noparticles will stop deep bleeding in a matter of minutes and keep the wound free from infection.[261]

Recently, French scientists "report[ed] the first attempt to control the combustion and the detonation properties of a high explosive through its structure."[262]

Nanotechnology is likely to improve the strength and longevity of machinery,[263] advance stealth technology,[264] allow the creation of more powerful and efficient bombs,[265] and result in miniature nuclear weapons.[266] It will eventually allow for the creation of microscopic nanobots that can be controlled and used as sensors to gather information or as weapons to carry lethal toxins or genomic alterers into the bodies of humans.[267]

Nanotechnology is a development with almost unlimited applications to future armed conflict. It will make weapons smaller, more mobile, and more potent. It will provide easier, quicker, and more accurate means of collecting information. It will allow greater range, effect, and lethality. For actors with the technology, it has the potential to completely change armed conflict as we know it.

v. Directed Energy

Directed energy weapons include lasers of various magnitude, microwave and millimeter-wave weapons. These weapon systems are based on relatively new technology and almost all are still in the early stages of development. Despite this, in a report by the U.S. Defense Science Board dealing with directed energy,[268] the co-chairs lament the lack of focus on what they term a "transformational 'game changer'."[269] Though the DoD

---

261. Wolfe & van den Bergh, *supra* note 259.

262. *Military Nanotechnology: High Precision Explosives Through Nanoscale Structuring*, NANOWERK NEWS (June 5, 2008), http://www.nanowerk.com/spotlight/spotid=5956.php.

263. *Benefits and Applications*, NAT'L NANOTECHNOLOGY INITIATIVE, http://nano.gov/you/nanotechnology-benefits (last visited Mar. 9, 2014).

264. Clay Dillow, *Carbon Nanotube Stealth Paint Could Make Any Object Ultra-Black*, POPSCI (Dec. 6, 2011, 12:15 PM), http://www.popsci.com/technology/article/2011-12/paint-imbued-carbon-nanotubes-could-make-any-object-absorb-broad-spectrum-light.

265. Adrian Blomfield, *Russian Army 'Tests the Father of All Bombs'*, TELEGRAPH (Sept. 12, 2007, 12:01 AM), http://www.telegraph.co.uk/news/worldnews/1562936/Russian-army-tests-the-father-of-all-bombs.html.

266. *Military Uses of Nanotechnology: The Future of War*, THENANOAGE.COM, http://www.thenanoage.com/military.htm (last visited Mar. 9, 2014).

267. Scientists and the University of California, Berkeley, are already working on the Micromechanical Flying Insect Project. *Micromechanical Flying Insect*, U. CAL. BERKELEY, http://robotics.eecs.berkeley.edu/~ronf/mfi.html/index.html (last visited Mar. 9, 2014); *Nanotech Weaponry*, CENTER FOR RESPONSIBLE NANOTECHNOLOGY (Feb. 12, 2004), http://www.crnano.typepad.com/crnblog/2004/02/nanotech_weapon.html; Caroline Perry, *Mass-Production Sends Robot Insects Flying*, LIVE SCI. (Apr. 18, 2012, 5:51 PM), http://www.livescience.com/19773-mini-robot-production-nsf-ria.html.

268. DEF. SCI. BD. TASK FORCE, DIRECTED ENERGY WEAPONS (2007), *available at* http://www.acq.osd.mil/dsb/reports/ADA476320.pdf.

269. *Id.* at vii.

is working on a number of potential systems, "years of investment have not resulted in any currently high-operational laser capability."[270] There are a number of functioning systems such as the Airborne Laser and the Advanced Tactical Laser,[271] but these systems have not proven to be effective battlefield weapons to this point,[272] though the Navy recently shot down a drone with ship-mounted laser.[273]

Despite these recent setbacks, directed energy weapons of various types are likely to be deployed in future armed conflicts. They will be used as maritime, airborne, land-based, and space-based systems. They will be used both as lethal and non-lethal variants.[274]

vi. Biological Agents

Biological agents have rarely appeared in armed conflict since the early twentieth century.[275] However, "[s]ince 2001, senior members of both the Obama and Bush administrations, who have reviewed classified intelligence, have consistently placed biodefense at or near the top of the national-security agenda."[276] A 2008 report on the use of weapons of mass destruction, including biological agents, believes that "a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013" and that "terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon."[277] Though such an attack has not materialized, the concern about such capability is still valid as evidenced by the fact that the FBI has recently established a Biological Countermeasures Unit that monitors the growing Do-It-Yourself Biology

---

270. *Id.*

271. Blake & Imburgia, *supra* note 33, at 177.

272. DEF. SCI. BD. TASK FORCE, *supra* note 268, at 21–29.

273. Spencer Ackerman, *Watch the Navy's New Ship-Mounted Laser Shoot Cannon Kill a Drone*, WIRED (Apr. 8, 2013), http://www.wired.com/dangerroom/2013/04/laser-warfare-system/.

274. *See generally* DEF. SCI. BD. TASK FORCE, *supra* note 268; Fritz Allhof, *Why Does International Law Restrict Nonlethal Weapons More Than Deadly Ones?*, SLATE (Nov. 13, 2012), http://www.slate.com/articles/technology/future_tense/2012/11/nonlethal_weapons_and_the_law_of_war.html.

275. 137 nations are parties to the Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65 [hereinafter Gas Protocol], and the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 26 U.S.T. 583, T.I.A.S. No. 8062; *see* Stefan Riedel, *Biological Warfare and Bioterrorism: A Historical Review*, 17 BAYLOR U. MED. CENTER PROCEEDINGS 400 (2004).

276. Wil S. Hylton, *How Ready are We for Bioterrorism?*, N.Y. TIMES (Oct. 26, 2011), http://www.nytimes.com/2011/10/30/magazine/how-ready-are-we-for-bioterrorism.html?pagewanted=all.

277. BOB GRAHAM ET AL., WORLD AT RISK: THE REPORT OF THE COMMISSION ON THE PREVENTION OF WMD PROLIFERATION AND TERRORISM, xv (2008), *available at* http://www.absa.org/leg/WorldAtRisk.pdf.

(DIYbio) movement.[278] The general consensus is that although the United States has made progress in its biodefenses, we are far from being adequately prepared.[279]

Recent advances in laboratory technology have allowed access to these horrific weapons to a much more general audience. Brett Giroir, former Director at the Defense Advanced Research Projects Agency (DARPA) argues that

> [w]hat took me three weeks in a sophisticated laboratory in a top-tier medical school 20 years ago, with millions of dollars in equipment, can essentially be done by a relatively unsophisticated technician. . . . A person at a graduate-school level has all the tools and technologies to implement a sophisticated program to create a bioweapon.[280]

Michael Daly writes that "there is already information in public databases that could be used to generate highly pathogenic biological warfare agents,"[281] and "biohacker communities have popped up around the globe, with hundreds of do-it-yourself biologists testing their experimental prowess."[282]

In addition to increased access, the methods of contamination make biological agents catastrophically dangerous. As Wil Hylton argues,

> The specter of a biological attack is difficult for almost anyone to imagine. It makes of the most mundane object, death: a doorknob, a handshake, a breath can become poison. Like a nuclear bomb, the biological weapon threatens such a spectacle of horror—skin boiling with smallpox pustules, eyes blackened with anthrax lesions, the rotting bodies of bubonic plagues—that it can seem the province of fantasy or nightmare or, worse, political manipulation.[283]

---

278. *See* Todd Kuiken, *DIYbio: Low Risk, High Potential*, THE SCIENTIST (Mar. 1, 2013), http://www.the-scientist.com/?articles.view/articleNo/34443/title/DIYbio—Low-Risk—High-Potential/; *On Guard Against WMD*, FBI (Feb. 21, 2012), http://www.fbi.gov/news/stories/2012/february/wmd_022112.

279. Wil S. Hylton, *How Ready are We for Bioterrorism?*, N.Y. TIMES, (Oct. 26, 2011), http://www.nytimes.com/2011/10/30/magazine/how-ready-are-we-for-bioterrorism.html?pagewanted=all.

280. *Id.*

281. Michael J. Daly, *The Emerging Impact of Genomics on the Development of Biological Weapons: Threats and Benefits Posed by Engineered Extremophiles*, 21 CLINICS IN LABORATORY MED. 620, 621 (2001), *available at* http://www.usuhs.mil/pat/deinococcus/FrontPage_DR_Web_work/Pages/Lab_info/Daly_papers/clinicsLabMedicineVol21No3.pdf.

282. Hanno Charisius et al., *Becoming Biohackers: Learning the Game*, BBC FUTURE (Jan. 22, 2013), http://www.bbc.com/future/story/20130122-how-we-became-biohackers-part-1.

283. Hylton, *supra* note 276.

In combination with advances in nanotechnology, biological agents become even more deadly. As Immanuel has written, "the application of nanobiotechnology for engineering biological weapons opens pathways for an entirely new class of biology based nanoweapons. They could be self-replication or non-replicating, remotely operable and extremely destructive."[284]

Biological agents also pose some unique problems for deterrence and interdiction. Graham Allison, the founding Dean of Harvard's John F. Kennedy School of Government and a leading expert on nuclear proliferation, argues that biological terrorism presents some problems even more difficult than nuclear terrorism:

> Nuclear terrorism is a preventable catastrophe, and the reason it's preventable is because the material to make a nuclear bomb can't be made by terrorists. But in the bio case—oh, my God! Can I prevent terrorists from getting into their hands anthrax or other pathogens? No! Even our best efforts can't do that. I think the amazing thing is that one hasn't seen more bioterrorism, given the relative ease of making a bioweapon and the relative difficulty of defending.[285]

The combination of increasing accessibility, the difficulty of detection and interdiction, and the potentially catastrophic nature of biological weapons makes them a very appealing weapon for not only terrorists, but also for nation-states. Despite current legal prohibitions, biological weapons will remain a possible (and likely) weapon in armed conflict.

vii. Genomics

Genomics is the "study of genes and their function."[286] The rapid advances in genomics[287] have had a multitude of benefits for modern medicine and science in general. The costs are rapidly decreasing and accessibility rapidly increasing.

> A couple of decades ago, it took three years to learn how to clone and sequence a gene, and you earned a PhD in the process. Now, thanks to ready-made kits you can do the same in less than three days . . . [T]he cost of sequencing DNA has plummeted, from

284. Gifty Immanuel, *Biotechnology by Bioterrorism: Implications for Clinical Medicine, Biotechnology*, 12 BIOTECHNOLOGY 1, 4 (2007), *available at* http://www.eolss.net/Sample-Chapters/C17/E6-58-11-18.pdf.

285. Hylton, *supra* note 276 (quoting Graham Allison).

286. *Definition of Genomics*, MEDICINENET.COM, http://www.medterms.com/script/main/art.asp?articlekey=23242 (last visited Mar. 9, 2014).

287. Hoffman, *supra* note 144, at 78 ("One thing is certain: The technology for probing and manipulating life at the genetic level is accelerating. . . . But the inquiry itself highlighted the rapid pace of change in manipulating biology. Will rogue scientists eventually learn how to use the same techniques for evil?").

> about $100,000 for reading a million letters, or base pairs, of DNA code in 2001, to around 10 cents today.[288]

However, calls for controls on genetic research and development are increasing.[289]

Some scientists and concerned advocates argue for caution and restraint because "vulnerability arises from the relative ease with which this digital genetic code can be accessed, translated, and incorporated into conventional genetic technologies."[290] Machi and McNeill state that:

> In today's market it costs just a few thousand dollars to design a custom DNA sequence, order it from a manufacturer, and within a few weeks receive the DNA in the mail. Since select agents are currently not defined by their DNA sequences, terrorists can actually order subsets of select agent DNA and assemble them to create entire pathogens.[291]

They similarly estimate that "by 2020 malefactors will have the ability to manipulate genomes in order to engineer new bioterrorism weapons."[292]

The range of nefarious possibilities through the use of genes is very broad. As proposed at the beginning of this article, stealth viruses could be introduced covertly through agricultural infestation or nanobots into the genomes of a given population, and then triggered later by a signal.[293] "Bionanobots might be designed that, when ingested from the air by humans, would assay DNA codes and self-destruct in an appropriate place (probably the brain) in those persons whose codes had been program-

---

288. Charisius et al., *supra* note 282.

289. *See* Brian Vastag, *Environmental Groups Call for Tighter Regulation of 'Extreme Genetic Engineering,'* WASH. POST (Mar. 13, 2012), http://articles.washingtonpost.com/2012-03-13/national/35447443_1_synthetic-biology-environmental-groups-synthetic-organisms.

290. Daly, *supra* note 281, at 620; *see also* Anthony C. Littrell, *Biological Weapons of Mass Destruction: The Present and Future Threat*, CONFRONTING TERRORISM, 2002, at 339, *available at* http://digitalcorpora.org/corp/nps/files/govdocs1/065/065912.pdf; Melinda Willis, *Dangers of Genetically Engineered Weapons*, ABC NEWS (Oct. 5, 2011), http://abcnews.go.com/Health/story?id=117204&page=1#.T-3ze44zzbx.

291. Ethel Machi & Jena Baker McNeil, *New Technologies, Future Weapons: Gene Sequencing and Synthetic Biology*, HOMELAND SECURITY 2020, at 1 (Aug. 24 2010), *available at* http://thf_media.s3.amazonaws.com/2010/pdf/wm2986.pdf.

292. *Id.*; according to Paul Hansen's review, Jeffery Lockwood's book, *Six-Legged Soldiers*, describes how insects have been used in war over the last 100,000 years and suggests some possibilities for genomics and insects in the future. Paul Hansen, *Six-Legged Soldiers: Using Insects as Weapons of War by Jeffery A. Lockwood*, 13 J. MILITARY & STRATEGIC STUD. 140 (2009), *available at* http://jmss.org/jmss/index.php/jmss/article/viewFile/375/395. Lockwood also details "the possibility of future human-made genomic infused mosquito weapons in North America," specifically "the potential of insects to be used in future conflicts; terrorist attacks with crop destroying beetles, fireflies as natural guardians against biological attack, or cyborgs used for bomb detection based on the body of a cockroach as the ultimate indestructible and mobile platform." *Id.*

293. Mae-Wan Ho, *GM & Bio-Weapons in the Post-Genomics Era*, INSTITUTE OF SCIENCE IN SOCIETY (Apr. 30, 2002), http://www.i-sis.org.uk/gmbiopost.php.

med."[294] The genomic material could be designed to cause a wide array of results "including death, incapacitation, [and] neurological impairment."[295]

Some domestic legal restrictions are beginning to appear.[296] But the field of genomics and its potential weaponization is still new and difficult to accurately project or regulate. Even with this limited amount of information, it raises some important impacts on the LOAC that will be discussed below.

b. Methods

The method of targeting is most often a matter of tactics where the commander decides how and when to employ a weapon system. Commanders and individuals must not only concern themselves with the weapon they are using, but also with the way in which they are using it. Advancing technology allows weapons to be employed in creative ways that raise interesting legal issues.

i. Latent Attacks

Perhaps one of the most feared methods of attack is the latent attack. This type of attack is characterized by the placing or embedding of some weapon in a place or position where it will not be triggered until signaled sometime in the future or activated by some future action. Some latent attacks may even be triggered by the victim himself. As mentioned above in relation to genomics and biological weapons, latent attacks are a fertile area for development of stealth viruses and similar weapons. "The concept of a stealth virus is a cryptic viral infection that covertly enters human cells (genomes) and then remains dormant for an extended time. However, a signal by an external stimulus could later trigger the virus to activate and cause disease."[297] The unique aspect of this is that the viral genetic material might be implanted into the victim far in advance by a nanobot and potentially never activated or only activated upon some signal by the attacker or some other event, either triggered by an unknowing third party or the victim himself.

---

294. John L. Petersen & Dennis M. Egan, *Small Security: Nanotechnology and Future Defense*, 8 DEF. HORIZONS, Mar. 2002, at 1, 3, *available at* http://www.carlisle.army.mil/DIME/documents/DH08.pdf.

295. Neil Davison, *Biochemical Weapons: Lethality, Technology, Development, and Policy*, BRADFORD NON-LETHAL WEAPONS RESEARCH PROJECTS (May 8, 2004), http://www.brad.ac.uk/acad/nlw/research_reports/docs/biochemical_weapons_May04.pdf (quoting J. Petro, et al., *Biotechnology: Impact on Biological Warfare and Biodefense*, 1 BIOSECURITY AND BIOTERRORISM: BIODEFENSE STRATEGY, PRACTICE, AND SCIENCE 161, 168 (2003)).

296. Charisius et al., *supra* note 282.

297. Michael J. Ainscough, *Next Generation Bioweapons: Genetic Engineering and Biological Warfare*, *in* THE GATHERING BIOLOGICAL WARFARE STORM 165, 176–77, 180 (Barry R. Schneider & Jim A. Davis eds., 2002), *available at* http://www.bibliotecapleyades.net/ciencia/ciencia_virus08.htm.

The method of implanting the attack far in advance of its likely use is not unique to biological agents and genomics. Latent computer attacks have already caused concern[298] and continue to grow in appeal. Consider the manufacture of computer components. It is certainly possible that manufacturers of computer materials could embed source code in the hardware of computer components that would trigger certain functions or operations by that computer at a future time.[299] Similarly, consider weapons or military equipment sales. As countries sell military hardware to other countries, it is entirely possible that latent code has been implanted that might affect its future function. For example, the United States sells F-16 aircraft to numerous countries around the world. It seems not only plausible, but perhaps irresponsible to not implant in the computer functions of that aircraft some computer code that will not allow the F-16 to engage aircraft that it identifies as belonging to the United States.

The ability to perform latent attacks and keep them hidden until the appropriate time is a technological question, but it seems unlikely that if the potential for such actions exists, it would not be used extensively, even against current allies, as a hedge against changing political landscapes and alliances.

ii. Camouflage

It is clear that camouflaging soldiers or military equipment is a legitimate ruse of war and raises no LOAC issues generally.[300] However, future developments will allow camouflage in a different way than used before. Prior uses of camouflage included both blending in with the natural environment and mimicking other environments.[301] For example, dressing in a camouflaged uniform allowed soldiers to blend into their environment, but the nature of the uniform was known to opposing forces. Painting vehicles to match the anticipated terrain did not change the form of the vehicle.

New technologies will use electronic sensors to "project images of the surrounding environment back onto the outside of the vehicle enabling it to merge into the landscape and evade attack."[302] Use of this type of camouflage in cities or urban environments might actually project a tank to be a civilian object such as a car. Similar technology is being developed for individuals as well.[303]

---

298. Steve Stecklow, *U.S. Nuclear Lab Removes Chinese Tech Over Security Fears*, REUTERS (Jan. 7, 2013, 3:32 PM), http://www.reuters.com/article/2013/01/07/us-huawei-alamos-idUSBRE90608B20130107.

299. *Wary of Naked Force, Israel Eyes Cyberwar on Iran*, REUTERS, (Jul. 7, 2009), http://www.ynetnews.com/articles/0,7340,L-3742960,00.html.

300. Sean Watts, *Law-of-War Perfidy*, on file with author.

301. *Id.*

302. Sean Rayment, *Invisible Tanks Could Be On Battlefield Within Five Years*, TELEGRAPH (Jan. 9, 2011, 9:30 AM), http://www.telegraph.co.uk/news/uknews/defence/8247967/Invisible-tanks-could-be-on-battlefield-within-five-years.html.

303. *See, e.g.*, Charley Cameron, *Quantum Stealth Camouflage is a Hi-Tech Invisibility Cloak*, INHABITAT (Dec. 22, 2012), http://inhabitat.com/quantum-stealth-camouflage-is-a-hi-

Other forms of "camouflage" for modern weapons might include hiding specific computers or information through making it appear to be something else,[304] or piggybacking harmful malware or biological or genetic agents on useful or benign agents. These types of methods of attack, though not new in theory, will be much more prevalent because of the nature of new technologies and weapons in future armed conflict.

2. Emerging Law

Technologically advanced means and methods of warfare will change the way armed conflict occurs. As David Ignatius comments,

> The 'laws of war' may sound like an antiquated concept in this age of robo-weapons. But, in truth, a clear international legal regime has never been more needed: It is a fact of modern life that people in conflict zones live in the perpetual cross hairs of deadly weapons. Rules are needed for targets and targeters alike.[305]

The LOAC must respond by evolving in several specific but fundamental areas. The section below will outline some of the areas where adaptation is most needed.

a. Attack

As discussed above,[306] the LOAC provisions apply most completely and forcefully only to actions that are deemed an "attack." The meaning of attack is defined in GPI as "acts of violence against the adversary, whether in offence or in defence."[307] Many operations conducted with new technologies will not reach the threshold of an attack, meaning they are not proscribed. This has already been discussed with reference to cyber operations, but it equally applies to the other means and methods dis-

---

tech-invisibility-cloak/; Damien Gayle, *The Camouflage Fabric 'That Can Make Soldiers INVISIBLE'*, DAILY MAIL (Dec. 10, 2012), http://www.dailymail.co.uk/sciencetech/article-2245935/The-camouflage-fabric-make-soldiers-INVISIBLE-Company-claims-Pentagon-backing-miracle-material.html.

304. Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773 (2012).

305. Gary Marchant et al., *Nanotechnology Regulation: The United States Approach*, *in* NEW GLOBAL FRONTIERS IN REGULATION: THE AGE OF NANOTECHNOLOGY 189 (Graeme Hodge et al. eds., 2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1305256; Kenneth W. Abbot et al., *supra* note 245; Kenneth W. Abbott, et al., *A Framework Convention for Nanotechnology*, 36 ENVTL. L. REP. 10931 (2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=946777; Gary E. Marchant et al., *A New Soft Law Approach to Nanotechnology Oversight: A Voluntary Product Certification Scheme*, UCLA J. ENVTL. L. & POL'Y (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1483910; Gary E. Marchant et al., *Risk Management Principles for Nanotechnology*, 2 NANOETHICS 43 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1020104; David Ignatius, *Dazzling New Weapons Require New Rules for War*, WASH. POST (Nov. 11, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/10/AR2010111005500.html.

306. *See supra*, Part II.B.2.a.

307. Protocol I, *supra* note 9, art. 49.1.

cussed above. For example, the use of a nanobot to infiltrate an individual's body and collect data and then transmit that data to an adversary may seem more like espionage than an attack, despite its invasive nature. Similarly, the spreading of a gene[308] that creates an allergic sensitivity to pollen may have significant effect on a fighting force, but might not be termed an act of violence.

Perhaps more vexing with respect to the LOAC definition of attack is its inability to clearly demarcate the temporal limitations on actions. Recalling the example at the beginning of this article, when does the attack occur? Is it when the virus is sent to Samantha? Is it when Samantha ingests the virus? Does Samantha attack all of her friends, associates, and unwitting accomplices by spreading the virus through proximity? Does the attack occur when the first infected person, whether Samantha or someone who has caught the virus from her, enters an area where she is proximate to the President? What about when the President actually ingests the virus? Or is it not an attack until the virus actually begins to do its genetic work on the President? If an analogy to a mine or explosive is appropriate, the attack would not occur until the virus actual began to take effect in the President. That would mean that no proportionality analysis was necessary for such an attack, since there would be no collateral damage from that specific attack. Such a conclusion does not seem to support the purposes of the LOAC in protecting non-participants from the effects of armed conflict.

Similar scenarios can be created with most future weapons that have latent effects. Computer viruses may sit resident in computer systems until activated by the attacker or victim (or third party–see below). Swarms of microrobots may cross a nation's borders and take up residence at various critical points, awaiting the activation signal to commence their operations.[309] As advancing technologies are developed that might affect future

308. With respect specifically to genetic weapons, some commentators believe that all genetic weapons are already prohibited by the provisions of the 1925 Gas Protocol, Gas Protocol, *supra* note 275, and the 1972 Biological Weapons Convention which proscribes "microbial or other biological agents, or toxins[,]" Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, *supra* note 277. For example, Louise Doswald-Beck, in a presentation on the application of the LOAC to future wars, stated:

> Mention must be made of a potential new method of warfare that is already prohibited in law but that could have horrific effects if developed, namely genetic weapons. The specter of this as well as of new and obviously preliminary developments in bio-technology has already motivated States to begin negotiations for the development of verification methods for the Biological Weapons Convention.

Louise Doswald-Beck, *supra* note 2, at 44. However, this position is not universally accepted. Additionally, even if states accepted that they were limited in the use of genetic weapons and honored their obligations, those arms control conventions do not bind non-state actors and certainly wouldn't be a deterrent to terrorist organizations.

309. This scenario could also cause some reflection on the adequacy of the *jus ad bellum* under the U.N. Charter.

conflict, the LOAC will need to be ready to not only proscribe illegal behavior, but also signal in advance what kinds of behavior are prohibited.

b. Distinction and Discrimination

Article 48 of GPI embodies the foundational LOAC principle of distinction and states that "belligerents may direct their operations only against military objectives."[310] This rule is complemented by Article 51, paragraph 2 which states that "the civilian population as such, as well as individual civilians, shall not be the object of attack."[311] This rule is considered to be customary international law and binding on all nations, whether parties to the Additional Protocols or not.[312]

Discrimination in the attack, or the prohibition on indiscriminate attacks, is "an implementation of the principle of distinction"[313] and is codified in GPI, Article 51.4.[314] As discussed above, these restrictions only apply to "attacks," but even if one takes a very broad view of what constitutes an attack, the LOAC still struggles to signal effectively in the case of future weapons. For example, in the virus scenario from the beginning of the article, it appears that the lethal aspect of the virus can be and is directed at a specific military objective, and therefore not indiscriminate. Article 51.4(c) might allow one to argue that the virus was not discriminate in the attack because it was "of a nature to strike military objectives [the President in this case] and civilians or civilian objects without distinction."[315] However, the argument might be made equally convincingly that the virus did not "strike" civilians; it merely used or inconvenienced civilians.

A similar analysis can be made with cyber operations. Some have already made the argument that as a result of the use of Stuxnet by the United States, "contemporary warfare will change fundamentally" if cyber warfare is not regulated by international agreement.[316] Speaking specifically about distinction and discrimination, Patrick Lin, Fritz Allhoff, and Neil Rowe write:

---

310. Protocol I, *supra* note 9, art. 48.

311. *Id.* art. 51.2.

312. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8); 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 3 (2005), *available at* http://www.icrc.org/eng/resources/documents/publication/pcustom.htm.

313. 1 HENCKAERTS & DOSWALD-BECK, *supra* note 312, at 43.

314. Protocol I, *supra* note 9, art. 51.4.("Indiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.").

315. *Id.* art. 51.4.

316. Misha Glenny, *A Weapon We Can't Control*, N.Y. TIMES (June 14, 2012), http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html?_r=0.

> It is unclear how discriminatory cyberwarfare can be. If victims use fixed Internet addresses for their key infrastructure systems, and these could be found by an adversary, then they could be targeted precisely. However, victims are unlikely to be so cooperative. Therefore, effective cyberattacks need to search for targets and spread the attack, but as with biological viruses, this creates the risk of spreading to noncombatants: while noncombatants might not be targeted, there are also no safeguards to help avoid them. The Stuxnet worm in 2010 was intended to target Iranian nuclear processing facilities, but it spread far beyond intended targets. Although its damage was highly constrained, its quick, broad infection through vulnerabilities in the Microsoft Windows operating system was noticed and required upgrades to antivirus software worldwide, incurring a cost to nearly everyone. The worm also inspired clever ideas for new exploits currently being used, another cost to everyone.[317]

The apparent difficulties in applying the principles of distinction and discrimination[318] to potential uses of future weapons implies that an evolved LOAC would provide better protections to victims of armed conflicts.

c. Precautions and Re-engineering

Article 57 of the GPI is titled "Precautions in Attack"[319] and requires the commander or fighter to "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects"[320] and "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[321]

During the ratification process for the Protocol, there was great debate about what the term "feasible" meant.[322] Ultimately, "feasible" was generally understood "to mean that which is practicable or practicably

317. Lin et al., *supra* note 238.

318. *See* TALLINN MANUAL, *supra* note 42, at 157; Jensen, *supra* note 193, at 213–14.

319. Protocol I, *supra* note 9, arts. 57.2(a)(i)–(ii), 58.

320. *Id.* art. 57.2(a)(i).

321. *Id.* art. 57.2(a)(ii).

322. 14 Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva (1974-1977), at 199 (1978); Jensen, *supra* note 193, at 209.

possible, taking into account the circumstances ruling at the time."[323] This is the accepted standard when considering an attack.[324]

One of the interesting aspects of many future weapons systems that is different than historical weapon systems is the ability to re-engineer these weapons. Historically, when an attacker dropped a bomb on his adversary, he did not have to think of potential uses his adversary might make of that bomb. It was destroyed amidst the heat, blast, and fragmentation of the explosion. The same is not true of many future weapons. For example, when an attacker uses a virus or computer malware, the enemy can see those weapons, recover them, analyze their composition, and then re-create or re-engineer them and reuse that weapon. This would be equivalent to the United States, after using its new stealth aircraft in the fight against Saddam Hussein in Iraq, simply landing one of the aircraft at an Iraqi airport and inviting Saddam to give the aircraft to his scientists for analysis. Viruses, computer malware, genetic material, and many other future weapon systems do not self-destroy on impact. Re-engineering has already occurred in the case of computer malware[325] and will undoubtedly continue to do so with other modern and future weapon systems.

This raises the question of whether these new technologies lead to a requirement for commanders to consider the potential effects from re-engineering as part of their attack analysis. In other words, assume a commander has the following plan. He will release a swarm of microrobots, perhaps in the form of flies, that injects the general population with a deadly but limited toxin that will only become lethal when combined with a known vaccination usually given only to military. He knows that his toxin is very discriminate in the attack, but he also knows that some enterprising geneticist might come along and reengineer his virus to affect the population more generally, having lethal effect on millions instead of one. If his discreetly targeted toxin has the ability to be re-engineered and used to kill thousands or millions, must he consider that as part of his analysis when deploying the toxin?

d. Marking

The LOAC requirement of marking and its relation to future armed conflict has been addressed earlier in relation to actors on the battle-

323. Letter from Christopher Hulse, Ambassador from the U.K. to Switz., to the Swiss Gov't (Jan. 28, 1998), *available at* http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (listing the United Kingdom's reservations and declarations to Additional Protocol I, and explaining in paragraph (b) that "[t]he United Kingdom understands the term 'feasible' as used in the Protocol to mean that which is practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations"); *see also* JOINT DOCTRINE & CONCEPTS CENT., THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT 81 n. 191 (2004) (suggesting the same interpretation for the word "feasible").

324. Jensen, *supra* note 193, at 209–11.

325. Hoffman, *supra* note 144, at 80; *see* Ted Samson, *Hackers Release Decrypted Stuxnet Code—But Don't Panic*, INFOWORLD (15 Feb. 2011), http://www.infoworld.com/t/malware/hackers-release-decrypted-stuxnet-code-dont-panic-685.

field.[326] The fundamental principle is that an attacker is required to distinguish himself in the attack.[327] Similar concerns exist with relation to means and methods. Even if the actors are distinguishing themselves, to what extent is there or should there be a requirement that the weapon be distinguishable? For example, in the virus scenario, the victim state could have taken precautions had it been able to distinguish Samantha's flu-like symptoms from a potentially deadly virus. As future weapons transform from "over the horizon" to "from everywhere," the LOAC will need to provide some way for the victim to identify the attacker.

One of the more obvious examples of this is brought about by advances in camouflage, discussed above. As both vehicles and individuals use advanced technology to look like the surrounding environs, it is likely that both vehicles and fighters will take on civilian aspects. A tank that is parked amongst civilian vehicles and takes on their visual attributes may cross the line between ruse and perfidy. Is a genetically linked virus, masquerading as the common flu, significantly different? Similar concerns may exist in cyber warfare.[328]

Conclusion

The rule of law is the civilian's best bulwark not only against his own government but against those who would hold him hostage to their political objectives by threatening him with violence.[329]

When Samantha and the others to whom she has already spread the virus enter the auditorium where the President will soon be speaking and carry with them the genetically targeted virus, they will be launching the LOAC on a course it is not currently prepared to travel. It is likely that many nations are on the brink of developing similar capabilities and they will undoubtedly be used in the future.

As Professor Bobbitt states above, the rule of law is vital to protecting the victims of armed conflict from the effects of armed conflict.[330] The LOAC's role as a signaling mechanism to states and other developers of future technologies that will appear on the battlefield is vital to continuing to limit hostilities with legal proscriptions. Future changes in the places, actors and means and methods of armed conflict will stress the LOAC's ability, as currently understood and applied, to sufficiently regulate that conflict.

Now is the time to act. In anticipation of these developments, the international community needs to recognize the gaps in the current LOAC and seek solutions in advance of the situation. As the LOAC evolves to

326. *See supra*, section II.B.1.c.i.

327. Protocol I, *supra* note 9, art. 44.3.

328. Lin et al., *supra* note 238.

329. Bobbitt, *supra* note 138, at 260.

330. *See id.*

face anticipated future threats, its signaling function will help ensure that advancing technologies comply with the foundational principles of the LOAC and that future armed conflicts remain constrained by law.

Keynote Article

Future War, Future Law

Eric Talbot Jensen*

ABSTRACT

Advancing technology will dramatically affect the weapons and tactics of future armed conflict, including the "places" where conflicts are fought, the "actors" by whom they are fought, and the "means and methods" by which they are fought. These changes will stress even the fundamental principles of the law of armed conflict, or LOAC. While it is likely that the contemporary LOAC will be sufficient to regulate the majority of future conflicts, the international community must be willing to evolve the LOAC in an effort to ensure these future weapons and tactics remain under control of the law.

Though many of these advancing technologies are still in the early stages of development and design, the time to act is now. In anticipation of these developments, the international community needs to recognize the gaps in the current LOAC and seek solutions in advance of the situation. As the LOAC evolves to face anticipated future threats, it will help ensure that advancing technologies comply with the foundational principles of the LOAC and future armed conflicts remain constrained by law.

- - - - - - - - - -

I would like to express my gratitude to the *Minnesota Journal of International Law* for inviting me to this

* Associate Professor, Brigham Young University Law School. The author wishes to express gratitude to the staff of the *Minnesota Journal of International Law* for having the foresight to organize a symposium on such an important issue and for editorial assistance on the article. The author also expresses gratitude to Allison Arnold and Aaron Worthen for invaluable research assistance. A video recording of this speech can be found on the *Minnesota Journal of International Law's* website, http://www.minnjil.org/?page_id=913.

symposium, and really, for having this symposium. This is a very important subject and one which, if we do not engage on now, we will miss an opportunity to really have an impact on the future of the law of armed conflict.

In a recent address, Harold Koh, the State Department Legal Advisor, said "Increasingly, we find ourselves addressing twenty-first-century challenges with twentieth-century laws."[1] Mr. Koh is not the only person to espouse this belief.[2] The twenty-first century challenges that Mr. Koh is referring to involve rapidly advancing technologies and changing tactics that are beginning to seriously challenge even the foundational principles of the Law of Armed Conflict, or LOAC.[3] I would like to spend the next few minutes discussing what I think are some waning factors in future armed conflicts and the resulting waning legal norms and then attempt a brief peek into the future factors that will emerge from advancing technologies and even posit some suggestions concerning emerging legal norms.

I do this with some trepidation. As Louise Doswald-Beck stated, "Any attempt to look into the future is fraught with difficulty and the likelihood that much of it will be wrong."[4] However, I believe that we are currently at a point when we can see into the future of armed conflict and project, at least to some degree, the effect of advancing technologies on armed conflict and the governing LOAC. It is likely that the

1. Harold Hongju Koh, *The State Department Legal Adviser's Office: Eight Decades in Peace and War*, 100 GEO. L.J. 1747, 1772 (2012).

2. *See* Rosa Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 745 (2004); P.W. Singer, Address at the United States Naval Academy William C. Stutt Ethics Lecture: Ethical Implications of Military Robotics (Mar. 25, 2009), http://www.au.af.mil/au/awc/awcgate/navy/usna_singer_robot_ethics.pdf.

3. *See* Koh, *supra* note 1, at 1772.

4. Louise Doswald-Beck, *Implementation of International Humanitarian Law in Future Wars*, *in* 71 NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 39, 39 (Michael N. Schmitt & Leslie C. Green eds., 1998); *see also* Stephen Peter Rosen, *The Future of War and the American Military*, HARV. MAG., May–June 2002, at 29 ("The people who run the American military have to be futurists, whether they want to be or not. The process of developing and building new weapons takes decades, as does the process of recruiting and training new military officers. As a result, when taking such steps, leaders are making statements, implicitly or explicitly, about what they think will be useful many years in the future."). Despite the difficulty, it is a vital requirement of militaries and one in which plenty of people are still willing to engage. *See* Frank Jacobs & Parag Khanna, *The New World*, N.Y. TIMES (Sept. 22, 2012), http://www.nytimes.com/interactive/2012/09/23/opinion/sunday/the-new-world.html.

contemporary LOAC will be sufficient to regulate the majority of future conflicts, but we must be willing and able to evolve the LOAC in an effort to ensure these future weapons and tactics remain under control of the law.

Our current situation is not unlike those who met at the Lateran Council of 1139.[5] Tradition has it that at the council, one of the issues raised was the new invention of the crossbow.[6] The crossbow caused alarm for several reasons. First, it allowed killing at a distance, which was not the traditional way of combat.[7] Secondly, it allowed a peasant who was properly trained to kill a knight.[8] This combination meant that a peasant, who was traditionally of little value as a fighter, could now kill a knight, an asset of great value and a major investment in training and equipment.[9]

Consequently, the Council outlawed the use of the crossbow, at least when Christians were fighting each other.[10] Of course, that legal prohibition hardly survived the vote that was taken to sustain it.[11] The important point this example makes is that as we contemplate future technologies and their linkage with the law, we have to take a practical view. We cannot assume that we can merely pronounce a developing weapon or tactic as illegal and expect universal compliance.[12] That is not the lesson history teaches us.[13]

5. *See generally* Harold E. Harris, *Modern Weapons and the Law of Land Warfare*, 12 MIL. L. & L. WAR REV. 7, 9 (1973).

6. Martin van Creveld, *The Clausewitzian Universe and the Law of War*, J. CONTEMP. HIST. 403, 416 (1991).

7. *Id.*

8. *Id.*

9. *See id.* ("The story of the early firearms which, by enabling a commoner to kill a knight from afar, threatened the continued existence of the medieval world, is well known.").

10. Harris, *supra* note 5, at 9; Donna Marie Verchio, *Just Say No? The SIrUS Project: Well-Intentioned, But Unnecessary and Superfluous*, 51 A.F. L. REV. 183, 187 (2001).

11. *See* W.T. Mallison, Jr., *The Laws of War and the Juridical Control of Weapons of Mass Destruction in General and Limited Wars*, 36 GEO. WASH. L. REV. 308, 316 (1967) (discussing the continued use of the crossbow after the ban).

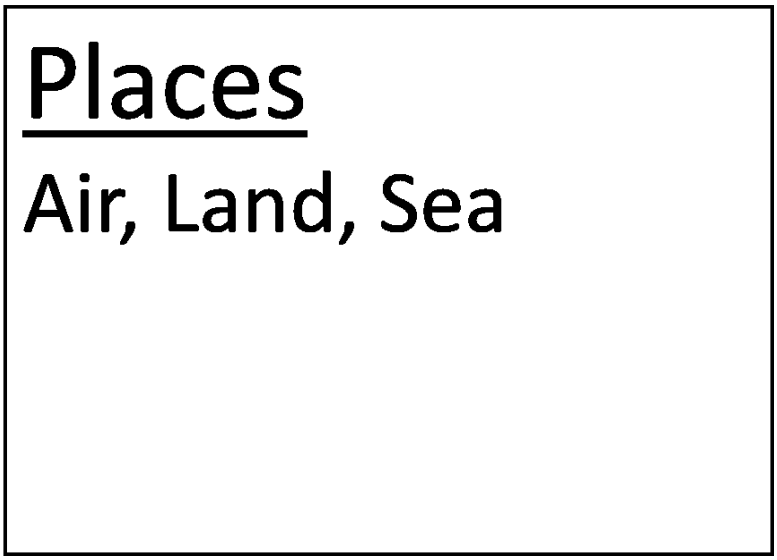
12. *Id.*

13. Vericho, *supra* note 10, at 187 ("The situation at that point in history is the same we observe today-no weapon has been effectively restricted or eliminated by international regulation.").

For convenience of my analysis, I will focus on the "places" where conflicts are fought, the "actors" by whom they are fought, and the "means and methods" by which they are fought. I remind you that predicting the future is not a promising line of work, and I do this hesitantly. My guess is that many of you will take issue with my characterization of what the future holds. However, I hope that even if you disagree with me, you will see the value of having the discussion and engaging on the issue of evolving the law of war in order to maintain its relevance in your version of the future.

Lest I be misunderstood, I am certainly not saying that these principles of law are no longer binding or useful in any situations throughout the world. Undoubtedly, advancing technologies which test these laws will emerge gradually and unequally among the international community. The majority of the current LOAC will continue to apply to most armed conflicts for the foreseeable future, but as technologies continue to advance, particularly among the advanced nations of the world, the LOAC will need to evolve to keep pace with innovation.

I. PLACES



Throughout history, armed conflict has taken place in "breathable air" zones—the land, the surface of the ocean, and recently the air above the land.[14] As the LOAC developed, these breathable air zones were concurrently being divided into areas of sovereign control,[15] with the exception of the high seas and the commons, such as the poles.[16] The effect of this was that the LOAC developed around rules governing sovereign territory and was based on presumptions about where armed conflict would occur.[17] These presumptions are now losing their applicability, requiring the international community to

14. *See* David Alexander, *Pentagon to Treat Cyberspace as "Operational Domain"*, REUTERS, July 14, 2011, *available at* http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714 (identifying the "air, land and sea" as traditional areas of operational domain for the military).

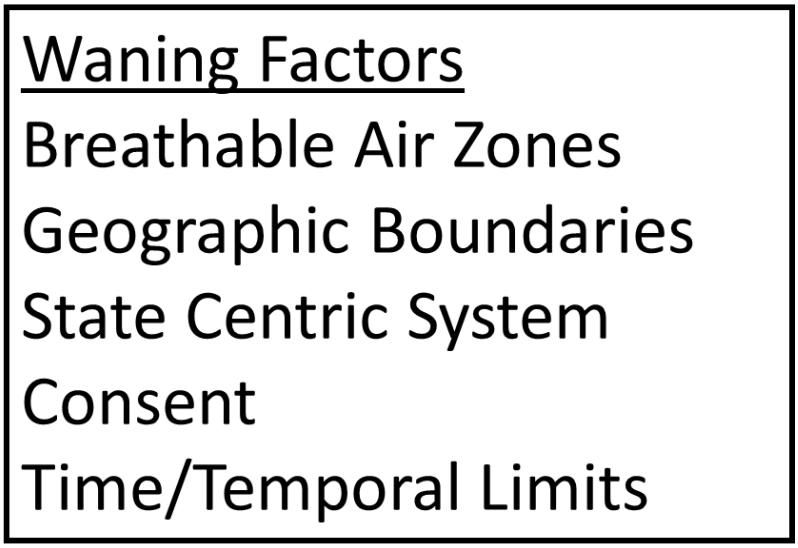
15. Eric Talbot Jensen, *Applying a Sovereign Agency Theory of the Law of Armed Conflict*, 12 CHI. J. INT'L L. 685, 707–09 (2012).

16. *See generally* Ron Purver, *Security and Arms Control at the Poles* 39 INT'L J.888, 888–92 (1984) (discussing historical examples of the use of the poles for military purposes and noting that military operations in the poles were eventually banned for all countries in the first article of the Antarctic Treaty).

17. *See* Singer, *supra* note 2 at 14–16 (noting that "going to war" has meant the same thing for 5,000 years and the changing nature of law raises legal questions never before considered).

reconsider the validity of many LOAC provisions.[18]

A. WANING FACTORS



I will not discuss each of my proposed waning factors, but several deserve specific mention. As I mentioned a moment ago, one of the most important waning factors in future conflict is the limitation to breathable air zones.[19] As I will discuss later concerning "actors," the limitation of operating in breathable air zones is swiftly disappearing.[20] Miniaturization and robotics are opening areas to use that have previously not been available.[21] We will soon not think of the ability to breath as a limitation on our ability to operate. As technology increases, military planners will not feel constrained by human restrictions, but will find other tools that can function equally

18. *Id.* at 16 (suggesting one reason the LOAC needs to be reconsidered is that modern enemies know the laws and are using them to their advantage).

19. Alexander, supra note 14.

20. *Id.* (discussing the increased need for protection from cyber-attacks and suggesting the United States has suffered $1 trillion in economic losses as a result of past cyber-attacks).

21. Jon Cartwright, *Rise of the Robots and the Future of War*, THE OBSERVER (Nov. 20, 2010), http://www.guardian.co.uk/technology/2010/nov/21/military-robots-autonomous-machines (discussing the increasing role of robots in warfare and how technological developments will likely change warfare).

well in these areas that lack breathable oxygen.[22]

Just as advancing technologies have opened access to new areas, existing geographic boundaries are beginning to feel pressure from scientific innovation. Armed conflict has for centuries been based on the Westphalian style demarcation of boundaries.[23] Crossing the boundary with your army was a sign that armed conflict had begun.[24] People on one side of the boundary generally associated themselves with one group of fighters and people on the other side with the other group.[25] This perspective on geographic boundaries is diminishing.[26] Individuals do not necessarily limit themselves or their emotional or patriotic attachments by the geographic boundaries which surround them.[27] Other means of association, such as global social networking, are lessening the perceived binding nature of geographic affiliations.[28]

Speaking of Westphalia, the system of state supremacy instituted by the post-Westphalian peace is quickly eroding.[29] States find their sovereignty threatened both politically and

22. Nick Hopkins, *Militarisation of Cyberspace: How the Global Power Struggle Moved Online*, THE GUARDIAN (Apr. 16, 2012), http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle (discussing an assertion made by the head of the US Military, General Martin Dempsey, that the United States needed to fully include space and cyberspace operations along with its traditional air-land-sea operations).

23. *See generally* PHILIP C. BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY 75–143, 501–538 (2002) (detailing historical armed conflicts and describing how boundaries factored into the conflicts).

24. *See* Saikrishna Prakash, *Unleashing the Dogs of War: What the Constitution Means by "Declare War"*, 93 CORN. L. REV. 45, 67–77 (November 2007).

25. *See* Koh, *supra* note 1, at 1772 (suggesting the traditional actors in wars were blocs of countries, but the actors in future conflicts will likely be "networks of actors connected in countless tangible and intangible ways").

26. *Id.*; Frederic Megret, *War and the Vanishing Battlefield*, 9 LOY. U. CHI. INT'L L. REV. 131, 131–33 (2011) (discussing the classic notion of a battlefield and its diminishing relevance in modern conflicts).

27. *See* Singer, *supra* note 2, at 11 (discussing a fundraiser held by college students at Swarthmore to take a stand against genocide in Darfur in which the proceeds were used to enter negotiations to rent drones to deploy to Sudan).

28. *See* Koh, *supra* note 1, at 1771–72 ("[W]e live in an age not divided by a Berlin Wall but linked by a World Wide Web.").

29. *See generally* Bobbitt, *supra* note 7, at 283–342, 667–807 (discussing how the development of the market-state and increasing number of global problems such as AIDS, environmental issues, and the changing landscape of war are eroding traditional notions of state sovereignty).

territorially by a number of emerging forces, supra- and supernational in nature.[30] It used to be that States were the final speaker on issues considered incident to sovereignty, such as the internal and external use of force, domestic policing, treatment of citizens, and relations with peers.[31] State-centricity as the sole way of viewing the world is waning and being overtaken by other views that have much more traction today.[32] I am not arguing that the state system is going away, but that its exclusivity—and possibly its supremacy in relation to certain previously sovereign prerogatives—is evaporating.

Finally, just a word about consent; much has been said lately about consent as the basis for extraterritorial military actions. The United States continues to rely—at least in part—on consent for its prosecution of the war on terror in countries such as Yemen and Pakistan.[33] The question remains unanswered as to whether, if that consent were removed, the United States would cease military operations it could justify under a self-defense argument.[34] I believe that the U.S. is setting a precedent that will inevitably weaken the doctrine of consent and, coupled with the weakening of geographic borders, allow future military actions under various self-defense theories that will dramatically weaken the need for consent.

30. *Id.*

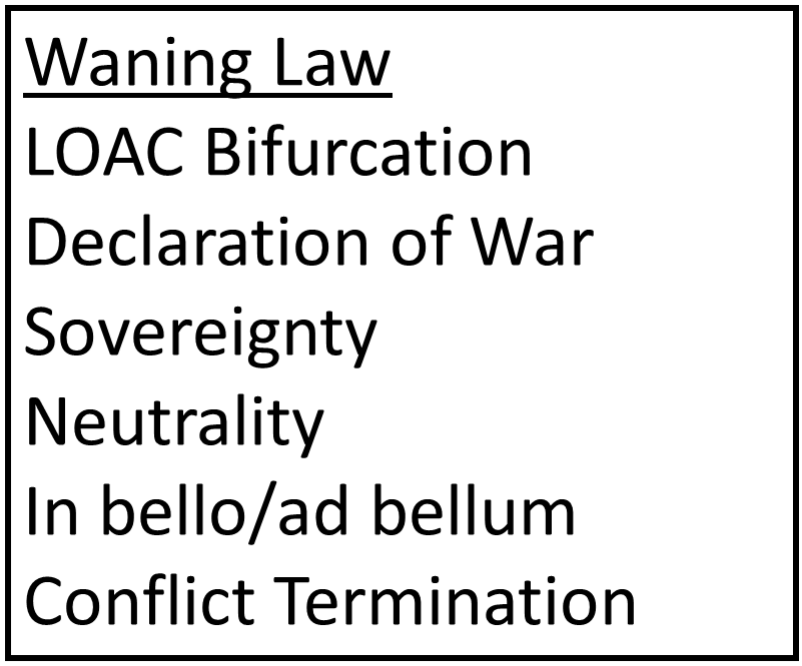
31. *See* Oscar Schachter, *The Decline of the Nation-State and its Implications for International Law*, 36 COLUM. J. TRANSNAT'L L. 7, 7–8 (1998).

32. *Id.* (discussing the abundance of scholarship produced by economists, businessmen, political scientists, and journalists that suggests the state-centric model is on the decline).

33. Greg Miller, *Yemen's Leader Says He Approves All Drone Strikes*, WASH. POST, Sept. 30, 2012, at A3; Adam Entous, Siobhan Gorman & Evan Perez, *U.S. Unease Over Drone Strikes*, WALL ST. J. (Sept. 26, 2012), http://online.wsj.com/article/SB10000872396390444100404577641520858011452.html.

34. Entous, Gorman & Perez, *supra* note 33 (noting the United States believes it has broad authority to defend itself against those who planned the attacks of September 11, 2001).

B. WANING LAW



The waning of these (and other) factors will impact the law and particularly the LOAC. As geographic boundaries lose meaning and the primacy of states wanes, a number of particular LOAC principles will face increasing attack.

The bifurcation of the LOAC between international armed conflicts, or IACs, and non-international armed conflicts, or NIACs, is already under fire.[35] The International Committee of the Red Cross, or ICRC,[36] as well as international tribunals[37]

35. Jensen, *supra* note 15, at 702–706.

36. *See* Jakob Kellenberger, ICRC President, Address at the Sixtieth Anniversary of the Geneva Conventions: Sixty Years of the Geneva Conventions: Learning from the Past to Better Face the Future (Aug. 12, 2009), http://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-president-120809.htm; Jakob Kellenberger, ICRC President, Address at the Follow-Up Meeting to the Sixtieth Anniversary of the Geneva Conventions: Strengthening Legal Protection for Victims of Armed Conflicts (Sept. 21, 2010), http://www.icrc.org/eng/resources/documents/statement/ihl-development-statement-210910.htm.

37. In addition to the quote beginning Section V, the *Tadić* Appellate Court also argued that "[i]f international law, while of course duly safeguarding the legitimate interests of States, must gradually turn to the protection of human beings, it is only natural that the [bifurcation between

and renowned scholars[38] have all argued that the LOAC bifurcation has lost its usefulness. In a powerful quote by the International Criminal Tribunal for the Former Yugoslavia (ICTY), the Court stated "What is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife."[39] The division of the binding nature of LOAC principles, those that apply to NIACs and those that apply to IACs, is quickly becoming obsolete.[40]

Little needs to be said about the declaration of war, a now antiquated idea.[41] As Robert Turner has written, "Although conflicts between and among states continue, no state has issued a formal declaration of war [since the 1948 Arab-Israeli War]."[42] Similarly, the idea that conflicts terminate with a formal agreement on cessation of hostilities also lacks currency.[43] It is hard to imagine the United States signing a peace accord with the various iterations of al-Qaeda to signify the formal end to that conflict.[44]

IAC and NIAC] should gradually lose its weight." Prosecutor v Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 97 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

38. *See* Emily Crawford, *Unequal Before the Law: The Case for the Elimination of the Distinction between International and Non-International Armed Conflicts*, 20 LEIDEN J. INT'L L. 441, 483–84 (2007); Avril McDonald, *The Year in Review*, 2 Y.B. INT'L HUMANITARIAN L. 113, 121 (1998) ("With the increase in the number of internal and internationalised armed conflicts is coming greater recognition that a strict division of conflicts into internal and international is scarcely possible, if it ever was."); *see also* Michael Reisman, Remarks at a Panel on the Application of Humanitarian Law in Noninternational Armed Conflicts (Apr. 18, 1991), *in* 85 AM. SOC'Y INT'L L. PROC. 83, 85 (suggesting a bifurcated system serves as "a sweeping exclusion device that permits the bulk of armed conflict to evade full international regulation"); Michael N. Schmitt, Yoram Dinstein & Charles H.B. Garraway, *The Manual on the Law of Non-International Armed Conflict: With Commentary*, INT'L INST. HUMANITARIAN L. (2006), http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf (suggesting that laws addressing the growing problems created by NIACs need to be developed).

39. Prosecutor v Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 119 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

40. *See supra* notes 35–39 and accompanying text.

41. ROBERT F. TURNER, THE WAR POWERS RESOLUTION: ITS IMPLEMENTATION IN THEORY AND PRACTICE 25 (1983).

42. *Id.*

43. Brooks, *supra* note 2, at 725–729 (noting the erosion of temporal restrictions on some international conflicts).

44. *Id.* at 726 (suggesting a peace accord between the United States and al-Qaeda is unlikely for several reasons, including the nature of the "war on

While technically not a part of the LOAC, the distinction between the applicability of the *jus ad bellum*, or the law of going to war, and the *jus in bello*, or the LOAC, is also on the wane.[45] Current technologies such as cyber warfare have led many to discuss the difficulty of determining when states are actually in armed conflict.[46] Future technologies will make that an even more difficult distinction to make as the idea of crossing a border to signal hostilities becomes increasingly anachronistic.[47]

Finally for this section, the law of neutrality will also become less and less applicable as geographic boundaries become more porous and states struggle to maintain the monopoly of violence. The soon-to-be-published "Tallinn Manual on the International Law Applicable to Cyber Warfare,"[48] in which I participated, struggled to apply the doctrines of neutrality to cyber warfare and acknowledged that the current rules need to evolve to deal effectively with future technologies.[49]

terrorism" and fact that al-Qaeda is not a state and as such may not be able to enter a formal peace agreement).

45. Eyal Benvenisti, *Rethinking the Divide Between Jus ad Bellum and Jus in Bello in Warfare Against Nonstate Actors*, 34 YALE J. INT'L L. 541, 541–42 (2009).

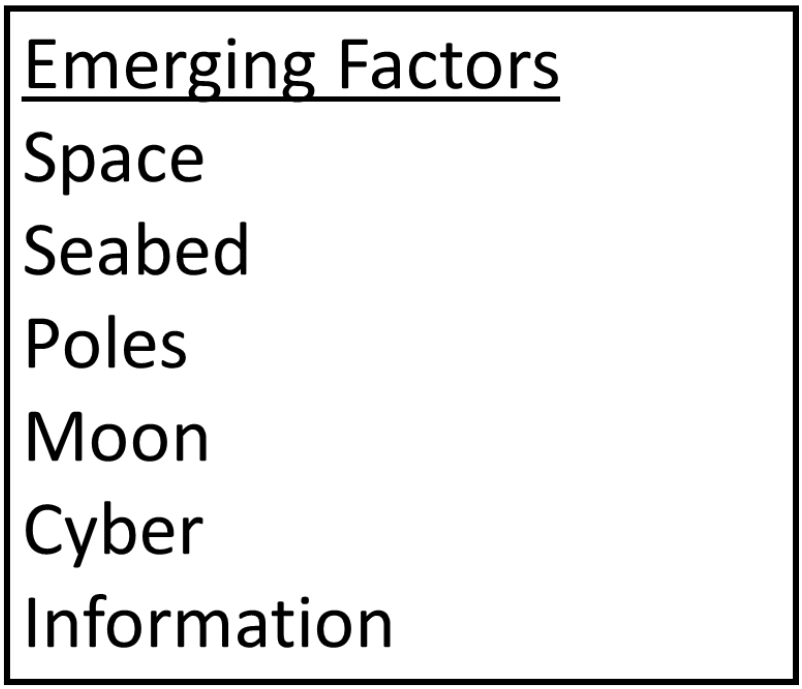
46. Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense*, *in* 87 INT'L L. STUD. 59, 71–72 (Raul A. "Pete" Pedrozo & Daria P. Wollschlager eds., 2011).

47. *See id.*; Megret, *supra* note 26, at 132 (noting that the notion of the traditional "battlefield" is disappearing).

48. THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 214 (Michael N. Schmitt ed.) (forthcoming March 2013).

49. *Id.* at 212, *see generally* Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L.J. 815, 838–841 (2012).

C. EMERGING FACTORS



The lack of limitation to breathable air zones will move armed conflict to areas where it is currently not occurring.[50] Future armed conflicts will occur without respect to national borders, on the seabed, under the ground, and in space.[51] It will also occur across the newly recognized domain of cyberspace.[52] And it will occur in all of these places simultaneously.

The United States has already demonstrated in its "Global War on Terror" that the LOAC is not well prepared to regulate an armed conflict against a transnational non-state terrorist actor who does not associate itself with geographic boundaries.[53] The waning geographic affiliation and increasing global social affiliation which will be discussed more later will create transnational linkages between previously unconnected people

50. *See* Hopkins, *supra* note 22.

51. *Id.*

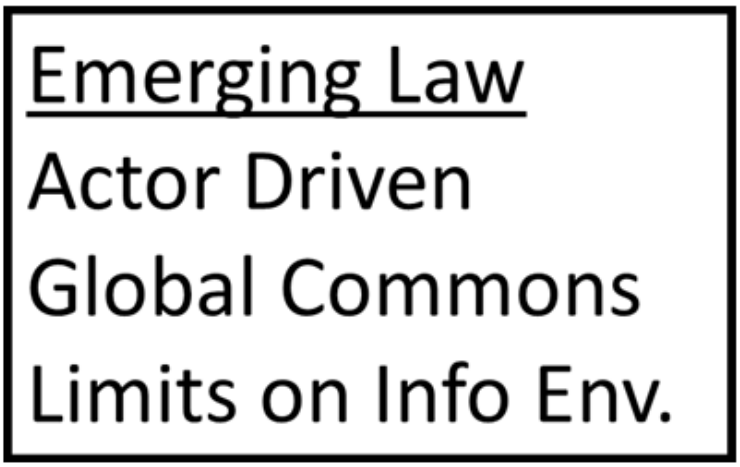
52. Alexander, *supra* note 14.

53. Megret, *supra* note 26, at 132 (arguing that the "death of the battlefield significantly complicates the waging of war and may well herald the end of the laws of war as a way to regulate violence).

will make identifying the battlefield extremely difficult. Mackubin Owens has written that "multidimensional war in the future is likely to be characterized by distributed, weakly connected battlefields."[54]

Few of these areas have seen armed conflict to this point.[55] And perhaps that will continue. However, as technology advances and these areas become available for weaponization, or at least for the placement of sensors, the temptation to militarize these areas will be irresistible.[56]

D. EMERGING LAW



Many of these individual domains just discussed are regulated by a treaty regime. For example, the Outer Space Treaty discourages military activities in space.[57] There is also a treaty which prohibits the use of nuclear weapons on the ocean floor or seabed.[58] These international agreements will become

54. Mackubin Thomas Owens, *Reflections on Future War*, 61 NAVAL WAR C. REV. 61, 71 (2008).

55. *See* Hopkins, *supra* note 22 (suggesting more sophisticated tools of cyber-warfare exist but have rarely been used).

56. *Id.* (suggesting the potential to conduct future military operations in space and cyberspace).

57. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies arts. 3-4, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 201.

58. Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and Ocean Floor and in the Subsoil Thereof, Feb. 11, 1971, 23 U.S.T. 701, 955 U.N.T.S. 115.

more and more difficult to apply and to comply with.[59]

Even if states continue to regard these rules as binding in the face of the transformation of geographic boundaries, these agreements still serve only to bind states.[60] The continuing diversification of actors in armed conflict will force states to consider whether they should remain militarily outside of these areas while non-state actors begin to operate within;[61] states will reconsider their legal obligations and take actions to establish control in these currently unmilitarized areas.[62] Laws might form to authorize states to exclude non-state actors from operating in these areas.[63] A new regime established around the global commons, ensuring state access but allowing states to enforce exclusion to non-state actors, could develop.[64]

Many possibilities exist for resolution here, but the new legal answer will revolve around actors, rather than geographic boundaries. The commons will be accessible by certain actors, rather than open to all.

This focus on actors and their impact on the places where armed conflict will occur in the future provides an excellent transition to the next area of emphasis—actors in future armed conflict.

59. *See* Doswald-Beck, *supra* note 4 ("In the light of such developments, States cannot continue to simply assume that the present scope of application of humanitarian law treaties suffices.").

60. *See id.* ("Recent attempts by the government of Colombia to indicate clearly that the new treaty banning antipersonnel mines applies to non-State entities ran into difficulties when certain Western governments could not accept the proposition that such entities might have responsibilities under international law.").

61. Mégret, *supra* note 26, at 145, 148-151.

62. *See id.* at 149, 151 ("However, it is not only 'transnational terrorists' who fundamentally change the nature of the battlefield, but also the states that chose to follow them on that terrain, effectively fighting 'a war' as if it unfolded on a 'global battlefield.'. . . [H]umanitarians have been tempted to extend the scope of the battlefield to make sure that as much violence as possible falls under its constraints.").

63. See Wolff Heintchel von Heinegg, *Current Legal Issues in Martime Operations*, 80 INT'L L. STUD. 207, 216 for precedent on exclusion zones in the context of, and questionable legality, under traditional LOAC.

64. *See id.*

II. ACTORS

The Geneva Conventions and Additional Protocols categorize everyone in armed conflict as either combatants or civilians.[65] The United States continues to assert that there is a small category of individuals who exist in the twilight between these two categories, most recently known as "unprivileged belligerents."[66] Within the category of civilians are individuals who forfeit their protections by taking a "direct part in hostilities."[67] As the post 9-11 "War on Terror" has progressed, this category has been understood to include organized armed groups[68] (e.g. terrorist organizations). There is much we could

65. Geneva Convention Relative to the Treatment of Prisoners of War, arts. 3, 4, 6, Aug. 12, 1949, U.S.T. 3316, 75 U.N.T.S. 135; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 50, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

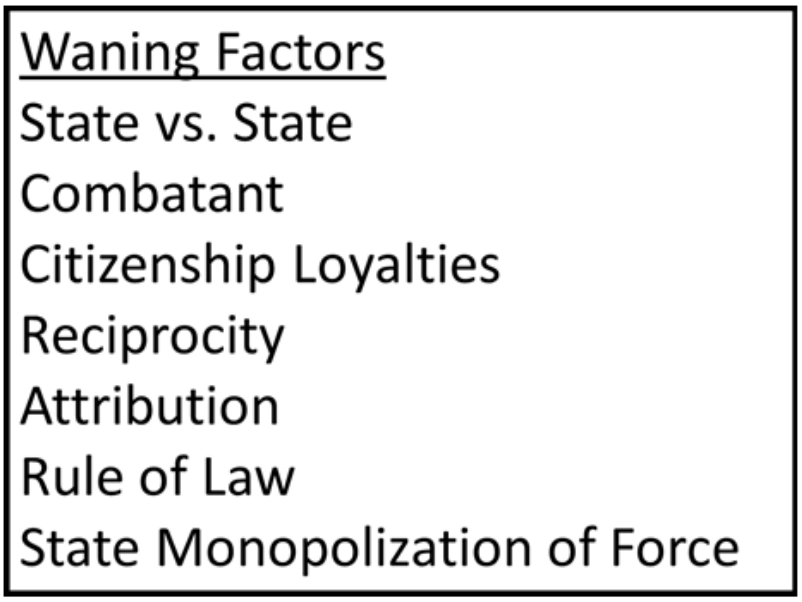
66. *See* In re Guantanamo Bay Detainee Litigation, Respondents' Memorandum Regarding the Government's Detention Authority Relative to Detainees Held at Guantanamo Bay, In Re: Guantanamo Bay Detainee Litigation, NO. 08-0442 (D.D.C., filed March 13, 2009); *Prosecuting Terrorists; Civilian and Military Trials for GTMO and Beyond: Hearing Before the Subcomm. on Terrorism, Technology and Homeland Security of the S. Comm. on the Judiciary*, 111th Cong. 47 (2009) (statement of Michael J. Edney, Counsel, Gibson, Dunn & Crutcher, LLP.).

67. Protocol I, *supra* note 65, art. 51.

68. Nils Melzer, Int'l Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 90 INT'L REV. RED CROSS 991, 1006-09

say about these categorizations, but the waters on these issues will get deeper and murkier.

A. WANING FACTORS



As mentioned previously, the LOAC was formulated largely based on a Westphalian model of state sovereignty.[69] Principles such as reciprocity[70] and the state's monopolization of force[71] were foundational principles which undergird the LOAC, especially the provisions applying to actors on the battlefield. However, the notion of a battlefield populated by only organized state militaries who comply with all aspects of the LOAC is not what future battlefields will be like, if they ever were like that.[72] Modern battlefields are fluid and ill-defined spaces where the actors are seldom clearly identified[73]

(2008), *available at* http://www.icrc.org/eng/resources/documents/article/review/review-872-p991.htm.

69. *See generally* BOBBITT, *supra* note 23, at 75–143, 501–538.

70. *See* Doswald-Beck, *supra* note 4, at 41 ("[R]eciprocity did become important with the introduction of new rules in treaties, namely, the international law rule that parties need to be bound by the treaties in question.").

71. Jensen, *supra* note 15, at 708, 715.

72. Kellenberger, *supra* note 36.

73. Sean Watts, *Law-of-War Perfidy* (unpublished manuscript) (on file with author.).

and often not even present at the place of attack.[74]

The vast majority of the armed conflicts in recent decades have not been between states, but between states and non-state actors or between two groups of non-state actors.[75] Advancing technologies will make this phenomena even more pronounced.[76] The ability of non-state actors to exert state-level violence combined with the diminishing association of individuals and groups to states will result in the waning of many factors currently prevalent in armed conflict.[77]

A result of the decreasing number of armed conflicts between states is that fewer and fewer conflicts occur between "combatants" and more and more involve some form of "fighters," whether those be organized armed groups, narco-terrorists, or individuals who are directly participating in hostilities.[78] The changing nature of participants in armed conflict should cause a reassessment of the applicability of the current LOAC paradigm. This process has already begun with the ICRC's issuance of the Interpretive Guidance on Direct Participation in Hostilities.[79] This tacit acceptance that the current understanding that the LOAC needs updated is a harbinger of things to come. Future armed conflict will undoubtedly increase the difficulty of defining actors on the battlefield.[80] The differentiation between fighters and non-fighters will become even more blurred as global technologies allow linkages and associations among people not contemplated in 1949 or 1977.[81]

In addition to the categorization of participants in armed

74. Megert, *supra* note 26, at 154 ("[T]his will cover crimes committed outside actual battle zones but that nonetheless display a strong element of connection to them.").

75. Themnér, Lotta Themnér & Peter Wallensteen, 2012. *Armed Conflicts by Type, 1946-2011*, 49(4) JOURNAL OF PEACE RESEARCH 565, 566, 568 (2012), *available at* http://www.pcr.uu.se/digitalAssets/122/122552_conflict_type_2011.pdf.

76. *See* Watts, *supra* note 46, at 61 ("Second, and related, CNA will produce a significantly expanded cast of players, creating a complex and uncontrollable multipolar environment comprising far more States and non-State actors pursuing far more disparate interests than in previous security settings. CNA are unprecedented conflict levelers.").

77. *See id.* at 62, 73, 76 ("Either one accepts a real threat to the positive jus ad bellum's claim to law, or one accepts very real threats to States' security as a trade-off for preserving legal idealism.").

78. *See* Jensen, *supra* note 15; Crawford, *supra* note 38, at 442.

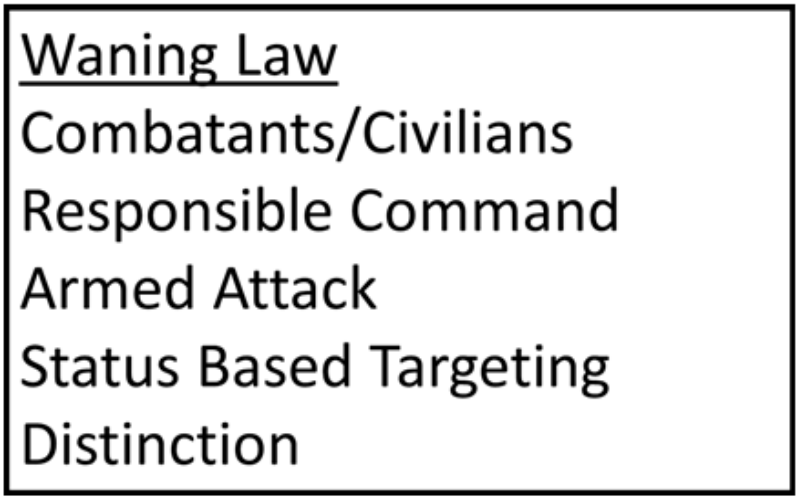
79. *See* Melzer, *supra* note 68.

80. *See* Mégret, *supra* note 26, at 138; Watts, *supra* note 46.

81. *See* Mégret, *supra* note 26, at 138; Brooks, *supra* note 2, at 677.

conflict, the ability to attribute actions in armed conflict to specific actors is being significantly undermined through the use of advancing technologies. Cyber operations are a good example of this difficulty. The difficulty of attributing cyber actions has been well documented.[82] The ability to hide one's identity or appear to be someone else is more problematic with stand-off weapons such as cyber weapons. Future weapons will continue to make attribution difficult, forcing the international community to reevaluate the approach to attribution.

B. WANING LAW



The increasing conflation of fighters and civilians will devalue the legal distinctions between combatant and civilian as categories that determine protections from targeting.[83] To the extent that the legal classification is useful in current armed conflicts, its utility will decrease as asymmetrical disadvantages force non-state fighters to seek anonymity while taking part in hostilities.[84]

The results of this conflation will undermine the current regime of status-based targeting and instead require most targeting decisions to be based on conduct.[85] Recent conflicts in

82. Collin Allan, *Attribution Issues in Cyberspace*, CHI.–KENT J. INT'L & COMP. L. (forthcoming May 2013).

83. Brooks *supra* note 2, at 730-31, 761.

84. *See* Watts, *supra* note 46, at 72-73.

85. *See* Brooks, *supra* note 2, at 706, 756-57 ("Thus, for instance, one's

Iraq and Afghanistan have already verified this emerging trend.[86] Status-based targeting will only be applicable to a very limited number of circumstances and will force states to look for other means of determining targets.[87]

The inability to meaningfully differentiate between actors on the battlefield will have a detrimental effect on the bedrock principle of distinction.[88] As states suffer devastating effects from non-attributable sources, the pressure for an evolved understanding of the principle of distinction will be great. For example, protecting a nation's critical infrastructure from computer attack[89] may be so important that attribution (and even individualized distinction) may become a casualty of the need to prevent significant social harm.[90]

status as a 'lawful combatant' under the Geneva Conventions hinges, as a threshold matter, not on one's substantive actions but on certain questions of form: whether one is under responsible command, whether one wears 'a fixed distinctive sign recognizable at a distance,' and whether one carries arms openly. . . . Status as a lawful combatant should not hinge on whether a person is 'commanded by a person responsible for his subordinates,' has a 'fixed distinctive sign recognizable at a distance' (e.g, a uniform or other sign by which combatants can be visually distinguished from civilians), or whether she 'carr[ies] arms openly.'").

86. *Id.* passim.

87. *See* Watts, *supra* note 46 ; Mégret, *supra* note 26.

88. *See* Mégret, *supra* note 26.

89. *See* Sean M. Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J. L. & TECH. 403, 421 (2007).

90. *See id.*

C. EMERGING FACTORS

At the sixty-year commemoration of the Geneva Conventions, then-President of the ICRC, Jakob Kellenberger, stated that "the potential range of 'new actors' whose actions have repercussions at the international level is of course vast. While many of these 'new actors' have in fact been around for some time, they have called into question—and will continue to call into question—some of the more traditional assumptions on which the international legal system is based."[91]

I divide my remarks in this area into two subcategories:

91. Jakob Kellenberger, President, Int'l Red Cross, Sixty Years of the Geneva Conventions and the Decades Ahead at the Conference on the Challenges for IHL posed by New Threats, New Actors and New Means and Methods of War, ICRC (Sept. 11, 2009), http://www.icrc.org/eng/resources/documents/statement/geneva-convention-statement-091109.htm.

emerging factors concerning influences on "existing actors" and emerging factors concerning "new actors." I will begin with the latter category.

This Article has already alluded to the break-down of geographic boundaries and the resulting traditional associations. Modern and future social networking capabilities will allow instantaneous linkages between individuals and groups from across the globe. These "instantaneous transnational communities of interest" mean that, as Jeffrey Walker argues, "[i]t's simply no longer necessary to have a state sponsor for an interested group of people to effect changes within the international community."[92] Anthony Lake describes how these instantaneous transnational communities of interest use "technology to forge vast alliances across borders, and . . . a whole host of new actors challenging, confronting, and sometimes competing with governments on turf that was once their exclusive domain."[93] Philip Bobbitt has written, "The internet enabled the aggregation of dissatisfied and malevolent persons into global networks."[94]

Social networking's effects on armed conflict have already been demonstrated during the Arab Spring.[95] The future effects of this phenomenon will undoubtedly increase over time. Audrey Kurth Cronin draws the analogy between social networking and the *levée en masse*. She argues that it allows cyber mobilization of people across the entire globe on issues of common ideology.[96] The result of this expanding social networking linkage is that people will begin to view themselves less as Americans or Germans or Iranians and more as members of global ideologies created, maintained, and mobilized through social media.[97] The resulting cultural

92. Jeffrey K. Walker, *Thomas P. Keenan Memorial Lecture: The Demise of the Nation-State, the Dawn of New Paradigm Warfare, and a Future Profession of Arms*, 51 A.F. L. REV. 323, 329330329-30 (2001).

93. Walker, *supra* note 92, at 330 (quoting ANTHONY LAKE, SIX NIGHTMARES: REAL THREATS IN A DANGEROUS WORLD AND HOW AMERICA CAN MEET THEM 281–82 (2000)).

94. Philip C. Bobbitt, *Inter Arma Enim Non Silent Leges, View of Law and War*, 45 SUFFOLK U. L. REV. 253, 259 (2012).

95. George Griffin, *Egypt's Uprising:Tracking the Social Media Factor*, PBS.ORG (Apr. 20, 2011), http://www.pbs.org/newshour/updates/middle_east/jan-june11/revsocial_04-19.html.

96. Audrey Kurth Cronin, *Cyber-Mobilization: the New Levée en Masse*, 36 PARAMETERS 77 passim (2006).

97. *See* Michigan State University News, *Civilian Cyber-Warriors Not*

uncertainty will provide a means and incentive for like-minded individuals to connect and interact on areas of agreement that are not determined by geographic borders or national affiliation.

These groups will use social networks to recruit, gather resources, provide financial support, collect and pass intelligence, and create and transmit plans of action including attacks. The communications will occur far from where the effects of the communications will eventually be felt, but could conceivably have significant effects on ongoing armed conflicts.

A current example of a developing trend is the computer activist group known as "Anonymous."[98] In addition to state-affiliated hacking groups and their documented participation in armed conflict,[99] hacktivists, who have organized themselves around a social theme or ideology, such as the members of Anonymous, have also started to take part in armed conflict.[100]

While many of the participants are conscious of the influence of social networking on armed conflict, advancing technology will increase the likelihood that individuals and groups will become unwitting "direct participants." As will be discussed later, the use of future technologies such as virology and nanotechnology will allow attackers to increase the reach of their weapons by using the civilian population to propagate their weapons.[101] A DNA-coded virus will eventually reach its target after harmlessly passing through the population.[102]

Cyber attackers will use the same methodology. As with

Driven by Patriotism, MICH. ST. U. RES. (Sept. 10, 2012), http://research.msu.edu/tags/cyber-warriors.

98. *Anonymous*, N.Y. TIMES (Mar. 8, 2012), http://topics.nytimes.com/top/reference/timestopics/organizations/a/anonymous_internet_group/index.html.

99. Collin Allan, *supra* note 82; David E. Hoffman, *The New Virology: From Stuxnet to Biobombs, The Future of War by Other Means*, 185 FOREIGN POL'Y 78, 80 (2011), *available at* http://www.foreignpolicy.com/articles/2011/02/22/the_new_virology?print=yes&hidecomments=yes&page=full.

100. Jana Winter & Jeremy A. Kaplan, *Communications Blackout Doesn't Deter Hackers Targeting Syrian Regime*, FOXNEWS.COM (Nov. 30, 2012), http://www.foxnews.com/tech/2012/11/30/hackers-declare-war-on-syria/#ixzz2Ht69GA1J.

101. *Id.*

102. Andrew Hessel, Marc Goodman & Steven Kotler, *Hacking the President's DNA*, ATLANTIC MAG. (Nov. 2012), http://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/.

STUXNET,[103] malware will be fashioned to spread broadly through the internet but only cause damage to specific systems in a precision targeted attack.[104] For this to work, individual civilians and their computer systems will be a vital, though unwitting, part of the attack. Similarly, hacktivists, such as the members of Anonymous, participate along a spectrum of activity. Some may be writers of harmful code; others may be coordinators of the attack. Still others may simply leave their computers on, allowing those running the malware to slave their computers and put them to a nefarious use. In this way, they may become unwitting participants. However, to the individual or state being attacked, there will be almost no timely way of ascertaining the difference. Nations will struggle to deal with how to classify and then respond to such individuals, especially when the groups are extremely large and geographically dispersed.[105]

In addition to influences on actors, future technologies will create wholly new actors that are either a limited part, or not part at all, of the current paradigm.[106] These new actors will nonetheless emerge as important factors in future armed conflict. These include those who deal in new types of weapons—referred to as "new arms" dealers—global criminal enterprises, corporate armies and robots or autonomous weapon systems.

Advancing technology will provide a wide array of new weapons, many of which do not require state financing and organization to produce or market. In addition to computer hacktivists, bio engineers who are creating viruses and other DNA-linked tools are springing up around the world.[107] There is already a very lucrative market for cyber "arms." It is

103. *See Factbox: What is Stuxnet*, REUTERS (Sept.. 24, 2010), http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUSTRE68N3PT20100924.

104. *See* Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need For Modifications to the Law of Armed Conflict?* 35 FORDHAM INT'L L.J. 842 passim ((March 2012).

105. *See* Pierre Thomas &and Jack Cloherty, *FBI, Facebook Team Up to Fight 'Butterfly Botnet'*, ABC NEWS (Dec. 12, 2012), available at http://abcnews.go.com/Technology/butterfly-botnet-targets-11-million-including-computer-users/story?id=17947276.

106. *See* Watts, *supra* note 46.

107. Hanno Charisius, Richard Friebe & Sascha, & Karberg, *Becoming Biohackers: Learning the Game*, BBC FUTURE (Jan. 22, 2013), http://www.bbc.com/future/story/20130122-how-we-became-biohackers-part-1.

sourced almost exclusively by non-state actors.[108] A similar market for biological and genetic weapons will undoubtedly emerge.[109] Many of these individuals or groups will see this as a business, not as dealing in weapons. Nevertheless, in some instances, they will produce, transport, and even sometimes unleash these new types of weapons on the targets.

In addition to these relatively unorganized groups, a number of highly organized armed groups will emerge on the future battlefield. These include corporate armies, including private security companies (PSCs), and global criminal enterprises.[110] Recent events in Algeria[111] are making corporations rethink their reliance on state forces for protection of multi-billion dollar complexes. Corporate assets will continue to exist in unstable areas and even in areas of armed conflict. Businesses whose annual revenue exceeds that of the gross domestic product of the country in which they have assets are unlikely to continue to rely on state forces or police for protection if such protection fails. Rather, they will hire private security companies or raise their own armies to ensure the safety of their personnel and assets. ExxonMobil in Indonesia and Talisman Energy in Sudan have already "hired" and/or controlled national military forces to protect their business interests.[112] As armed conflicts ebb and flow, these corporate armies will inevitably become involved in armed conflicts, stressing the current application of the LOAC.[113] Corporate

108. Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BUSINESSWEEK (July 20, 2011), http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html.

109. *See* Charisius, *supra* note 107; Hessel, *supra* note 102.

110. *See generally* FROM MERCENARIES TO MARKET: THE RISE AND REGULATION OF PRIVATE MILITARY COMPANIES (Simon Chesterman & Chia Lehnhardt eds., 2007).

111. Aomar Ouali & Paul Schemm, *Al-Qaida-linked Militants Seize BP Complex in Algeria, Take Hostages Over Mali Intervention*, YAHOO! NEWS, Jan. 16, 2013, http://news.yahoo.com/al-qaida-linked-militants-seize-bp-complex-algeria-185156149.html.

112. Jonathan Horlick et al., *American and Canadian Civil Actions Alleging Human Rights Violations Abroad by Oil and Gas Companies*, 45 ALTA. L. REV. 653, 657–58 (2008); *see also Developments in the Law, International Criminal Law*, 114 HARV. L. REV. 1943, 2025, 2029–30 (2001).

113. *See generally* FROM MERCENARIES TO MARKET, *supra* note 110; Eric Talbot Jensen, *Combatant Status: Is it Time for Intermediate Levels of Recognition for Partial Compliance*, 46 VA. J. INT'L L. 214 (2005); Christopher J. Mandernach, *Warriors Without Law: Embracing a Spectrun of Status for Military Actors*, 7 APPALACHIAN J.L. 137 (2007). Christopher J.

armies have already been implicated in "unlawful taking of property, forced labor, displacement of populations, severe damage to the environment, and the manufacture and trading of prohibited weapons."[114] This trend will increase in the future.

Another emerging factor is the role played by global criminal enterprises. These would include organizations such as the narco-traffickers operating in Mexico and other parts of Central and South America.[115] Reports place the number of armed fighters supporting the narco-trafficking in Mexico alone at over 100,000.[116] This army is substantially larger than the armies involved in most recent armed conflicts.

Global criminal enterprises are also involved in other illegal activity, including money laundering, arms smuggling, counterfeiting, and the sex trade.[117] Criminal enterprises often have links to armed conflict because of the goods or services that they offer.[118] As demand for their goods increases, the number of criminal enterprises will only increase.

We have just heard a truly superb discussion on robotics and autonomous weapon systems.[119] I will just add a few comments of my own. I will revisit these weapons under the category of means and methods of warfare, but to the extent that robots or other similar weapons systems become autonomous, they must also be considered as actors. We have

114. Regis Bismuth, *Mapping a Responsibility of Corporations for Violations of International Humanitarian Law Sailing Between International and Domestic Legal Orders*, 38 DENV. J. INT'L L. & POL'Y 203, 204 (2010); *see also* Int'l Comm. of the Red Cross, *Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises Under International Humanitarian Law* 24 (2006); Erik Mose et al., *Corporate Criminal Liability and the Rwandan Genocide*, 6 J. INT'L CRIM. JUST. 947, 973–974 (2008).

115. Carina Bergal, Note, *The Mexican Drug War: The case for a Non-International Armed Conflict Classification*, 34 FORDHAM INT'L L.J. 1042, 1066–72 (2011).

116. *Id.* at 1066.

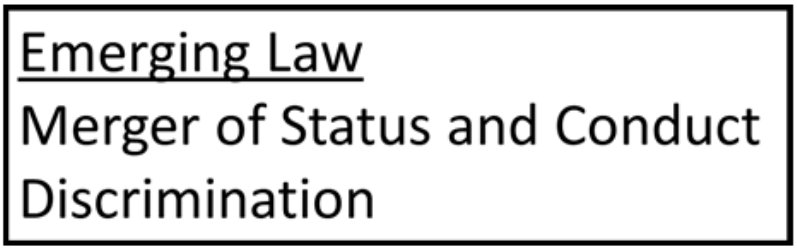
117. John Evans, *Criminal Networks, Criminal Enterprises*, UNIV. B. C., INT'L CTR. FOR CRIMINAL LAW REFORM, at 2, http://www.icclr.law.ubc.ca/publications/reports/netwks94.pdf (last visited Feb. 24, 2013).

118. *Id.*

119. To review these discussions, please see other Articles in 22 MINN. J. INT'L L. (Summer 2013), as well as some articles found in 23 MINN. J. INT'L L. (forthcoming Winter 2014). To see video recordings of the discussions that took place at the 2013 Symposium, please see the *Minnesota Journal of International Law's* website, http://www.minnjil.org/?page_id=913.

discussed both the Department of Defense's recently issued Directive titled "Autonomy in Weapon Systems,"[120] which says "autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force,"[121] and the Human Rights Watch report[122] calling for a multilateral treaty that would "prohibit the development, production and use of fully autonomous weapons."[123] My personal prognostication is that fully autonomous weapon systems will absolutely make their way onto the battlefield and eventually become the predominant actors. Having been in combat, I believe that controlled and regulated use of autonomous weapons systems can provide more reliable responses in many cases than relying on human senses and decision making. I am firmly convinced it is not a matter of "if," but "when."

D. EMERGING LAW



We could spend much more time discussing the emerging factors that will affect the actors in future armed conflict, but let's move to a discussion of the emerging law. I will highlight two points that I think are important to this discussion: the first is the merging of status and conduct by actors, and the second is the effects on the principle of discrimination.

120. DEP'T OF DEF., DIRECTIVE NO. 3000.09, AUTONOMY IN WEAPON SYSTEMS (Nov. 21, 2012). This Directive followed a DoD Defense Science Board Task Force Report issued in July of 2012. DEP'T OF DEF. DEF. SCI. BOARD, THE ROLE OF AUTONOMY IN DOD SYSTEMS (July 2012), *available at* http://www.fas.org/irp/agency/dod/dsb/autonomy.pdf.

121. DEP'T OF DEF., DIRECTIVE NO. 3000.09, AUTONOMY IN WEAPON SYSTEMS (Nov. 21, 2012).

122. HUMAN RIGHTS WATCH, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS (2012), *available at* http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf.

123. *Id.* at 5, 46.

As alluded to previously, individuals are targeted based on either their status as combatants or fighters or on their inappropriate conduct as civilians. Emerging technologies and tactics will make states want to blur these distinctions. For example, the members of "Anonymous" who are preventing the military leadership from communicating to subordinates are likely taking a direct part in hostilities and are therefore targetable. However, if the attack is generated by thousands of slaved computers, some owned by witting participants, others by unwitting participants, what are the targeting options for the target state? Further, is the civilian recreational hacker who develops the malware or establishes the botnet targetable?

In the area of virology, is the designer of the DNA-linked virus targetable, even if he or she is just selling it to a customer? It is unclear if that individual would be a direct participant, especially if he did not know the eventual target of the viral attack. What about an organization who sells such DNA-linked viruses to the highest bidder? What about the completely unwitting carrier of the virus who is about to enter the auditorium where the President is about to speak and doesn't know that she is going to infect the President with the lethal virus?[124]

Transnational social networking communities present similar problems. As individuals pass along vital information, including attack plans, do they become targetable? Their counterparts in a geographically contained kinetic conflict would be. Does the fact that these interactions occur thousands of miles from the intended event and the originating group make a targeting difference?

Transitioning now to the principle of discrimination, the LOAC requires attackers to discriminate in the attack.[125] We could have a long discussion about what the word "attack" means with respect to these new technologies, but I will delay that to discuss the impact of new actors on the principle of discrimination. Much has already been said about the need for human discretion in the attack as it relates to autonomous weapon systems. I will add my own thoughts just to say that the requirement is that the attack is discriminate, not that a human make the decision as to whether to conduct the attack

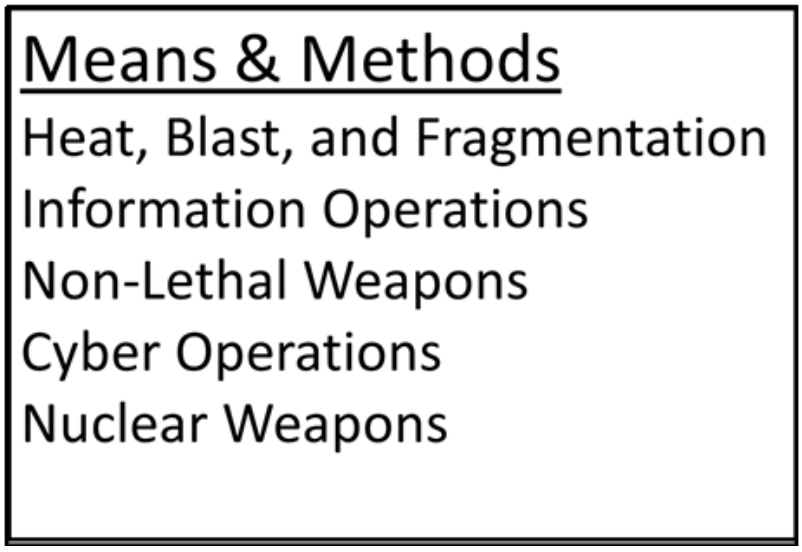
124. Hessel, *supra* note 102.

125. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51, *supra* note 25, 1125 U.N.T.S. at 29.

or not.

We are making and using computer malware that is making the ultimate decision on discrimination in the attack. Stuxnet had been programmed to and was presumably acting on its own when it identified the computer controlling the centrifuges and then conducted the "attack" on that computer. Emerging weapon systems will increasingly be making those decisions through automated or natural processes that are based on controlled circumstances. To the extent that our current interpretation of discrimination is bothered by that, we may have to evolve that LOAC understanding. I think it is clear that autonomous weapons on the battlefield will increase, and the autonomy of those weapon systems will also increase. To the extent that we need to adjust the current understanding of discrimination in the attack, the LOAC needs to be responsive and evolve in order to ensure that these "actors" act responsibly.

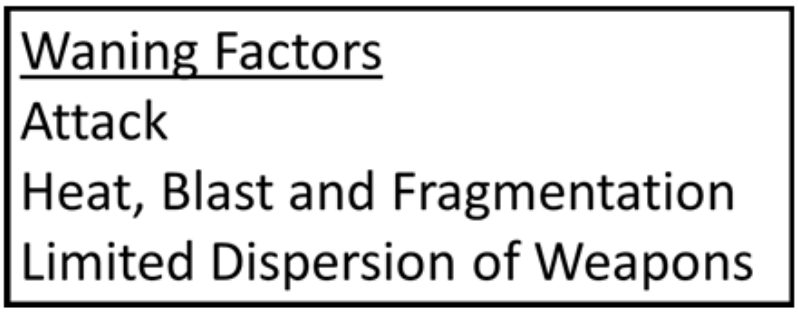
III. MEANS AND METHODS



Moving now to means and methods of warfare, since the development of gunpowder, modern conflicts have been characterized by heat, blast, and fragmentation. We have recently included some innovative means of conflict including numerous non-lethal weapon systems which have proven to be

very effective. You will also note that I have cyber operations in the category of existing means and methods, though I do not believe that states have even begun to tap into the potential cyber operations presents.

A. WANING FACTORS



Despite the fact that all of these means and methods will continue to be a vital part of future armed conflicts, they will not maintain the role they currently have. For example, while most weapons will still likely use heat, blast, and fragmentation as the primary source of injury, the proportion of such weapons that are produced and used in any armed conflict will steadily decrease. As other weapons that use advanced technology enter the arsenal, they will provide more options to the commander and will better suit his needs. For example, if a commander had access to a DNA-linked virus that would effectively kill an enemy leader, he could avoid all the LOAC concerns such as proportionality and distinction that would be part of a targeting analysis using heat, blast, and fragmentation weapons such as a missile.

Similarly, the idea of an "attack" will wane in the face of new weapons. The meaning of attack is defined in API as "acts of violence against the adversary, whether in offence or in defence."[126] This definition is mired in the armed conflict of heat, blast, and fragmentation which was characterized by violence. However, such a definition is not clear enough to adequately address the weapons of the future. Is a cyber-attack an act of violence? What about infecting someone with a virus? Certainly the victim of the DNA-linked virus is attacked, but what about the intermediate carrier who is merely infected but

126. *Id.* art. 49, at 25.

has no effects?

The important point this raises is that if infecting a host carrier (or a thousand host carriers) with a DNA-linked virus that has no physical effects is not an attack, the majority of the LOAC principles would not apply to that action and would not limit a commander's ability to conduct such an action. A similar analysis applies to cyber actions. Cyber operations that merely cause inconvenience are likely not attacks and can therefore potentially be targeted at civilians.[127] Given the underlying purposes of the LOAC, it is unlikely that this understanding of "attack" can survive these new weapon systems and will have to evolve to provide the protections expected from the LOAC.

One of the characteristics of heat, blast, and fragmentation weapons was a limited dispersal. The military has computer programs which model the blast radius of weapons to assist commanders in making a correct proportionality analysis. The limited dispersion of the weapon system is not an exact science, but it is generally discernible. This may not be true of many future weapon systems.

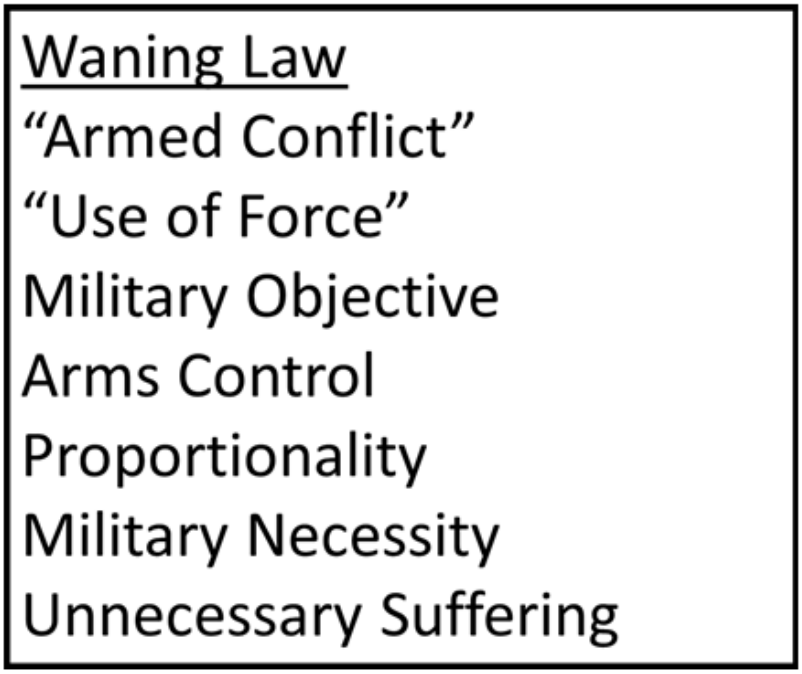
Stuxnet again provides an interesting perspective on this topic. Despite its creators' apparent best attempts, the malware made it onto computers that it was not intended to infect.[128] Though it did not have negative effects on those computers,[129] its dispersal was still not tightly controlled. Similar problems will occur with other future weapons systems. The inability to project the actual dispersal of some future weapons will make this a waning principle in the conduct of future armed conflict.

127. *See* THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 18, at 91–95, 133.

128. *See* Holger Stark, *Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War*, SPEIGEL ONLINE, Aug. 8, 2011, http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html.

129. Richmond, *supra* note 104, at 860–61.

B. WANING LAW



I anticipate that my list of waning law will be quite controversial, but remember that I am not necessarily saying that these principles will disappear. My argument is that they will wane as we currently know them. For example, though it is not a LOAC principle, consider for a minute the *jus ad bellum* principle of "use of force" as used in the UN Charter. This is applicable here because presumably a use of force would be governed by the LOAC. What level of cyber operation equates to a "use of force?" There are differing views, though I think the predominant view now is the effects test initially set out by Michael Schmitt. However, like the previous discussion of "attack," these legal terms need to evolve to maintain their currency and ability to regulate future armed conflict.

Similarly, the LOAC defining principle of "armed conflict" will wane as well. The LOAC is not triggered until there is an armed conflict. Traditionally, this required some level of hostilities.[130] In an era of bloodless weapons, as Blake and

130. *See generally* Commentary, Convention Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 22–23 (Jean S. Pictet ed., 1960),

Imburgia call them,[131] is the trigger of "armed conflict" going to be clear enough to regulate conflict? When is a cyber-operation "armed?" Or the dispersion of nanobots? Or the spreading of **GENOMIC** altering viruses?

These weapons will also make us reconsider time-honored LOAC principles such as military objective, unnecessary suffering, and proportionality. For example, one of the potentially unanticipated consequences of Stuxnet is that it has the possibility of being reengineered and reused.[132] Bernhard Langner who first discovered Stuxnet warns that such malware can proliferate in unexpected ways: "Stuxnet's attack code, available on the Internet, provides an excellent blueprint and jump-start for developing a new generation of cyber warfare weapons. . . . Unlike bombs, missiles, and guns, cyber weapons can be copied. The proliferation of cyber weapons cannot be controlled. Stuxnet-inspired weapons and weapon technology will soon be in the hands of rogue nation states, terrorists, organized crime, and legions of leisure hackers."[133]

The possibility of reengineering raises an interesting question about the proportionality analysis for commanders. With heat, blast, and fragmentation weapons, commanders did not have to concern themselves with the potential of the weapon being reused. However, with cyber malware such as Stuxnet, or with a DNA-linked virus, or with a genetic mutation, the malware, or virus or mutation remain and can be reengineered, reused and resold, potentially leading to significant impacts, including death and injury, on civilians who were never even implicated in the original attack. Must the commander consider this potentiality as he does his proportionality analysis prior to using the weapon? I think the LOAC does not yet provide a clear answer for that question. To the extent that experts have opinions, I have found them to differ widely.

Finally, another waning legal norm is arms control. Arms

available at http://www.icrc.org/ihl.nsf/COM/375-590007?OpenDocument.

131. Duncan Blake & Joseph S. Imburgia, *"Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons"*, 66 A.F. L. REV. 157 (2010).

132. *See* Mark Clayton, *From the Man Who Discovered Stuxnet, Dire Warnings One Year Later*, CHRISTIAN SCI. MONITOR (Sept. 22, 2011), http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later.

133. David E. Hoffman, *supra* note 42 (*quoting* Ralph Langer, the German industrial control systems security expert who discovered Stuxnet).

control has been an effective means of limiting states in the production and use of certain weapons, such as chemical[134] or biological agents,[135] as well as nuclear weapons.[136] However, these international agreements have legally bound states but do not reach non-state actors. In an age where many new means and methods of warfare are not controlled or controllable by states, but can be created in an individual's garage[137] or office, arms control agreements lose much of their value. Until the international community finds a way to get individuals to agree to weapons controls and voluntarily comply, arms control agreements will have limited utility for many future weapon systems.

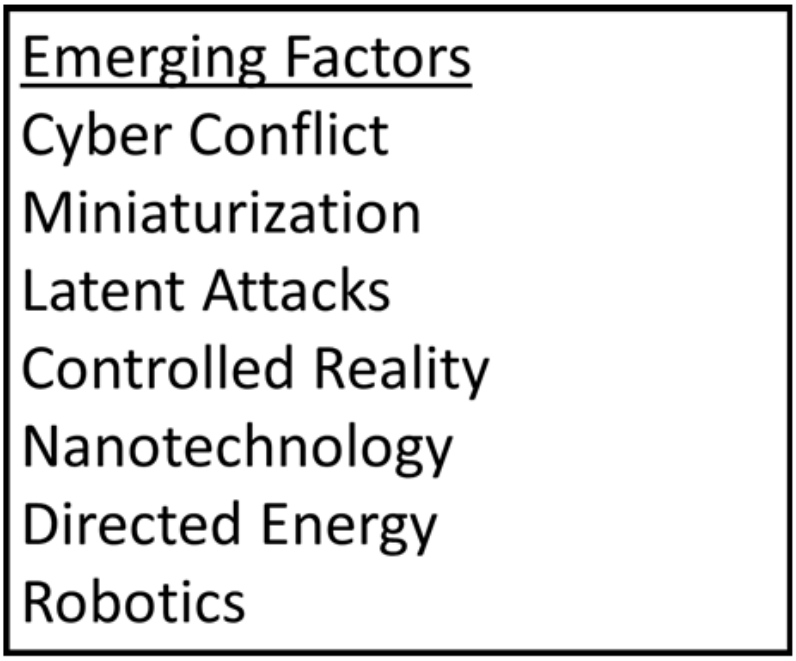
134. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, *opened for signature* Jan. 13, 1993, 3 U.N.T.S. 1974.

135. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, *opened for signature* Apr. 10, 1982, *available at* http://www.icrc.org/ihl.nsf/FULL/450?OpenDocument.

136. Treaty on the Non-Proliferation of Nuclean Weapons, *opened for signature* July 1, 1968, 21 U.S.T. 483 (entered into force Mar. 5, 1970).

137. Wil S. Hylton, *How Ready Are We for Bioterrorism*? N.Y. TIMES, Oct. 26, 2011, http://www.nytimes.com/2011/10/30/magazine/how-ready-are-we-for-bioterrorism.html?pagewanted=all&_r=0.

C. EMERGING FACTORS



U.S. Deputy Defense Secretary William J. Lynn III recently stated that "few weapons in the history of warfare, once created, have gone unused."[138] This quote reinforces the point demonstrated by the Lateran Council that once a weapon or technology that can be weaponized is developed, it almost inevitably ends up on the battlefield. Specific arms control regimes have had some success in this area, but the general rule is that technology drives weapon development and those developed are eventually used in warfare.

I will start with cyber conflict. While cyber technology is not really new, its future uses leave it squarely in the category of emerging factors. The potential uses, and dangers, of cyber technology are only beginning to be understood. Cyber capabilities were viewed by top national security professionals and policymakers as the most dangerous of emerging capabilities in a recent survey conducted by *Foreign Policy*.[139]

138. John D. Banusiewicz, *Lynn Outlines New Cybersecurity Effort*, FED. INFO. & NEWS DISPATCH, INC., June 16, 2011.

139. *See The FP Survey: The Future of War*, FOREIGN POL'Y, Mar./Apr. 2012, http://www.foreignpolicy.com/articles/2012/02/27/The_Future_of_War?print=ye

Of course, the general availability of cyber means of armed conflict is part of what causes the concern. Many nations, including both China and the United States, have institutionalized their cyber forces.[140] A recent estimate suggests that 140 nations already have or are actively building cyber capabilities within their military.[141] The recent malware packages known as Stuxnet, Flame, and Red October aptly illustrate that states are already using cyber space to conduct military activities that cause harm, similar to kinetic operations.[142]

Additionally, non-state actors and even individuals have access to cyber weapons. Symantec estimates that Stuxnet could be created by as few as five to ten highly trained computer technicians in as little as six months.[143] Non-state actors have been known to develop sophisticated malware that cause great damage.[144]

---

s&hidecomments=yes&page=full (ranking cyberwarfare at a 4.6 on a 1-7 scale, 1 being the largest threat and 7 being the least threat); Micah Zenko, *The Future of War*, FOREIGN POL'Y, Mar./Apr. 2011, http://www.foreignpolicy.com/articles/2011/02/22/the_future_of_war. (Mar./Apr.

140. *See* Tania Branigan, *Chinese Army to Target Cyber War Threat*, THE GUARDIAN, July 22, 2010, http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department; Andrew Gray, *Pentagon Approves Creation of Cyber Command*, REUTERS, June 23, 2009, http://www.reuters.com/article/2009/06/24/us-usa-pentagon-cyber-idUSTRE55M78920090624; Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 96 (2009).

141. Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties*, 13 SMU SCI. & TECH. L. REV. 249, 249 (2010).

142. *See STUXNET Malware Analysis Paper,* CODEPROJECT (Sep. 11, 2011), http://www.codeproject.com/Articles/246545/Stuxnet-Malware-Analysis-Paper (explaining Stuxnet was created to sabotage Iran's nuclear program); *Full Analysis of Flame's Command and Control Servers*, SECURELIST (Sep. 17, 2012), http://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers (explaining Flame malware, the advanced cyber-espionage tool, was a large scale campaign targeting several countries in the Middle East); *Red October Computer Virus Found*, TELEGRAPH (Jan. 14, 2013), http://www.telegraph.co.uk/technology/news/9800946/Red-October-computer-virus-found.html (explaining Red October focused targeting countries in eastern Europe).

143. Josh Halliday, *STUXNET Worm is the 'Work of a National Government Agency'*, THE GUARDIAN, Sept. 24, 2010, http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency.

144. *See* David Kleinbard & Richard Richtmyer, *U.S. Catches 'Love' Virus: Quickly Spreading Virus Disables Multimedia Files, Spawns Copycats*, CNNMONEY, May 5, 2000, http://money.cnn.com/2000/05/05

Moving on to nanotechnology, it is "the understanding and control of matter at the nanoscale, at dimensions between approximately 1 and 100 nanometers, where unique phenomena enable novel applications."[145] Nanotechnology has already proven its value.[146] For example, "a nanoparticle . . . has shown 100 percent effectiveness in eradicating the hepatitis C virus in laboratory testing."[147] The U.S Government Accountability Office reported:

> From fiscal years 2006 to 2010, the National Science and Technology Council (NSTC) reported more than a doubling of National Nanotechnology Initiative (NNI) member agencies' funding for nanotechnology environmental, health, and safety (EHS) research—from approximately $38 million to $90 million. Reported EHS research funding also rose as a percentage of total nanotechnology funding over the same period, ending at about 5 percent in 2010.[148]

And the United States is not alone. China and Russia are also "openly investing significant amounts of money in nanotechnology."[149]

As with other innovations, nanotechnology is well on its way to being at the forefront of military operations. Between

/technology/loveyou/ (describing how the "I Love You" virus swept through banks, securities firms, and Web companies causing damage).

145. *What it is and How it Works*, NAT'L NANOTECHNOLOGY INST., http://nano.gov/nanotech-101 (last visited Feb. 6, 2013).

146. David Brown, *Making Steam Without Boiling Water, Thanks to Nanoparticles*, WASH. POST, Nov. 19, 2012, http://articles.washingtonpost.com/2012-11-19/national/35505658_1_steam-nanoparticles-water ("It shows you could make steam in an artic environment.").

147. Dexter Johnson, *Nanoparticle Completely Eradicates Hepatitis C Virus*, IEEE SPECTRUM (July 17, 2012), http://spectrum.ieee.org/nanoclast/semiconductors/nanotechnology/nanoparticle-completely-eradicates-hepatitis-c-virus?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IeeeSpectrumSemiconductors+%28IEEE+Spectrum%3A+Semiconductors%29; *see also "Nanorobot" Can be Programmed to Target Different Diseases*, PHYS.ORG, July 16, 2012, http://phys.org/news/2012-07-nanorobot-diseases.html (explaining the programmable nature of the nanoparticle makes it useful against cancer and other viral infections).

148. *US Government Accountability Office Releases Report on Nanotechnology EHS Research Performance*, NANOWERK, June 22, 2012, http://www.nanowerk.com/news2/newsid=25691.php.

149. *See* Blake & Imburgia, *supra* note 131, at 180.

2001 and 2006, the Department of Defense spent over $1.2 Billion on nanotechnology research.[150] Blake and Imburgia argue that nanotechnology will significantly affect future weapons and warfare. They write:

> Scientists believe nanotechnology can be used to develop controlled and discriminate biological and nerve agents; invisible, intelligence gathering devices that can be used for covert activities almost anywhere in the world; and artificial viruses that can enter into the human body without the individual's knowledge. So called 'nanoweapons' have the potential to create more intense laser technologies as well as self-guiding bullets that can direct themselves to a target based on artificial intelligence. Some experts also believe nanotechnology possesses the potential to attack buildings as a 'swarm of nanoscale robots programmed only to disrupt the electrical and chemical systems in a building,' thus avoiding the collateral damage a kinetic strike on that same building would cause.[151]

Nanotechnology will also eventually produce more powerful and efficient bombs, and result in miniature nuclear weapons.[152] It will lead to the creation of microscopic nanobots that can act as sensors to gather information or as weapons to attack humans.[153] The results of nanotechnology will be

150. Josh Wolfe & Dan van den Bergh, *Nanotech Takes on Homeland Terror*, FORBES.COM, Aug. 14, 2006, http://www.forbes.com/2006/08/11/nanotech-terror-cepheid-homeland-in_jw_0811soapbox_inl.html.

151. *See* Blake & Imburgia, *supra* note 131, at 180.

152. *Military Uses of Nanotechnology: The Future of War*, THENANOAGE.COM, http://www.thenanoage.com/military.htm (last visited Feb. 7, 2013).7, 2013).

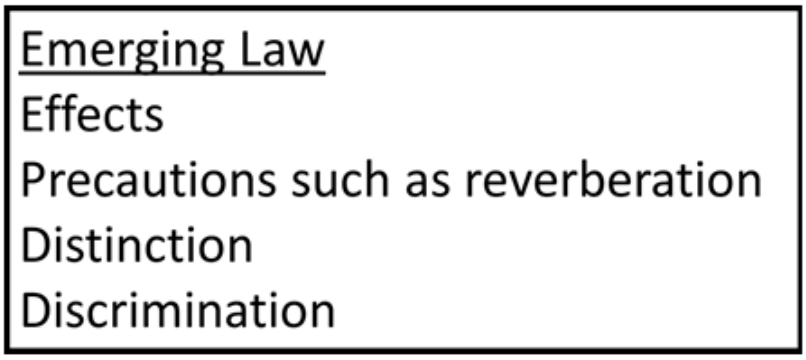
153. Scientists and the University of California, Berkeley, are already working on the Micromechanical Flying Insect Project; *see Micromechanical Flying Insect*, U.C. BERKELEY, http://robotics.eecs.berkeley.edu/~ronf/mfi.html/index.html (last visited Feb. 7, 2013) (describing the goal of micromechanical flying insect project is to develop a 25 mm device capable of sustained autonomous flight); *Nanotech Weaponry*, CENTER FOR RESPONSIBLE NANOTECHNOLOGY (Feb. 12, 2004), http://www.crnano.typepad.com/crnblog/2004/02/nanotech_weapon.html (explaining molecular manufacturing could lead to a weapon capable of seeking and injecting toxin into unprotected humans); Caroline Perry, *Mass-Production Sends Robot Insects Flying*, LIVE SCI., Apr. 18, 2012,

weapons that are smaller, more mobile, and more potent; sensors that are quicker and more accurate, and platforms with greater range, effect, and lethality.

In addition to the means of warfare I have discussed, let me also discuss a method of attack—the method of latent attack. A latent attack is when a weapon of some kind is placed in position, but will not be triggered until sometime in the future. The attack may be triggered by a signal sent by the weapon's creator or even by the victim's own actions. Though possible with viruses and nanotechnology delivery systems, the classic latent attack is done via computer malware.[154] The application of this form of emerging warfare as it relates to sales of weapons or military equipment is significant.

To illustrate, assume the United State sells F-16 aircraft to other countries, some of which the United States is not sure will remain allies. As a precautionary measure, the aircraft engineers embed some code in the targeting system that prevents that aircraft from targeting United States aircrafts. Such a valuable capability and tactic raises interesting legal issues which I will discuss next.

D. EMERGING LAW



Emerging technology will require emerging law. There are

http://www.livescience.com/19773-mini-robot-production-nsf-ria.html (stating a new technology will soon allow clones of robotic insects to be mass produced).

154. The Los Alamos National Laboratory in New Mexico, responsible for maintaining America's arsenal of nuclear weapons, discovered its computer systems contained Chinese-made network switches which are used to manage data traffic on computer networks. *See* Steve Stecklow, *U.S. Nuclear Lab Removes Chinese Tech Over Security Fears*, REUTERS, Jan. 7, 2013, http://www.reuters.com/article/2013/01/07/us-huawei-alamos-idUSBRE90608B20130107.

two particular areas of emerging law that I will discuss and both need to evolve in order to keep pace with advancing technologies. The first emerging area of law is the principles of distinction and discrimination.

Article 48 of API states the foundational LOAC principle of distinction: belligerents may "direct their operations only against military objectives."[155] API Article 51, paragraph 2 reinforces that norm: "The civilian population as such, as well as individual civilians, shall not be the object of attack."[156] In contrast, the principle of discrimination, or the prohibition on indiscriminate attacks, comes from API Article 51.4, and prohibits attacks which are "not directed at a specific military object" and "those which employ a method or means of combat which cannot be directed at a specific military objective" or "which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."[157] The principle of discrimination is considered "an implementation of the principle of distinction."[158]

Future weapons present options that are difficult to analyze under the existing law. For example, assume that the United States wants to kill a foreign enemy leader and chooses to do so by way of a DNA-linked virus. In order to get the virus into the vicinity of the enemy leader, a covert operator spreads the virus liberally in the area where the covert operator frequents. The virus will infect thousands of civilians but will only have a lethal effect on the enemy leader. I remind you, first of all, that these restrictions only apply to "attacks." Analyzing the law, one might argue that API Article 51.4(c) would preclude the attack because it was "of a nature to strike military objectives (the enemy leader) and civilians or civilian objects without distinction." However, one might equally make the argument that the attack did not "strike" civilians; it merely used or inconvenienced civilians. The attack ultimately discriminated when it finally exercised its lethal payload on the

155. *See* Protocol I, *supra* note 65, art. 48.

156. *See id.* art. 51.2.

157. *See id.* art. 51.4.

158. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 43 (Cambridge Univ. Press 2005), *available at* http://www.icrc.org/eng/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.

enemy leader. Is infecting the general populace a violation of distinction even though the virus is absolutely discriminating in the attack?

Jeremy Richmond made a similar analysis of the Stuxnet computer malware and concluded that had it been used during armed conflict, it would have complied with the LOAC despite its general dispersion.[159] Further clarity in this area of emerging technology will provide guidance to states as future technologies develop and continue to be used.

I have already introduced the idea of precautions and the potential impact of re-engineering as a factor in the commander's proportionality analysis. API Article 57 requires that commanders do "everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects"[160] and "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[161]

Does that mean that a commander cannot choose to use a weapon that can potentially be re-engineered and used again against civilians? Or does it mean that he has to weigh the likelihood of it being re-engineered and the likelihood of it being used against civilians? Or does it mean that he has to do everything feasible to prevent it from being re-engineered without having to consider the potential effects if it is?

Currently, the law is unclear as to the application of the proportionality standard to this analysis. This is another area where, as technology advances, the law should advance as well.

IV. CONCLUSION

Let me now conclude with a quote from David Ignatius. He stated:

> The 'laws of war' may sound like an antiquated concept in this age of robo-weapons. But, in truth, a clear international legal regime has never been more needed: It is a fact of modern life that people in conflict zones live in the perpetual cross hairs of deadly weapons. Rules

159. *See* Richmond, *supra* 104, at 894.
160. *See* Protocol I, *supra* note 65, art. 57.2(a)(i).
161. *See id.* art. 57.2(a)(ii)

> are needed for targets and targeters alike.[162]

I would add that it is not just people living in combat zones, but potentially people anywhere in the world are in the cross hairs of deadly weapons.

Now is the time to act. In anticipation of these developments, the international community needs to recognize the gaps in the current LOAC and seek solutions in advance of a future situation. As the LOAC evolves to face anticipated future threats, it will help ensure that advancing technologies comply with the foundational principles of the LOAC and future armed conflicts remain constrained by law.

162. David Ignatius, *Dazzling New Weapons Require New Rules for War*, WASH. POST, Nov. 11, 2010; *see generally* Gary Marchant, Douglas Sylvester & Kenneth W. Abbott, *Nanotechnology Regulation: The United States Approach*, *in* NEW GLOBAL FRONTIERS IN REGULATION: THE AGE OF NANOTECHNOLOGY 189 (Graeme Hodge et al. eds., 2007); Kenneth W. Abbot, Douglas S. Sylvester & Gary E. Marchant, *Transnational Regulation of Nanotechnology: Reality or Romanticism?*, *in* INTERNATIONAL HANDBOOK ON REGULATING NANOTECHNOLOGIES (Edward Elgar ed., forthcoming); Kenneth W. Abbott, Gary E. Marchant, & Douglas J. Sylvester, *A Framework Convention for Nanotechnology*, 36 ENVTL. L. REP. 10931 (2006); Gary E. Marchant, Douglas J. Sylvester & Kenneth W. Abbott, *A New Soft Law Approach to Nanotechnology Oversight: A Voluntary Product Certification Scheme*, 28 UCLA J. ENVTL. L. & POL'Y. 123 (2010).

Places
Air, Land, Sea
Actors
Combatants
Civilians
DPH
Terrorists
Organized Armed Groups
Narco Terrorists
Means & Methods
Heat, Blast, and Fragmentation
Information Operations
Non-Lethal Weapons
Cyber Operations
Nuclear Weapons
Warfare Factors
Breathable Air Zones
Geographic Boundaries
State Centric System
Context
Time/Temporal Limits
Warfare Law
LOAC Bifurcation
Declaration of War
Sovereignty
Neutrality
In bello/ad bellum
Conflict Termination
Warfare Factors
State vs. State
Combatant
Citizenship Loyalties
Reciprocity
Attribution
Role of Law
State Monopolization of Force
Warfare Law
Combatants/Civilians
Resp. Command
Armed Attack
Status Based Targeting
Distinction
Warfare Factors
Weapons
Heat, Blast and Frag.
Limited Dispersion of Weapons
Warfare Law
"Armed Conflict"
"Use of Force"
Military Objective
Arms Control
Proportionality
Military Necessity
Unnec. Suffering
Emerging Factors
Space
Seabed
Poles
Moon
Cyber
Information
Emerging Law
Actor Driven
Global Commons
Limits on Info Env.
Emerging Factors
Robotics
Human "Tools"
Social Networks
Corporate Armies
"New Arms" Dealers
Cultural Uncertainty
Global Criminal Enter.
Arms/Actors Ebay
Lawfare
Emerging Law
Merger of States and Conduct
Discrimination
Emerging Factors
Cyber Conflict
Miniaturization
Latent Attacks
Controlled Reality
Nanotechnology
Directed Energy
Robotics
Emerging Law
Effects
Precautions such as reverberation
Distinction
Discrimination

12-31-2007

The ICJ'S Uganda Wall: A Barrier to the Principle of Distinction and an Entry Point for Lawfare

Eric Talbot Jensen
BYU Law, jensene@law.byu.edu

THE ICJ'S "UGANDA WALL": A BARRIER TO THE PRINCIPLE OF DISTINCTION AND AN ENTRY POINT FOR LAWFARE

ERIC TALBOT JENSEN[a]

To determine the magnitude, causes, distribution, risk factors and cumulative burden of injury in a population experiencing armed conflict in northern Uganda since 1986...we took a multistage, stratified, random sampling from the Gulu district...1 of 3 districts in Northern Uganda affected by war since 1986... A similar rural district (Mukono) not affected by war was used for comparison...Of the study population, 14% were injured annually...Only 4.5% of the injured were combatants...The annual mortality of 7.8/1000 in Gulu district is 835% higher than that in Mukono district.[1]

The risk to civilians in armed conflict has steadily risen since World War II,[2] and the United Nations currently estimates that ninety percent of the casualties in modern armed conflict are women and children, presumably civilians.[3] This is particularly deplorable given that the 1949 Geneva Convention Relative to the

---

[a] Lieutenant Colonel, Chief, International Law Branch, The Office of The Judge Advocate General, U.S. Army. B.A., Brigham Young University (1989); J.D., University of Notre Dame (1994); LL.M., The Judge Advocate General's Legal Center and School (2001); LL.M. Yale University (2006). The author wishes to thank Professor W. Michael Reisman for his superb instruction and mentorship, and Christian Behrendt, Anthony Buti, and Jason Morgan-Foster for their comments on prior drafts. The views expressed in this article are those of the author and not The Judge Advocate General's Corps, the United States Army, or the Department of Defense.

1. Ronald R. Lett, Olive Chifefe Kobusingye, & Paul Ekwaru, *Burden of Injury During the Complex Political Emergency in Northern Uganda*, 49 CAN. J. OF SURGERY 51, 51 (2006).

2. *See, e.g.*, Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F. L. REV. 1, 75 (2005). *See also* Lett, et al., *supra* note 1, at 51 (stating, "The proportion of civilian war-related deaths has increased from 19% in World War I, 48% in World War II, to more than 80% in the 1990s. Civilians are used as shields to protect the military, abducted, enslaved, tortured, raped and executed.").

3. UNICEF, CHILDREN IN CONFLICT AND EMERGENCIES, http://www.unicef.org/protection/index_armedconflict.html; See also Lisa Avery, The Women and Children in Conflict Protection Act: An Urgent Call for Leadership and the Prevention of Intentional Victimization of Women and Children in War, 51 LOY. L. REV. 103, 103 (2005) (stating, "During the last decade alone, two million children were killed, another six million were seriously injured or left permanently disabled, and twice that number of children were rendered homeless by the ravages of war.").

Protection of Civilian Persons in Time of War[4] (GCC) was written in response to the dramatic numbers of civilian casualties in World War II.[5] There are, undoubtedly, a number of reasons for this increase.[6] However, one of the most significant reasons for the rise in civilian deaths has been the mingling of combatants[7] with civilians on the battlefield.[8]

Nowhere has this been more obvious than in the recent conflict in Iraq. Not only have insurgents such as Abu Musab al-Zarqawi specifically targeted civilians,[9] but they have also refused to distinguish themselves from the civilian population.[10] Rather, they have chosen to blend in with the local populace,

---

4. Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S 287 [hereinafter Convention Relative to the Protection of Civilians].

5. *See, e.g.*, LTC Paul Kantwill & MAJ. Sean Watts, *Hostile Protected Persons or "Extra-Conventional Persons:" How Unlawful Combatants in the War on Terrorism Posed Extraordinary Challenges for Military Attorneys and Commanders*, 28 FORDHAM INT'L L.J. 681, 725 (2005), *and* Reynolds, *supra* note 2, at 58; HISTORY LEARNING SITE, CIVILIAN CASUALTIES OF WORLD WAR II, http://www.historylearningsite.co.uk/civilian_casualties_of_world_war.htm (estimating civilian casualties to amount to more than half of the total casualties during WWII).

6. *See* Judith Graham & Michelle Jarvis, *Women and Armed Conflict: The International Response to the Beijing Platform for Action*, 32 COLUM. HUM. RTS. L. REV. 1, 10-11 (2000) (arguing that the use of indiscriminate weapons such as landmines is a significant factor; *and* R George Wright, *Combating Civilian Casualties: Rules and Balancing in the Developing Law of War*, 38 WAKE FOREST L. REV. 129, 131 (2003) (arguing that some weaker foes intentionally target civilians for the sake of military necessity or perceived necessity).

7. Geneva Convention Relative to the Treatment of Prisoners of War, art. 4, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (Though there may be a few exceptions, persons on the battlefield can generally be divided into three categories: combatants, noncombatants, and civilians. Combatants are those members of the armed forces that meet the qualifications of Article 4 of the Geneva Convention Relative to the Treatment of Prisoners of War); Convention Respecting the Laws and Customs of War on Land, Annex to the Convention Regulations Respecting the Laws and Customs of War on Land, § 1, ch. 1, art. 3, Oct. 18, 1907, 1907 U.S.T. LEXIS 29, 1 Bevans 631 (Noncombatants are also members of the armed forces under Article 3 of the Annex on Regulations Respecting the Laws and Customs of War on Land to the Hague Convention (IV) respecting the Laws and Customs of War on Land); Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I), art. 43, June 8, 1977, 1125 U.N.T.S. 3, *available at* http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (Noncombatants include combatants who meet the above definition who are *hors de combat* and other members of the armed forces such as chaplains and medical personnel. Civilians are not covered by the above definitions. However, in many cases, including works and articles cited herein, noncombatants is used more generally to include all who are not combatants).

8. Reynolds, *supra* note 2, at 75-77 (arguing that "concealment warfare," or the mixing of military personnel or targets with civilians, has been partially responsible for this increase).

9. John Ward Anderson & Jonathan Finer, *The Battle for Baghdad's Future; Three Years After Its Fall, Capital Is Pivotal to U.S. Success in Iraq, Officers Say*, WASH. POST, Apr. 9, 2006, at A17; Julian E. Barnes, *Sliding Toward an Uncivil War*, U.S. NEWS & WORLD REPORT, March 6, 2006, at 14-15; Gabriel Swiney, *Saving Lives: The Principle of Distinction and the Realities of Modern War*, 39 INT'L LAW. 733 (2005).

10. *See CNN Live Event: Coalition News Briefing* (CNN television broadcast Apr. 11, 2004) (Transcript No. 041101CN.V54) (BG Kimmitt stating, "At 4:45, while moving from (UNINTELLIGIBLE) to clear an armed enemy—a coalition force was ambushed by enemy elements of unknown size. Reports indicate at least 20 rocket grenades were observed during the course of the

making it much more difficult for coalition and Iraqi military to distinguish between the insurgents and the innocent bystanders.[11] The obvious result of such tactics is to increase the danger to civilians. This creates a difficulty for those who are trying to comply with the law of war.

> When faced with such opponents, militaries intent on complying with the Law of War struggle between the requirements of distinction and their desire to protect non-combatants, and the practical reality of protecting their force from fighters... who act as combatants when engaging in combat but dissolve into the crowd of non-combatants when faced with opposing military forces.[12]

This intermixing of combatants with civilians while engaging in hostilities violates one of the most fundamental principles of the law of armed conflict: the principle of distinction. This bedrock principle of the law of war requires those involved in conflict to mark themselves so they can be distinguished from those who are not involved in combat. The most common method of compliance is for combatants to wear a uniform, but other methods of setting a combatant apart from a non-combatant are also authorized.[13] By requiring distinction, both combatants and civilians know who is involved in the combat and who is not. Thus, they can both make informed decisions of how to proceed in a combat environment.

The derogation from the principle of distinction is among the most serious issues facing the law of war today.[14] As combatants relax the requirement obliging them to mark themselves, erosion of this distinction will lead to greater intermixing of combatants with civilians. Increased civilian casualties will inevitably result because of the inability to discern who is "targetable" and who is not. Unfortunately, the current trend in the development of the law of war seriously undermines the principle of distinction by allowing, or even encouraging, would-be fighters to evade distinguishing themselves. Instead, these combatants seek the protections of civilians while not accepting the responsibilities of eschewing combatants' acts. This is a devastating trend that must be reversed or it will result in the destruction of the current law of war.

---

engagement. Forty to 50 armed individuals were observed, some wearing black pajamas, uniforms, others wearing civilian clothes.").

11. *See CNN Live Sunday: U.S. Helicopter Shot Down in Iraq, Both Pilots Killed; 7 Chinese Citizens Taken Hostage in Iraq* (CNN television broadcast Apr. 11, 2004) (Transcript No. 041104CN.V36) (quoting a military spokesperson as saying:

> We are working at a disadvantage...The lack of uniforms, so that you can't define the enemy very well. And the intertwining of the enemy with combatants is very, very difficult. So you've got combatants and non-combatants mixed together intentionally...[I]f you think about just the way that, for instance, the Shi'ias could basically in this area right here, thousands of pilgrims on their way into this region right here, and the militia being able to just take off the black uniforms, and blend right in, into all those pilgrims).

12. Eric Talbot Jensen, *Combatant Status: It is Time for Intermediate Levels of Recognition for Partial Compliance*, 46 VA. J. INT'L. L. 209, 211 (2005).

13. Major William H. Ferrell, III, *No Shirt, No Shoes, No Status: Uniforms, Distinction, and Special Operations in International Armed Conflict*, 178 MIL. L. REV. 94, 106-09 (2003).

14. *See* George H. Aldrich, *The Hague Peace Conferences: The Laws of War on Land*, 94 AM. J. INT'L. L. 42, 42 (2000) (listing combatant status and protection of civilians as two of the top five areas of the law that need further development in the early 21st century).

This paper will briefly introduce the principle of distinction, reviewing its basis in customary international law and early conventional codifications. The Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflict (GPI) will then be analyzed and proffered as the beginning of the official derogation from the principle of distinction and the genesis of an increasing disregard of the requirement that combatants distinguish themselves from civilians. Two recent cases from the International Court of Justice (ICJ), the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory[15] and the Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo *v.* Uganda),[16] will then be discussed and criticized for promoting the same trend, giving official incentive for nations to use non-uniformed insurgents rather than official militaries who would be expected to comply with the law of armed conflict. The significant danger this poses to the law of war in the age of asymmetrical lawfare will then be illustrated. Finally, some recommendations will be made as to steps the international community can take to reinstate the principle of distinction and reinvigorate the protections afforded to civilians.

I. PRINCIPLE OF DISTINCTION

"At the very heart of the law of armed conflict is the effort to protect non-combatants by insisting on maintaining the distinction between them and combatants."[17] This principle "prohibits direct attacks on civilians or civilian objects"[18] and is codified in Article 48 of the GPI[19] which states, "In order to

15. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 131 (July 9) [hereinafter Advisory Opinion No. 131].

16. Case Concerning Armed Activities on the Territory of the Congo (Dem. Rep. Congo *v.* Uganda) (Order of Dec. 19, 2005), *available at* http://www.icj-cij.org/docket/files/116/10455.pdf (last visited Oct. 10, 2007) [hereinafter Dem. Rep. Congo v. Uganda].

17. W. Michael Reisman, *Holding the Center of the Law of Armed Conflict*, 100 AM .J. INT'L .L. 852, 856 (2006).

18. Michael N. Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 YALE HUM. RTS. & DEV. L.J. 143, 148 (1999).

19. Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I), *supra* note 7, at art. 48. (Concerning article 48, the Commentary to GPI states:

> The basic rule of protection and distinction is confirmed in this article. It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected in armed conflict, and for this purpose they must be distinguished from combatants and military objectives. The entire system established in The Hague in 1899 and 1907 (1) and in Geneva from 1864 to 1977 (2) is founded on this rule of customary law. It was already implicitly recognized in the St. Petersburg Declaration of 1868 renouncing the use of certain projectiles, (3) which had stated that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy." Admittedly this was concerned with preventing superfluous injury or unnecessary suffering to combatants by prohibiting the use of all explosive projectiles under 400 grammes in weight, and was not aimed at specifically protecting the civilian population. However, in this instrument the immunity of the population was confirmed indirectly);

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Commentary, part IV, § 1, ch. 1, art. 48, para.

ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[20] However, this principle only attained such general acceptance after a long history of slow evolution in the laws of armed conflict. This evolution began millennia ago and arose out of recognition that regulating conflict, even if only to a limited degree, would have benefits.[21]

Many ancient cultures had rules concerning the conduct of hostilities.[22] As these rules evolved through time and culture, their focus was to provide protections for those who were engaged in hostilities and were acceptable only if they provided some military advantage or fulfilled some military purpose.[23] For example, as early as the 5th century B.C., Sun Tzu wrote, "Treat the captives well, and care for them... Generally in war the best policy is to take a state intact; to ruin it is inferior to this."[24] Sun Tzu's apparent concern for captives and enemy property and persons was not born from a humanitarian desire to preserve his adversary but as part of the overall goal to conquer that enemy. Contrast Sun Tzu's tactics with that of the Roman armies during the 5th and 6th centuries. Although they had rules about military conduct in war, "Plunder was general; and no distinction was recognized between combatants and noncombatants"[25] because the military's need to plunder was too great. Similar approaches were taken by the Babylonians, Hittites, Persians, Greeks, and others.[26] Any protections granted to noncombatants and civilians grew generally out of a utilitarian view of warfare and not from an ideological desire to preserve them from the horrors of war.[27]

During the age of chivalry, the customs and usages of war continued to take a utilitarian view and developed rather intricate rules for plunder[28] and siege.[29]

1863, *available at* http://www.icrc.org/ihl.nsf/COM/470-750061?OpenDocument [hereinafter GPI Commentary].); *see also* Ferrell, III, *supra* note 13 (offering an excellent discussion on the practical application of the principle of distinction, and particularly the provisions of GPI, to special operations forces).

20. Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I), *supra* note 7, at art. 48.

21. *Id.* at Preamble.

22. *See, e.g.*, William Bradford, *Barbarians at the Gates: A Post-September 11th Proposal to Rationalize the Laws of War*, 73 MISS. L. J. 639, note 12 (2004).

23. *Id.* at 697-710 (presenting an excellent overview of this concept).

24. SUN TZU, THE ART OF WAR 76 (Samuel Griffith trans., Oxford Univ. 1963).

25. Thomas C. Wingfield, *Chivalry in the Use of Force*, 32 U. Tol. L. Rev. 111, 114 (2001) (giving an excellent overview of the laws of war during the Age of Chivalry).

26. Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II*, 47 NAVAL. L. REV. 176, 182-85 (2000).

27. *See, e.g.*, David B. Rivkin, Jr. & Lee A. Casey, *Leashing the Dogs of War*, THE NAT'L INTEREST, Fall 2003, at 6 (stating, "The reasoning behind the practical nature of both customary law and the Geneva Conventions was obvious: a humanitarian 'law' that impeded the ability of states to defend their vital interests would, in practice, amount to nothing but a series of pious aspirations.").

28. *See* Wingfield, *supra* note 25 at 115-16 (stating:

> To preserve discipline and guarantee a fair distribution, the booty was usually gathered centrally and then distributed after the battle to each soldier in accordance with his rank and merit. The precise

They contained a number of very important rules for relations between fighters, such as ransom[30] and parole,[31] as well as combat rules, such as the distinction between ruses and perfidy.[32] As the feudal system gave way to the rise of the nation state, and its dominance as the major player in international relations,[33] knights also gave way to the use of professional armies. While civilians had been incidental to the conflicts up to this point, this transition broadened the scope of who participated in hostilities. As Nathan Canestaro writes:

> The erosion of the line between civilians and the professional military began with the fundamental changes in warfare seen in the Napoleonic era. The expanding scale of warfare, the advent of popular revolutions in some European countries, especially France, and repeated clashes between professional soldiers and armed peasantry during the Napoleonic wars, brought commoners into warfare in significant numbers for the first time.[34]

With this increase in the scope of hostilities, the battlefield was prepared for a renewed focus on the laws governing war, including the consideration of noncombatants and civilians.

By the middle of the 19th century, nations began to codify the rules that had developed up to that point.[35] Examples of this include the 1863 Lieber Code,[36] the

---

customs governing the division of spoil varied from country to country, but everywhere this distribution created a legally recognized, heritable, and assignable right of property in the captured objects. Military historians have long admired the close coordination between English naval forces patrolling along the coast of northern France and the English land armies pillaging the interior of the country. The admiration is not misplaced; but it is worth remarking that this fleet not only provided food and supplies to the army. It also acted as a kind of floating safe-deposit box for the troops, who could be sure that their loot would get back to their families in England even if they did not survive the campaign).

29. *Id.* at 117-19 (stating:

> A siege began when a herald went forward to demand that a town or castle admit the besieging lord. If the town agreed, this constituted surrender, and the lives and property of the townspeople would be protected. If the town refused to surrender, however, this was regarded by the besieging lord as treason, and from the moment the besieger's guns were fired, the lives and property of all the town's inhabitants were therefore forfeit . . . . Strictly speaking, the resulting siege was not an act of war but the enforcement of a judicial sentence against the traitors who had disobeyed their prince's lawful command).

30. *Id.* at 116-17; Scott R. Morris, *The Laws of War: Rules by Warriors for Warriors*, 1997 ARMY LAW. 4, 4 (1997) (noting, "The practice of not killing one's captives, however, was rooted in fiscal reasons, not humanitarian reasons.").

31. *See* Maj. Gary D. Brown, *Prisoner of War Parole: Ancient Concept, Modern Utility*, 156 MIL. L. REV. 200, 201-08 (June, 1998).

32. *Wingfield, supra* note 25, at 131.

33. *See* Nathan A. Canestaro, *"Small Wars" and the Law: Options for Prosecuting the Insurgents in Iraq*, 43 COLUM. J. TRANSNAT'L L. 73, 83 (2004) (noting, "The principle that the right to wage war is limited to sovereign authority was asserted by the prominent Sixteenth Century legal scholar and father of international law, Hugo Grotius . . . .").

34. *Id.* at 84.

35. *See* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 706 (2004) (arguing that the codification of the modern law of armed conflict is a generally western notion).

36. DIETRICH SCHINDLER & JIRI TOMAN, THE LAWS OF ARMED CONFLICTS: A COLLECTION OF

1868 Declaration of St. Petersburg,[37] the unratified Brussels Conference of 1874,[38] the Hague Conventions of 1899 and 1907,[39] and the 1909 Naval Conference of London.[40] These conventions came to be known as the "Hague tradition."[41]

The Hague tradition, typified by the 1907 Hague Regulations, became the foundation upon which all modern laws of armed conflict are built,[42] and they embody concepts still valid today.[43] This Hague tradition focused on the

---

CONVENTIONS, RESOLUTIONS, AND OTHER DOCUMENTS 3 (3rd ed. 1988) (An analysis of the provisions of the Lieber Code show that it "acknowledge[s] the supremacy of the warrior's utilitarian requirements even though explicitly referring to the need to balance military necessity with humanitarian concerns."); Eric Krauss & Michael Lacey, *Utilitarian vs. Humanitarian: The Battle Over the Law of War,* PARAMETERS, Summer 2002, at 76, *available at* http://www.carlisle.army.mil/USAWC/Parameters/02summer/lacey.htm; Reynolds, *supra* note 2, at 7-8 (writing:

> The Lieber Code specifically prohibited the targeting of civilians and civilian objects. It also recognized that collateral damage should be avoided, but was acceptable if it was the result of an attack on a legitimate military objective. The Lieber Code articulates basic principles of the law of war, including the principle of military necessity in Articles 14 and 15. "Military necessity [consists of] . . . those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war." Further, "Military necessity admits of all direction of destruction of life or limb of armed enemies, and of other persons whose destruction is incidentally unavoidable . . . ." Lieber defined the principle of distinction when he stated, "the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit").

37. SCHINDLER & TOMAN, *supra* note 36, at 101, *available at* http://www.icrc.org/IHL.nsf/FULL/130?OpenDocument (stating in the preamble, "The only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy.").

38. *Id.* at 25, *available at* http://www.icrc.org/IHL.nsf/FULL/135?OpenDocument (though civilians are not defined, Article 9 deals with combatants and states:

> The laws, rights, and duties of war apply not only to armies, but also to militia and volunteer corps fulfilling the following conditions:
>
> 1. That they be commanded by a person responsible for his subordinates;
> 2. That they have a fixed distinctive emblem recognizable at a distance;
> 3. That they carry arms openly; and
> 4. That they conduct their operations in accordance with the laws and customs of war.
>
> In countries where militia constitute the army, or form part of it, they are included under the denomination 'army').

39. *Id.* at 63-103.

40. *Id.* at 843.

41. *See* Derek Jinks & David Sloss, *Is the President Bound by the Geneva Conventions?* 90 CORNELL L. REV. 97, 108-09 (2004) (stating:

> The jus in bello is further subdivided into Geneva law and Hague law. Comprised principally of the four 1949 Geneva Conventions and the two 1977 Additional Protocols, Geneva law is a detailed body of rules concerning the treatment of victims of armed conflict. Embodied principally in the 1899 and 1907 Hague Conventions, Hague law prescribes the acceptable means and methods of warfare, particularly with regard to tactics and general conduct of hostilities. Though Geneva law and Hague law overlap, the terminology distinguishes two distinct regimes: one governing the treatment of persons subject to the enemy's authority (Geneva law), and the other governing the treatment of persons subject to the enemy's lethality (Hague law). International humanitarian law embraces the whole jus in bello, in both its Geneva and Hague dimensions).

42. Christopher L. Blakesly, *Ruminations on Terrorism & Anti-Terrorism Law & Literature*, 57 U. MIAMI L. REV. 1041, 1064-65 (2003).

43. Int'l. & Operational Law Dep't, The Judge Advocate General's Legal Center and School, U.S.

combatants and was based on a utilitarian view of warfare not only to provide limited protections for fighters while in battle but also to maintain the warrior ethos of chivalry.[44] Commenting on the utilitarian nature of the Hague tradition, George Aldrich wrote, "The 1907 Hague Regulations contain very few provisions designed to protect civilians from the effects of hostilities. Aside from the prohibition on the employment of poison or poisoned weapons, which was primarily intended to protect combatants, the only such rules are Articles 25-28."[45]

This era of codification, steeped in the notion of the law of war being a tool for combatants rather than an external limitation, is typified by the statement traditionally attributed to the German Chancellor, Otto von Bismarck: "What leader would allow his country to be destroyed because of international law?"[46] International law was formed from the combatant's point of view, not the noncombatant.

Concurrent with the codification of the utilitarian law of war in the middle of the 19th century, others began exercising an increasingly prominent voice relating to the laws of armed conflict.[47] These voices expressed concern for the victims of armed conflict, which were initially combatants, but later included noncombatants and civilians. The founding of the International Committee of the Red Cross (ICRC) after Henri Dunant's experience at the 1859 Battle of Solferino[48] and the subsequent 1864 Convention for the Amelioration of the Condition of the Wounded in Armies in the Field[49] with its accompanying Additional Articles of 1868[50] are examples of the developing movement. This was followed by

---

ARMY, JA 422, OPERATIONAL LAW HANDBOOK, 12-15 (Derek I. Grimes ed., 2006).

44. *See Wingfield*, *supra* note 25, at 135-36.

45. *See* Aldrich, *supra* note 14, at 50 (continuing:

> Article 25 forbids the bombardment 'of towns, villages, dwellings, or buildings which are undefended.' By undefended, it was clear that the article meant that there were no defending armed forces in the town or other area in question or between it and the attacking force and consequently that it was open for capture by the attacker. It clearly did not apply to towns, villages, and so forth, that were in the hinterland and consequently were not open to immediate capture – or, in 1907, even to bombardment. Essentially, the article was a commonsense prohibition against bombarding something that could be taken without cost to the attacker. Articles 26 and 27 were precautionary measures, and neither suggests that its primary object was to minimize civilian casualties, although they might have provided some beneficial incidental effects for civilians in places under siege or bombardment. Article 28, which prohibits pillage, protects civilians only after the fall of the town or place and was necessary to make clear that the ancient custom permitting pillage of places that had resisted sieges was no longer acceptable).

46. *See* Chris af Jochnick & Roger Normand, *The Legitimation of Violence: A Critical History of the Laws of War*, 35 HARV. INT'L L.J. 49, 63-64 (1994).

47. *See* LOUISE DOSWALD-BECK, *Implementation of International Humanitarian Law in Future Wars, in* THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM 42 (Naval War College International Law Studies, vol. 71) (Michael N. Schmitt & Leslie C. Green eds., 1998) (arguing the advance in weapons technology also drove states to try and enact laws to limit warfare).

48. *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, *From the Battle of Solferino to the Eve of the First World War*, at http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/57JNVP (providing a concise history of Dunant, including the Battle of Solferino).

49. SCHINDLER & TOMAN, *supra* note 36, at 279.

50. *Id.* at 285.

continuing codifications such as the 1906 Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field.[51]

These humanitarian efforts focused on greater protections for combatants and became known as the "Geneva tradition"[52] because the ICRC was headquartered in Geneva, Switzerland, and many of the early conferences were held there. These innovations were welcomed by the combatants and are still accepted as imbedded in the practical realities of warfare.[53]

WWII exhibited an exponential rise in wartime costs to civilians, both in terms of lives lost and in property damage.[54] Increasingly lethal technology and weapons led to increasing effects on civilians.[55] "At the end of the nineteenth century, the overwhelming percentage of those killed or wounded in war were military personnel. Toward the end of the twentieth century, the great majority of persons killed or injured in most international armed conflicts have been civilian non-combatants."[56] This disturbing direction of warfare heightened the concern for the victims of warfare, particularly after the devastation of WWII.

In the years immediately following the war, a shifting of focus continued to add protections for combatants and noncombatants but also began to intertwine them with protections for civilians.[57] Codification of this shift began with the four 1949 Geneva Conventions.[58] While the first three Geneva Conventions[59] built upon preexisting established principles that survived WWII and were aimed at treatment of members of the armed forces, the Convention (IV) relative to the Protection of Civilian Persons in Time of War[60] extended certain protections to civilians based on their status as non-participants in the conflict.[61] All four conventions were advances in humanitarian law and proscribed many of the horrors of WWII in order to prevent them from occurring again. In fact, the fourth convention required military commanders to modify operations based solely on their potential effects on the civilians on the battlefield.

Underlying all four conventions was the idea that all persons on the battlefield could be divided into three distinct groups (combatants, noncombatants or

---

51. *Id.* at 301.

52. *See Wingfield*, *supra* note 25, at 134-35.

53. DOSWALD-BECK, *supra* note 47, at 41.

54. Compare the estimated number of deaths in WWII (http://www.valourandhorror.com/DB/BACK/Casualties.htm) with those in WWI (http://www.vw.cc.va.us/vwhansd/HIS122/WWIcasualties.html).

55. Richard R. Baxter, *So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs*, 28 BRIT. Y.B. INT'L L. 323, 326 (1951).

56. Aldrich, *supra* note 14, at 48.

57. *See* Rivkin & Casey, *supra* note 27, at 60-61.

58. Bradford, *supra* note 22, at 765-70.

59. SCHINDLER & TOMAN, *supra* note 36, at 305-425.

60. *Id.* at 427-85.

61. Krauss & Lacey, *supra* note 36, at 77 (noting, "[p]revious conventions had forced the utilitarians to deal with issues such as the treatment of the sick and wounded and prisoners of war . . . [t]he Civilian Convention for the first time placed affirmative obligations . . to address the food, shelter, and health-care needs of civilians").

civilians), and that it is unlawful to target those who were not combatants.[62] Although no definition was provided for persons who were not combatants, all who wanted the protections and privileges of prisoners of war were obliged to strictly comply with Article 4 of the Geneva Convention Relative to the Treatment of Prisoners of War (GPW).[63] This includes a requirement for all to distinguish themselves from the local populace who were not engaging in combatant activities.

In the two decades that followed the 1949 Geneva Conventions, the global political climate developed into a bi-polar world, with the United States and its North Atlantic Treaty Organization members directly opposing the Soviet Union and its supporting Warsaw Pact members. The most significant aspect of this bi-polar world was the lack of armed conflict between the major powers.[64] While many conflicts erupted across the globe, they were characterized by struggles for self-determination or other small-scale wars where nations acted as surrogates for the superpowers.[65] These wars were not characterized by the massing of large, uniformed, state-sponsored armies, but rather by small groups of often unorganized and un-uniformed freedom fighters.[66]

During one such war, the Vietnam War, numerous allegations arose that many of the provisions of the Geneva Conventions were disregarded,[67] including fighters not distinguishing themselves in the conduct of battle. In response to these violations and in an attempt to update the 1949 Geneva Conventions,[68] the ICRC led the world[69] in adopting the 1977 Protocols to the Geneva Conventions.[70]

---

62. Maj. Charlotte M. Liegl-Paul, *Civilian Prisoners of War: A Proposed Citizen Code of Conduct*, 182 MIL. L. REV. 106, 113 (2004); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257 (July 8), *available at* http://www.icj-cij.org/docket/files/95/7495.pdf [hereinafter Legality of the Threat Opinion] (holding, "The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following . . . States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets").

63. SCHINDLER & TOMAN, *supra* note 36, at 355-425.

64. *See* Diane P. Wood, *The Rule of Law in Times of Stress*, 70 U. CHI. L. REV. 455, 462-65 (2003).

65. *See* Thomas M. Franck, *The UN and the Protection of Human Rights: When, If Ever, May States Deploy Military Force Without Prior Security Council Authorization?*, 5 WASH. U. J.L. & POL'Y 51, 61 (2001).

66. *Id.* at 60-61.

67. Cara Levy Rodriguez, *Slaying the Monster: Why the United States Should Not Support the Rome Treaty*, 14 AM. U. INT'L L. REV. 805, n.130 (1999) (referencing the alleged American violations of the law of war); Jeffrey F. Addicott & William A. Hudson, *The Twenty-Fifth Anniversary of My Lai: A Time to Inculcate the Lessons*, 139 MIL. L. REV. 153, 174-75 (1993) (referencing the alleged North Vietnamese violations of the law of war); *Cf.* Adam Roberts, *The Laws of War: Problems of Implementation in Contemporary Conflicts*, 6 DUKE J. COMP. & INT'L L. 11, 43 (1995) (stating that law of war violations were not prosecuted during this time period because of the superpower deadlock between the United States and the Soviet Union).

68. Theodor Meron, *The Time Has Come for the United States to Ratify Geneva Protocol I*, 88 AM. J. INT'L L. 678, 679 (1994); Aldrich, *supra* note 14, at 45 ("In the years since the Geneva Conventions were concluded in 1949, the world has clearly changed greatly. A majority of the present states did not exist as states in 1949, and many of them gained their independence only after armed struggles against colonial powers.").

69. Lee A. Casey & David B. Rivkin, Jr., *Double-Red-Crossed*, THE NAT'L INT. 63, 67 (2005);

These Protocols, and particularly the Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (GPI), accomplished the complete amalgamation of the Hague and Geneva traditions, breaking through that invisible barrier that had seemed to divide the two regulatory streams,[71] but at the expense of the "historic rule" of distinction.[72]

II. GPI AND THE EROSION OF THE PRINCIPLE OF DISTINCTION

One hundred and sixty-seven states are parties to GPI,[73] with an additional five countries that have signed but not yet ratified the text,[74] including the U.S.[75] Article 1 of GPI states the coverage of the Protocol:

> Art 1. General principles and scope of application....
>
> 3. This Protocol, which supplements the Geneva Conventions of 12 August 1949 for the protection of war victims, shall apply in the situations referred to in Article 2 common to those Conventions.
>
> 4. The situations referred to in the preceding paragraph include armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination, as enshrined in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.[76]

The reference to Common Article 2 of the 1949 Geneva Conventions is important in that it limits the application both to whom and when it applies.[77] Common Article 2 states:

> Art 2. In addition to the provisions which shall be implemented in peace-time, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

Thomas J. Murphy, *Sanctions and Enforcement of the Humanitarian Law of the Four Geneva Conventions of 1949 and Geneva Protocol I of 1977*, 103 MIL. L. REV. 3, 46 (1984).

70. SCHINDLER & TOMAN, *supra* note 36, at 551-629.

71. Legality of the Threat Opinion, *supra* note 62, at 256 ("These two branches of the law applicable in armed conflict have become so closely interrelated that they are considered to have gradually formed one single complex system, known today as international humanitarian law.").

72. Reisman, *supra* note 17, at 856-57.

73. International Humanitarian Law –Treaties and Documents, available at http://www.icrc.org/ihl.nsf/CONVPRES?OpenView.

74. *Id.*

75. Vienna Convention on the Law of Treaties art. 18, May 23, 1969, 1155 U.N.T.S. 331; 8 I.L.M. 679 (1969) (As a signatory, but not party, to the GPI, the U.S. has the obligation to not "defeat the object and purpose" of its provisions).

76. SCHINDLER & TOMAN, *supra* note 36, at 558

77. Murphy, *supra* note 69, at 49.

> The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.
>
> Although one of the Powers in conflict may not be a Party to the present Convention, the Powers who are Parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.[78]

By their text, the application of the Conventions is limited to High Contracting Parties and to the three specific fact patterns: 1) declared war, 2) any other armed conflict even if the state of war is not recognized, and 3) partial or total occupation. The limit of the scope of the application to "High Contracting Parties" has been overcome by the acceptance of all four Geneva Conventions as customary international law, binding on all nations whether or not they are signatories.[79] However, the three specific fact patterns have not been expanded by any such generally accepted declaration. Therefore, that portion of the scope of common Article 2 is the substance that is directly incorporated into Article 1, paragraph 3, of GPI, limiting its scope and application.

Paragraph 4 of GPI, however, appears to expand the reach of the Protocol despite the language of paragraph 3.[80] In stating that "[t]he situations referred to in the preceding paragraph include armed conflicts which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination," the article establishes a potential overlap between the two paragraphs and the simultaneously promulgated Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protections of Victims of Non-International Armed Conflicts (GPII).[81]

GPII's scope and application is stated in Article 1:

> Art 1. Material field of application
>
> 1. This Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such

78. SCHINDLER & TOMAN, *supra* note 36, at 361-62.

79. *See* Marsha V. Mills, *War Crimes in the 21st Century*, 3 HOFSTRA L. & POL'Y SYMP. 47, 50 (1999).

80. Theodor Meron, *On the Inadequate Reach of Humanitarian and Human Rights Law and the Need for a New Instrument*, 77 AM. J. INT'L L. 589, 598 (1983); Murphy, *supra* note 69, at 49-50.

81. SCHINDLER & TOMAN, *supra* note 36, at 558.

> control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.
>
> 2. This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts.[82]

If the apparent division between the two Protocols is intended to be international versus non-international armed conflicts as the titles suggest, the scope of GPII was seriously eroded at inception by the expansion of GPI to include "armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination," conflicts that are the prototype for non-international, or internal, armed conflicts.[83] Further, similar to GPI, the statement that GPII "develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions or application" seems to be clear until the succeeding reference to Article 1 of GPI.

The United States strongly objects to this expansion of the coverage of the law of armed conflict and provides that as one of the reasons it refuses to ratify GPI.[84] In his Letter of Transmittal to the Senate, President Ronald Reagan stated:

> Protocol I is fundamentally and irreconcilably flawed. It contains provisions that would undermine humanitarian law and endanger civilians in war. One of its provisions, for example, would automatically treat as an international conflict any so-called "war of national liberation." Whether such wars are international or non-international should turn exclusively on objective reality, not on one's view of the moral qualities of each conflict. To rest on such subjective distinctions based on a war's alleged purposes would politicize humanitarian law and eliminate the distinction between international and non-international conflicts. It would give special status to "wars of national liberation," an ill-defined concept expressed in vague, subjective, politicized terminology.[85]

This is important to the present discussion because it was this expansion coupled with the desire to cover fighters engaged in "armed conflicts which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination" that has led to

---

82. *Id.* at 621.

83. *Id.* at 558. *But see* GPI Commentary, *supra* note 19, at para. 86-87, 90 (arguing that Common Article 2 initially contemplated inclusion of such conflicts, wars of liberation are really of an international character, and that wars of national liberation should be covered by the laws of armed conflict because of their characteristics, such as the intensity of the conflict).

84. *See* Remarks of Judge Abraham D. Sofaer, *The Position of the United States on Current Law of War Agreements*, 2 AM. U. J. INT'L L. & POL'Y 460, 463-71 (1987); Michael Lacey, *Passage of Amended Protocol II*, 2000 ARMY LAW. 7, n.3 (2000).

85. Ronald Reagan, *The U.S. Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims: Letter of Transmittal*, 81 AM. J. INT'L. L. 910, 911 (1987).

GPI's derogation from the principle of distinction.[86] By including those types of conflicts, which were traditionally not covered by the laws of combatant status, they included many fighters who traditionally do not comply with the requirements of combatant status.

Against the backdrop of expanded coverage, the Protocol then redefines the requirements for combatant status. After discussing a state's armed force in Article 43, GPI Article 44 provides:

> Article 44—Combatants and prisoners of war
>
> 1. Any combatant, as defined in Article 43, who falls into the power of an adverse Party shall be a prisoner of war.
>
> 2. While all combatants are obliged to comply with the rules of international law applicable in armed conflict, violations of these rules shall not deprive a combatant of his right to be a combatant or, if he falls into the power of an adverse Party, of his right to be a prisoner of war, except as provided in paragraphs 3 and 4.
>
> 3. In order to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack. Recognizing, however, that there are situations in armed conflicts where, owing to the nature of the hostilities an armed combatant cannot so distinguish himself, he shall retain his status as a combatant, provided that, in such situations, he carries his arms openly:
>
> (a) during each military engagement, and
>
> (b) during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate.
>
> Acts which comply with the requirements of this paragraph shall not be considered as perfidious within the meaning of Article 37, paragraph 1 (c).
>
> 4. A combatant who falls into the power of an adverse Party while failing to meet the requirements set forth in the second sentence of paragraph 3 shall forfeit his right to be a prisoner of war, but he shall, nevertheless, be given protections equivalent in all respects to those accorded to prisoners of war by the Third Convention and by this Protocol. This protection includes protections equivalent to those accorded to prisoners of war by the Third Convention in the

86. Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 1(4), June 8, 1977, 1125 U.N.T.S. 3, 16 I.L.M. 1391 [hereinafter Protocol on the Protection of Victims of International Armed Conflict].

> case where such a person is tried and punished for any offences he has committed.
>
> 5. Any combatant who falls into the power of an adverse Party while not engaged in an attack or in a military operation preparatory to an attack shall not forfeit his rights to be a combatant and a prisoner of war by virtue of his prior activities.
>
> 6. This Article is without prejudice to the right of any person to be a prisoner of war pursuant to Article 4 of the Third Convention.
>
> 7. This Article is not intended to change the generally accepted practice of States with respect to the wearing of the uniform by combatants assigned to the regular, uniformed armed units of a Party to the conflict.
>
> 8. In addition to the categories of persons mentioned in Article 13 of the First and Second Conventions, all members of the armed forces of a Party to the conflict, as defined in Article 43 of this Protocol, shall be entitled to protection under those Conventions if they are wounded or sick or, in the case of the Second Convention, shipwrecked at sea or in other waters.[87]

Article 44 was one of the most controversial provisions of the drafting convention,[88] and rightly so. It represents a significant change to the law of war. By reducing the requirement to participate in hostilities as a combatant to merely requiring an attacker to carry his arms openly,[89] the Protocol strikes a blow to the rule that has become the bedrock principle of civilian protection. As Professor Michael Reisman writes, "Article 44 constitutes a considerable relaxation, for at least one side to a conflict, of the historic requirement, as well as of the sanction that functioned as an enforcement mechanism. This change was not accomplished inadvertently."[90]

---

87. *Id.* at art. 44.

88. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 1949 para. 1684 (J. Pictet et al. eds., 1987), *available at* http://www.icrc.org/ihl.nsf/COM/470-750004?OpenDocument [hereinafter Pictet, COMMENTARY].

89. *See* Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (Article 4 of the GPW sets out the requirements for irregular forces to be given combatant status and prisoner of war privileges); Sofaer, *supra* note 84 at 466-67 (asserting that the provisions of article 44 undermine the protection for civilians and provide support for terrorist activities); John C. Yoo & James C. Ho, *The New York University-University of Virginia Conference on Exploring the Limits of International Law: The Status of Terrorists*, 44 VA. J. INT'L L. 207, 225-28 (2003) (discussing article 44 and arguing that it dilutes the protections to civilians by encouraging unlawful combatants such as terrorists to engage in hostilities without complying with the traditional requirements of article 4 of the GPW); *But see* Emanuel Gross, *Human Rights, Terrorism and the Problem of Administrative Detention in Israel: Does a Democracy Have the Right to Hold Terrorists as Bargaining Chips?*, 18 ARIZ. J. INT'L & COMP. LAW 721, 741-43 (2001) (arguing that the protections for civilians is still the main focus of the Protocol despite the expansion of the term combatant).

90. Reisman, *supra* note 17, at 858.

The target of this relaxation was "guerilla warfare," a "modern battlefield... phenomenon" which can not be ignored.[91] Pictet states in his commentary:

> Guerrilla fighters will not simply disappear by putting them outside the law applicable in armed conflict, on the basis that they are incapable of complying with the traditional rules of such law. Neither would this encourage them to at least comply with those rules which they are in a position to comply with, as this would not benefit them in any way.[92]

This argument makes a mockery of paragraph 3's recounting of the basis for the principle of distinction: "the protection of the civilian population from the effects of hostilities."[93] While it may widen the scope of those who are classified as combatants, it fatally blurs the distinction between combatants and civilians.

Specifically, by allowing battlefield fighters to attack without wearing a uniform or other distinguishing element, GPI has completely undermined the reciprocal underpinnings of the principle.

> The venerable requirement imposed on combatants that, to be lawful, they must wear uniforms and bear arms openly is an indispensable and easily implemented and policed means for protecting noncombatants. Without these distinctive insignia, belligerents cannot distinguish adversaries from civilians, with predictable results.[94]

The predictable results include increased civilian casualties, as has been so clearly illustrated by recent events in Iraq.[95] In a conflict where soldiers are incapable of discerning between civilians and illegal fighters, "They must decide either not to shoot those who appear to be noncombatants and risk being killed, or attempt to distinguish between combatants and noncombatants, and in doing so, knowingly accept the risk of killing noncombatants for self-preservation."[96]

---

91. Pictet, COMMENTARY, *supra* note 88, para. 1684.

92. *Id. But see* Nathaniel Berman, *Privileging Combat? Contemporary Conflict and the Legal Construction of War*, 43 COLUM. J. TRANSNAT'L L. 1, 19–20 (2004) (arguing that the delegates to the 1949 Geneva Conventions did not want to grant combatant protections to groups fighting against their own government).

93. Protocol on the Protection of Victims of International Armed Conflict, at art. 44, para. 3.

94. Michael Reisman, Holding the Center of the Law of Armed Conflict, 100 AM. J. INT'L. L. 852, 856 (2006); See also Derek Jinks, The Changing Laws of War: Do We Need a New Legal Regime After September 11?: Protective Parity and the Laws of War, 79 NOTRE DAME L. REV. 1493, 1497 (2004) (stating:

> the protection of noncombatants from attack is predicated on a clear distinction between combatants and noncombatants. If attacking forces cannot distinguish between enemy soldiers and civilians, this type of rule cannot work well....It is the goal of protecting innocent civilians that requires a sharp line between combatants and noncombatants).

95. Glenn Kutler, *Iraq Coalition Casualty Count*, iCasualties.org, http://icasualties.org/oif/IraqiDeaths.aspx (last visited July 28, 2007) (where claims of civilian deaths in Iraq are tracked and estimated. These large numbers of civilian deaths is attributable at least in part, if not in large part, to the intermixing of unlawful combatants with civilians); *CNN Live Event*, *supra* note 10; *CNN Live Sunday*, *supra* note 11.

96. Jensen, *supra* note 12, at 224; Mark D. Maxwell, *The Law of War and Civilians on the Battlefield: Are We Undermining Civilian Protections?* 9/1/04 MIL. REV 17, at 23 ("Absent this ability

President Reagan recognized this and stated in his Letter of Transmittal to GPI that it:

> would grant combatant status to irregular forces even if they do not satisfy the traditional requirements to distinguish themselves from the civilian population and otherwise comply with the laws of war. This would endanger civilians among whom terrorists and other irregulars attempt to conceal themselves. These problems are so fundamental in character that they cannot be remedied through reservations, and I therefore have decided not to submit the Protocol to the Senate in any form.[97]

Not content to stop at paragraph 3 with its dangerously relaxed provisions for combatant status, the Protocol explicitly confirms the disadvantage to uniformed militaries in paragraph 7 by requiring them to continue to fight in the traditional methods despite being faced with foes who do not.[98] It does not take much military savvy as an insurgent leader to figure out how to take advantage of a legal system where only one side is required to mark themselves as combatants and the other side has the opportunity to hide amongst those it is illegal for the uniformed armies to kill.

Thanks at least in part to the natural results of Protocol I's derogation from the combatant status requirements, Gabriel Swiney states, "[T]he Principle of Distinction is violated across the world, often openly so, and that problem is getting worse. Something must be done."[99] Something has been done. Two recent cases have been taken to the International Court of Justice (ICJ) giving this international adjudicative body a chance to reestablish the sanctity of the principle of distinction and halt or even reverse the path of erosion begun by GPI. Unfortunately, the ICJ did the exact opposite and turned a perverse authorization to conduct military operations from amongst the noncombatant population into an illicit incentive to do so.

---

to distinguish between lawful and unlawful combatants, an enemy might well be left with one of two targeting choices: do not engage any civilians, even though some are engaging its forces, or engage every enemy civilian on the battlefield. The latter choice will likely prevail."); Richard R. Baxter, *So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs*, 28 BRIT. Y.B. INT'L L. 323, 335 (1951) (arguing this as a reason why the existence of a *levee en masse* will likely force the invader to treat all civilians as hostile).

97. Ronald Reagan, *The U.S. Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims: Letter of Transmittal*, 81 AM. J. INT'L. L. 910, 911 (1987); Pictet, COMMENTARY, *supra* note 88, para. 1679 (Coming close to admitting the danger to civilians of this situation in the Commentary where he writes that "distinction between combatants and non-combatants may be more difficult as a result, but not to the point of becoming impossible.").

98. *See* Ferrell, *supra* note 13, at 105 (writing:

> [T]he [law of war] places a duty on parties to a conflict to distinguish combatants from civilians. This is a reciprocal duty, requiring all parties to distinguish among enemy combatants and civilians when conducting military operations and to ensure a party's own armed forces are distinguishable from enemy combatants and civilians.

99. Gabriel Swiney, *Saving Lives: The Principle of Distinction and the Realities of Modern War*, 39 INT'L LAW. 733 (2005) (arguing then for replacing the principle of distinction with the Principle of Culpability which is based on each individual's actions rather than his status as a noncombatant.).

III. THE ICJ INCENTIVIZES THE USE OF FORCES THAT DO NOT DISTINGUISH THEMSELVES

The ICJ was established at the San Francisco Conference of 1945[100] to be the "principal judicial organ" of the United Nations.[101] Its jurisdiction is non-compulsory[102] but limited to state parties[103] except for specific exceptions such as a request for an advisory opinion from the General Assembly.[104] It was just such a request from the General Assembly that precipitated the Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, known as the Wall Advisory Opinion.[105]

A. The Wall Advisory Opinion

In the Wall Advisory Opinion, the General Assembly asked the Court to provide an advisory opinion on the issue of:

> What are the legal consequences arising from the construction of the wall being built by Israel, the occupying Power, in the Occupied Palestinian Territory, including in and around East Jerusalem, as described in the report of the Secretary-General, considering the rules and principles of international law, including the Fourth Geneva Convention of 1949, and relevant Security Council and General Assembly resolutions?[106]

The question resulted from the construction of a large wall,[107] or fence as the Israeli Supreme Court called it,[108] that meandered through the occupied territory of the West Bank.[109] The ICJ determined that the wall was illegal for a number of reasons,[110] with one of its major objections being that the path of construction

---

100. Int'l Court of Justice, *The Court,* http://www.icj-cij.org/icjwww/igeneralinformation/ibbook/Bbookframepage.htm (for a short history of the ICJ).

101. *See* U.N. Charter, art. 92.

102. *See* STATUTE OF THE INT'L COURT OF JUSTICE, art. 36, 3 Bevans 1179; 59 Stat. 1031, T.S. No. 993.

103. *See id.* at art. 34.

104. *Id.* at arts. 65-68; U.N. Charter, art. 96

105. *See* Advisory Opinion No. 131, *supra* note 15.

106. *Id.* at para. 66.

107. This is the term used by the ICJ. *See* Karin Calvo-Goller, *Jurisdiction and Justiciability: More Than a Huge Imbalance: The ICJ's Advisory Opinion on the Legal Consequences of the Construction of the Barrier*, 38 ISR. L. REV. 165, 168-89 (2005) (arguing that the use of the term Wall illustrates the ICJ's purposeful misconstruing of the case); Emanuel Gross, *Combating Terrorism: Does Self-Defense Include the Security Barrier? The Answer Depends on Who You Ask*, 38 CORNELL INT'L L.J. 569, 571 (2005) (arguing that the Courts use of "this particular loaded term . . . would most likely cause people - even if unfamiliar with the issue - to feel a sense of aversion and antipathy towards a structure of this kind because of the immediate negative connotations of the expression.").

108. H.C.J. 2056/04 Beit Sourik Village Council v. The Government of Israel [2004] IsrSC 1 (Barak, C.J.) (The Israeli Supreme Court used the term "fence"); *Cf.* Joshua Kleinfeld, *The Legal Status of the Barrier Between Israel and the Occupied Territory: For International Law, Against the International Court* (on file with author) (discussing the prejudging nature of the title given to the construction).

109. *See* Kleinfeld, *supra* note 108 (The facts concerning the actual location of the wall at various periods is a matter of dispute).

110. *Id.* (analyzing the ICJ decision with some dissatisfaction for various reasons) ; *See also,*

appeared to be an attempt to illegally take Palestinian lands or at least prejudge any future negotiations on where the permanent boundary should be.[111]

In response to allegations of illegality, Israel argued that the fence was a self-defense measure under Article 51 of the UN Charter,[112] which states: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[113]

The Israeli permanent representative to the UN General Assembly, Ambassador Dan Gillerman, stated prior to the ICJ case:

> [A] security fence has proven itself to be one of the most effective non-violent methods for preventing terrorism in the heart of civilian areas. The fence is a measure wholly consistent with the right of States to self-defence enshrined in Article 51 of the Charter. International law and Security Council resolutions, including resolutions 1368 (2001) and 1373 (2001), have clearly recognized the right of States to use force in self-defence against terrorist attacks, and therefore surely recognize the right to use non-forcible measures to that end.[114]

It was Israel's contention that the fence was legal as a measure of self-defense and that it represented a humane and proportionate response to the terror attacks. The ICJ disagreed.

In response to Israel's Article 51 claim, the Court said:

> Article 51 of the Charter thus recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it are imputable to a

---

Alberto De Puy, *Bringing Down the Barrier: A Comparative Analysis of the ICJ Advisory Opinion and the High Court of Justice of Israel's Ruling on Israel's Construction of a Barrier in the Occupied Territories*, 13 TUL. J. INT'L & COMP. L. 275 (2005); Karin Calvo-Goller, *Jurisdiction and Justiciability: More Than a Huge Imbalance: The ICJ's Advisory Opinion on the Legal Consequences of the Construction of the Barrier*, 38 ISR. L. REV. 165 (2005); Rebecca Kahan, *Building a Protective Wall Around Terrorist—How the International Court of Justice's Ruling in the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Made the World Safer for Terrorists and More Dangerous for Member States of the United Nations*, 28 FORDHAM INT'L L.J. 827 (2005); Sean D. Murphy, *ICJ Advisory Opinion on Construction of a Wall in the Occupied Territories: Self-Defense and the Israeli Wall Advisory Opinion: An Ipse Dixit from the ICJ?*, 99 AM. J. INT'L. L. 62 (2005); Emanuel Gross, *Combating Terrorism: Does Self-Defense Include the Security Barrier? The Answer Depends on Who You Ask*, 38 CORNELL INT'L L.J. 569 (2005).

111. Advisory Opinion No. 131, *supra* note 15, at para. 121. *See also* U.N. GA Press Release GA/10179, *General Assembly, in Resumed Emergency Session, Demands Israel Stop Construction of Wall, Calls on Both Parties to Fulfill Road Map Obligations* (Oct. 21, 2003); De Puy, *supra* note 110, at 297-99.

112. *Id.* at para. 116, 138.

113. U.N. Charter art. 51.

114. Sean D. Murphy, *AGORA: ICJ Advisory opinion on Construction of a Wall in the Occupied Palestinian Territory: Self-Defense and the Israeli Wall Advisory Opinion: An Ipse Dixit From the ICJ?*, 99 AM. J. INT'L L. 62, 62 (2003) (quoting U.N. GAOR, Emergency Special Sess., 21st mtg. at 6, U.N. Doc. A/ES-10/PV.21 (Oct. 20, 2003)).

> foreign State.
>
> The Court also notes that Israel exercises control in the Occupied Palestinian Territory and that, as Israel itself states, the threat which it regards as justifying the construction of the wall originates within, and not outside, that territory. The situation is thus different from that contemplated by Security Council resolutions 1368(2001) and 1373(2001), and therefore Israel could not in any event invoke those resolutions in support of its claim to be exercising a right of self-defence.
>
> Consequently, the Court concludes that Article 51 of the Charter has no relevance in this case.[115]

The fact that Israel has been subject to serious terror attacks is not in dispute. However, the Court declined to recognize those attacks as justification for Israel's actions.[116] Rather, the Court held that the right to respond in self-defense only arises when state action is involved. This restrictive reading of self-defense has been met with significant disagreement,[117] including among several of the Court's own Judges.[118]

---

115. Advisory Opinion No. 131, supra note 15, at para. 139.

116. *See* Murphy, *supra* note 114, at 71-75.;

117. Murphy, *supra* note 114, at 62-63 (providing a detailed analysis of why the court erred in its analysis of article 51 by limiting armed attacks to states and stating eloquently:

> The position taken by the Court with respect to the *jus ad bellum* is startling in its brevity and, upon analysis, unsatisfactory. At best, the position represents imprecise drafting, and thus calls into question whether the advisory opinion process necessarily helps the Court "to develop its jurisprudence and to contribute to the progress of international law." At worst, the position conflicts with the language of the UN Charter, its *travaux preparatoires*, the practice of states and international organizations, and common sense. In addition to the lack of analytical reasoning, the Court's unwillingness to pursue an inquiry into the facts underlying Israel's legal position highlights a disquieting aspect of the Court's institutional capabilities: an apparent inability to grapple with complex fact patterns associated with armed conflict. Overall, the Court's style in addressing the *jus ad bellum* reflects an *ipse dixit* approach to judicial reasoning; the Court apparently expects others to accept an important interpretation of the law and facts simply because the Court says it is so).

118. *See* Advisory Opinion No. 131, supra note 15, at para. 33 (separate opinion of Judge Higgins) (Writing:

> I do not agree with all that the Court has to say on the question of the law of self-defence. In paragraph 139 the Court quotes Article 51 of the Charter and then continues "Article 51 of the Charter thus recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State." There is, with respect, nothing in the text of Article 51 that *thus* stipulates that self-defence is available only when an armed attack is made by a State. *That* qualification is rather a result of the Court so determining in *Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America) (Merits, Judgment, I.C.J. Reports 1986*, p. 14). It there held that military action by irregulars could constitute an armed attack if these were sent by or on behalf of the State and if the activity "because of its scale and effects, would have been classified as an armed attack . . . had it been carried out by regular armed forces" (*ibid.*, p. 103, para. 195). While accepting, as I must, that this is to be regarded as a statement of the law as it now stands, I maintain all the reservations as to this proposition that I have expressed elsewhere (R. Higgins, *Problems and Process: International Law and How We Use It*, pp. 250-251));

Advisory Opinion No. 131, supra note 15, at para. 6 (separate opinion of Judge Burgenthal) (writing "the United Nations Charter, in affirming the inherent right of self-defence, does not make its exercise dependent upon an armed attack by another State."); Advisory Opinion No. 131, supra note 15, at para.

After analyzing the Court's decision in the Wall Advisory Opinion, Professor Sean Murphy concludes:

> [T]he upshot of the Court's present jurisprudence appears to be that under the UN Charter, (1) a state may provide weapons, logistical support, and safe haven to a terrorist group; (2) that group may then inflict violence of any level of gravity on another state, even with weapons of mass destruction; (3) the second state has no right to respond in self-defense against the first state because the first state's provision of such assistance is not an "armed attack" within the meaning of Article 51; and (4) the second state has no right to respond in self-defense against the terrorist group because its conduct cannot be imputed to the first state, absent a showing that the first state "sent" the terrorist group on its mission. Such a legal construct, if intended, seems unlikely to endure.[119]

Professor Murphy's sobering assessment of the impact of the Court's decision is even more worrisome when its consequences to the principle of distinction are considered.

Imbedded in the Court's exposition of the right of self-defense is a crucial point concerning the principle of distinction and its continuing derogation. As mentioned above, the principle of distinction is designed to separate combatants from non-combatants in an effort to preserve the noncombatant population by disqualifying them as targets. In exchange for this willingness to be marked as a target (and meet the other qualifications of combatant status), combatants receive many benefits.[120] The greatest of these benefits is combatant immunity, which grants immunity for warlike acts, as long as fighters comply with the laws of war. Ideally, these incentives would be sufficient to entice those who want to engage in battlefield activities to legitimize themselves by meeting the requirements of GPW Article 4, including distinguishing themselves from the noncombatant populace. This can be done, in part, by becoming a member of a state's armed forces with its requirements of distinction, or otherwise clearly distinguishing oneself as part of an organized fighting group. Of course, the drawback to this commitment to distinction is that a fighter can no longer blend into the civilian noncombatant population and attack with some level of anonymity.

Even if the incentives were insufficient to entice individuals, the reciprocal benefits that would accrue to states from having all fighters clearly distinguished and subsequently eligible for combatant privileges should convince states to comply with the requirements of marking their forces. The argument is that as nations fight in compliance with the laws of war, honoring the principle of distinction not only benefits its uniformed armed forces by clearly identifying the

---

35 (separate opinion of Judge Kooijmans) (While not agreeing that Israel could invoke article 51 based on the fact that the terrorist activities come from within Israel, writes that Security Council Resolutions 1368 and 1373 provide a basis for Israel's argument).

119. Murphy, *supra* note 114, at 66.

120. *See generally* Geneva Convention Relative to the Treatment of Prisoners of War, *supra* note 7 (discussing the methods and means of warfare and the treatment of prisoners).

enemy, but also preserves its noncombatant civilian population. However, the ICJ's decision in the Wall Advisory Opinion has now tacitly removed that incentive both from states and from fighters who want to commit combatant acts from a position that gives them the cover of civilians.

The ICJ's decision gives states less incentive to use their armed forces when attacking another nation because unless the attacks can be attributed to a state, the target state does not attain the right to respond in self-defense. In other words, a state now has to balance the benefits it will gain from attacking with clearly marked armed forces against the benefits it will accrue if it opts to work clandestinely[121] through non-uniformed forces that it can support from a distance and still accomplish its goals but that it also knows will not give the target state the right to respond in self-defense. If a state thinks it can act through some armed rebel group and accomplish its aggressive purposes without having to fear military retribution, it will most certainly be more tempted to act. The inevitable result will be states making the decision to use armed rebels rather than uniformed state forces. This decision will undermine the principle of distinction by placing more fighters on the battlefield who may or may not decide to distinguish themselves from the local population.

While this unfortunate result of the Court's decision may not further affect the complex situation in Israel and Palestine,[122] the Court should be prescient enough to project the impact of its rulings on other evident scenarios. In the end, there has

---

121. Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, para 195 (June 27) (Holding:

> There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry our acts of armed force against another State of such gravity as to amount to" (*inter alia*) an actual armed attack conducted by regular forces, "or its substantial involvement therein". This description contained in Article 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular forces. But the Court does not believe that the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support.).

See Michael N. Schmitt, *The Rule of Law in Conflict and Post-Conflict Situations: U.S. Security Strategies: A Legal Assessment*, 27 HARV. J.L. & PUB. POL'Y 737, 751 (2004) (discussing the meaning of the Nicaragua case: "only attacks of a particular scale and of certain effects are 'armed attacks' justifying a military response in self-defense."). *But see* Advisory Opinion No. 131, supra note 15, at note 15 (making no mention of the scale of the attacks as a criterion for invoking self defense).

122. *See Lebanese talk show discusses UN team investigating Al-Hariri death*, BBC WORLDWIDE MONITORING, Sep. 10, 2005; *Italy, United States Reaffirm Solidarity Against Terror*, STATE NEWS SERVICE, July 13, 2005 (Israel faces both uniformed and non-uniformed armed groups that act along a spectrum of almost full state sponsorship to only limited financial or ideological backing. It is unclear that this situation will change drastically as a result of the ICJ's ruling).

been little direct impact on the situation in Israel as a result of the ICJ ruling,[123] but the effects of the Court's narrow construction of armed attack have already eroded the principle of distinction. This is exactly the opposite direction international law should be moving.[124]

Despite Professor Murphy's caution to the Court,[125] it has taken one more step down the path of undermining the principle of distinction, the step from tacitly approving to explicitly encouraging states to use armed militant groups who shun the rules of distinction and purposefully practice illegal battlefield tactics. This step occurred in the Case Concerning Armed Activities on the Territory of the Congo,[126] otherwise known as Congo v. Uganda.

B. Congo v. Uganda

The Case Concerning Armed Activities on the Territory of the Congo[127] arose from incidents that occurred between Uganda and the Democratic Republic of the Congo (DRC) from the late 1990s through 2004. In its application, the DRC alleged:

> acts of *armed aggression* perpetrated by Uganda on the territory of the Democratic Republic of the Congo, in flagrant violation of the United Nations Charter and of the Charter of the Organization of African Unity. ... Such armed aggression by Ugandan troops on Congolese territory has involved *inter alia* violation of the sovereignty and territorial integrity of the Democratic Republic of the Congo, violations of international humanitarian law and massive human rights violations.[128]

In the counterclaims and defenses, Uganda alleged, among other things, that it was acting in self-defense in compliance with Article 51 of the UN Charter.

---

123. Press Release, General Assembly Emergency Session Overwhelmingly Demands Israel's Compliance with International Court of Justice Advisory Opinion, U.N. DOC. GA/10248 (July 20, 2004). *See* Fr. Robert L. Araujo, S.J., *Implementation of the ICJ Advisory Opinion – Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory: Fences [do not] Make Good Neighbors?*, 22 B.U. INT'L L.J. 349, 387-96 (2004) (explaining the discussions concerning the General Assembly resolution, issued as a result of the Advisory Opinion, which was approved by a vote of 150 for, 6 against, and 10 abstaining).

124. Jensen, *supra* note 12, at 226.

125. Murphy, *supra* note 114, at 76 (writing:

> The Court would do well to heed these concerns. Its docket currently includes cases relevant to the *jus ad bellum*, such as those brought by the Democratic Republic of the Congo against Rwanda and Uganda. They are opportunities for the Court not only to decide concrete cases, but to help clarify in a cogent and thoughtful way the status of international law in its most critical area. States are willing to yield power to an international court of fifteen individuals only when they believe that the court's findings reflect higher levels of deliberation than are found within any one state's machinery. Findings that lack deep levels of reasoning, that fail to take account of and rebut divergent lines of thinking, are not salutary for any court, let alone one that holds itself up as the "supreme arbiter of international legality.").

126. Dem. Rep. Congo v. Uganda, *supra* note 16.

127. *Id.*

128. Application Instituting Proceedings, Armed Activities on the Territory of the Congo (Dem. Rep. Congo *v.* Uganda) (filed in the Registry of the Court June 23, 1999), *available at* http://www.icj-cij.org/icjwww/idocket/ico/icoapplication/ico_iapplication_19990623.pdf.

Uganda claimed that their forces were initially in the DRC at the invitation of then-president Joseph Kabila in order to control "anti government rebels who were active along the Congo-Uganda border, carrying out in particular cross-border attacks against Uganda."[129]

Although President Kabila subsequently removed this consent,[130] Uganda claimed that the cross-border attacks by armed rebels continued and that Uganda was required to take armed actions in self defense into the DRC to prevent these armed attacks.[131] Uganda further claimed that this intervention was warranted as the rebels "fled back to the DRC,"[132] and that the DRC was unable to stop the attacks.[133] The situation left Uganda with no other option than to suffer the attacks or to act in self-defense. A document produced by the Ugandan High Command lists the five stated reasons justifying its actions in self-defense:

> 1. To deny the Sudan opportunity to use the territory of the DRC to destabilize Uganda.
>
> 2. To enable UPDF neutralize Uganda dissident groups which have been receiving assistance from the Government of the DRC and the Sudan.
>
> 3. To ensure that the political and administrative vacuum, and instability caused by the fighting between the rebels and the Congolese Army and its allies do not adversely affect the security of Uganda.
>
> 4. To prevent the genocidal elements, namely, the Interahamwe, and ex-FAR, which have been launching attacks on the people of Uganda from the DRC, from continuing to do so.
>
> 5. To be in position to safeguard the territory integrity of Uganda against irresponsible threats of invasion from certain forces."[134]

Given the purposes of this paper, only the fourth reason need be considered here.[135]

---

129. Dem. Rep. of Congo v. Uganda, *supra* note 16, para. 45.

130. *Id.* at para. 53.

131. *Id.* at para. 92.

132. *Id.* at para. 109.

133. *See* Michael N. Schmitt, *The Rule of Law in Conflict and Post-Conflict Situations: U.S. Security Strategies: A Legal Assessment*, 27 HARV. J.L. & PUB. POL'Y 737, 760 (2004) (arguing that where a state is unable or unwilling to prevent attacks from its territory, the attacked state "may non-consensually cross the border for the sole purpose of conducting counterterrorist operations, withdrawing as soon as it eradicates the terrorist threat.").

134. Dem. Rep. Congo v. Uganda, *supra* note 16, para. 109.

135. *See* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 217-221 (2002) (Paragraph 2 appears to give rise to a claim of anticipatory self-defense under customary international law). *But see* Dem. Rep. Congo v. Uganda, *supra* note 16, para. 143 (Uganda never made the claim of anticipatory defense. In any case, such a claim may not have mattered as the ICJ, in a broad statement, proclaimed, "The Court first observes that the objectives of Operation 'Safe Haven', as stated in the Ugandan High Command document, were not consonant with the concept of self-defence as understood in international law.").

The fourth reason alleges actual attacks across the border by armed insurgents that resulted in death or injury to Ugandans.[136] The importance of this allegation is that it raised an issue for the ICJ's consideration that they did not face previously, at least according to Judge Kooijman's separate opinion, in the Wall Advisory Opinion.[137] If Judge Kooijmans was right, the ICJ's decision in the Wall Advisory Opinion can be read as claiming that these attacks were not armed attacks because they were internal to Israel, coming from within its controlled territory. Therefore, they did not justify a response in self-defense under Article 51 of the UN Charter. No such claim of internal attacks is made here. Rather, the fourth justification in the High Command document alleges attacks by armed rebels that originated from the DRC.

Uganda argued that during the period of 1998 to 2003, "the changed policies of President Kabila had meant that co-operation in controlling insurgency in the border areas had been replaced by 'stepped-up crossed-border attacks against Uganda by the ADF which was being re-supplied and re-equipped by the Sudan and the DRC government.'"[138] The DRC admitted that these attacks had taken place but claimed that the ADF alone was responsible. The Court also acknowledged that the attacks took place and took notice of an independent report that "seem[s] to suggest some Sudanese support for the ADF's activities. It also implies that this was not a matter of Congolese policy, but rather a reflection of its inability to control events along its border... However, the Court does not find this evidence weighty and convincing."[139]

Though not explicitly stated, it appears the Court is not swayed by this information because it is only looking for evidence of armed attacks tied to a nation state. In concluding the section of the opinion concerned with the use of force, the Court states:

> It is further to be noted that, while Uganda claimed to have acted in self-defence, it did not ever claim that it had been subjected to an armed attack by the armed forces of the DRC. The "armed attacks" to which reference was made came rather from the ADF. The Court has found above (paragraphs 131-135) that there is no satisfactory proof of the involvement in these attacks, direct or indirect, of the Government of the DRC. The attacks did not emanate

136. Dem. Rep. Congo v. Uganda, *supra* note 16, para. 143.

137. Advisory Opinion No. 131, supra note 15, para. 36 (separate opinion of Judge Kooijmans) (stating:

> The argument which in my view is decisive for the dismissal of Israel's claim that it is merely exercising its right of self defence can be found in the second part of paragraph 139. The right of self defence as contained in the Charter is a rule of international law and thus relates to international phenomena. Resolutions 1368 and 1373 refer to acts of international terrorism as constituting a threat to international peace and security; they therefore have no immediate bearing on terrorist acts originating within a territory which is under control of the State which is also the victim of these acts. And Israel does not claim that these acts have their origin elsewhere. The Court therefore rightly concludes that the situation is different from that contemplated by resolutions 1368 and 1373 and that consequently Article 51 of the Charter cannot be invoked by Israel).

138. Dem. Rep. Congo v. Uganda, *supra* note 16, para. 120.

139. *Id.* at para. 51.

> from armed bands or irregulars sent by the DRC or on behalf of the DRC, within the sense of Article 3 *(g)* of General Assembly resolution 3314 (XXIX) on the definition of aggression, adopted on 14 December 1974. The Court is of the view that, on the evidence before it, even if this series of deplorable attacks could be regarded as cumulative in character, they still remained non-attributable to the DRC.
>
> For all these reasons, the Court finds that the legal and factual circumstances for the exercise of a right of self-defence by Uganda against the DRC were not present. Accordingly, the Court has no need to respond to the contentions of the Parties as to whether and under what conditions contemporary international law provides for a right of self-defence against large-scale attacks by irregular forces. Equally, since the preconditions for the exercise of self-defence do not exist in the circumstances of the present case, the Court has no need to enquire whether such an entitlement to self-defence was in fact exercised in circumstances of necessity and in a manner that was proportionate.[140]

By determining that attacks occurred by armed rebels across the border from the DRC into Uganda, and then finding that because there was no "satisfactory proof of the involvement" of the DRC or any other "state," no right to self-defense accrued to Uganda, the Court has taken the bad ruling in the Wall Advisory Opinion and advanced it one step further. By refusing "to respond to the contentions of the Parties as to whether and under what conditions contemporary international law provides for a right of self-defense against large-scale attacks by irregular forces," the Court has ignored the reality of the situation. Further, the Court not only passed up a chance to right a ship that was heading the wrong direction, but has instead added hurricane-force winds to the sails, as recognized by ICJ Judges Kooijmans and Simma.[141]

---

140. *Id.* at para. 53.

141. Dem. Rep. Congo v. Uganda, *supra* note 16, para. 27 (separate opinion of Judge Kooijmans) (stating:

> The Court seems to take the view that Uganda would have only been entitled to self-defence *against the DRC* since the right of self-defence is conditional on an attack being attributable, either directly or indirectly, *to a State* . . . But, as I already pointed out in my separate opinion to the 2004 Advisory Opinion on *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Article 51 merely "conditions the exercise of the inherent right of self-defence on a previous armed attack without saying that this armed attack must come from another State even if this has been the generally accepted interpretation for more than 50 years". I also observed that this interpretation no longer seems to be shared by the Security Council, since in resolutions 1368 (2001) and 1373 (2001) it recognizes the inherent right of individual or collective self-defence without making any reference to an armed attack by a State).

Judge Kooijmans proposes an alternative based on his belief of current international law and grounded in the realities of the current world. He writes:

> If the attacks by the irregulars would, because of their scale and effects, have had to be classified as an armed attack had they been carried out by regular armed forces, there is nothing in the language of Article 51 of the Charter that prevents the victim State from exercising its *inherent* right of self-defence If armed attacks are carried out by irregular bands from such territory against a neighbouring State, they are still armed attacks even if they cannot be attributed to the territorial State. It would be unreasonable to deny the attacked State the right to self-defence merely because there is

This holding has the effect of encouraging every government that has aggressive designs on its neighbor to covertly create, train, and supply non-uniformed, armed rebels within its territory because even if the support meets the "direct or indirect involvement" standard first articulated in Nicaragua.[142] The current Court's unwillingness to address the quantum of attack necessary to trigger the right to self-defense is a step backward from the standard of "acts of armed force against another State of such gravity as to amount to (*inter alia*) an actual armed attack"[143] pronounced in Nicaragua. In other words, by making discernable "direct or indirect" involvement by a state a necessary "precondition" to the use of force in self-defense, the Court has given aggressive states a clear incentive to support, even encourage, attacks by armed rebel groups because they will not invoke the targeted state's right to respond in self-defense against either the rebels or the supporting state.

As a continuation of the Wall Advisory Opinion, this decision has devastating effects on the principle of distinction. By prohibiting a response in self-defense to external armed rebel attacks, regardless of the quantum, the Court encourages rogue states to carry out their illegal aggressive designs through un-uniformed, armed rebels who are virtually indistinguishable from the local population save for actually shooting their weapons in the attack. Because of the Court's regrettable decision, these rogue actors now see a way to orchestrate large scale armed violence without creating a right of self-defense for their victims and simultaneously increasing the survivability of their attackers by clothing them in the protections of civilians. This is truly a catastrophic development given modern battlefield tendencies.

As recognized by the Security Council in their resolutions 1368 and 1373,[144] the world is not the same place it was prior to September 11, 2001. Since those attacks, the major threats to international peace and security have not centered in only state actors, but also in non-state actors, many of whom have an international reach.[145] The standard for the exercise of self-defense by a state ought to be

---

no attacker State, and the Charter does not so require).

See also Dem. Rep. Congo v. Uganda, *supra* note 16, para. 13 (separate opinion of Judge Simma) (concurring with Judge Kooijmans' understanding of current international law and writing:

> I also subscribe to Judge Kooijmans' opinion that the lawfulness of the conduct of the attacked State in the face of such an armed attack by a non-State group must be put to the same test as that applied in the case of a claim of self-defence against a State, namely, does the scale of the armed action by the irregulars amount to an armed attack and, if so, is the defensive action by the attacked State in conformity with the requirements of necessity and proportionality?).

142. *See* Murphy, *supra* note 114, at 65-66.

143. Nicar. v. U.S., *supra* note 121, para. 103-104; Dem. Rep. Congo v. Uganda, *supra* note 16 (separate opinion of Judge Simma).

144. S.C. Res. 1368, U.N. SCOR, 4370th mtg., U.N. Doc. S/Res/1368 (Sept. 12, 2001); S.C. Res. 1373, U.N. SCOR, 4385th mtg., U.N. Doc. S/Res/1373 (Sept. 28, 2001). *See also* Vincent-Joel Proulx, *Babysitting Terrorists: Should States be Strictly Liable for Failing to Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L L. 615, 627 (2005) (arguing that the international community is moving to a system where states are held indirectly liable for the actions of entities within their borders).

145. WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 8-13 (September, 2002), *available at http://www.whitehouse.gov/nsc/nss/2006.*

"armed attack," from whatever source it springs. Only under this standard can states adequately protect themselves against modern threats.[146]

More importantly for this paper, utilizing this standard of armed attack, regardless of whether it is state sponsored or not, will also reverse the continuing trend of incentivizing states to "use" forces other than their nation's uniformed forces who do not feel compelled to distinguish themselves from the local populace in order to avoid giving rise to the right of self-defense. This trend began two decades ago with the Nicaragua decision,[147] but the ICJ has taken a definite turn in the wrong direction with their decision in the Wall Advisory Opinion and digressed even further with the recent Congo v. Uganda case. It is not coincidental that during this same time period since Nicaragua, there has been a rise in the use of law of war provisions as a tool against legally compliant nations in battle. This type of warfare is known as lawfare.[148]

IV. THE EROSION OF THE PRINCIPLE OF DISTINCTION AND THE RISE OF LAWFARE

Modern warfare is no longer typified by the arrangement of major armies along a two dimensional battle line.[149] In fact, modern warfare has even moved beyond the concept of three-dimensional "air land battle"[150] to the 360-degree concept of the common operational environment[151] where attacks can come from any direction and from any source. This new battlespace concept is intricately entwined with the concept of asymmetrical warfare.

Asymmetrical warfare describes the modern reality that wars are not being fought between equal or nearly equal armies on a defined battlefield. As now Major General (MG) Charles Dunlap, Jr.[152] writes, "In broad terms, 'asymmetrical' warfare describes strategies that seek to avoid an opponent's

---

146. *See* Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICH J. INT'L L. 513, 540-44 (2003) (arguing this point specifically in connection with defending against cross border attacks from non-state actors that amount to armed attack).

147. Dem. Rep. Congo v. Uganda, *supra* note 16, para. 21 (separate opinion Judge Kooijmans).

148. *See Lawfare, The Latest in Asymmetries*, Council on Foreign Relations, Mar. 18, 2003, *http://www.cfr.org/publication.html?id=5772* (defining lawfare as "a strategy of using or misusing law as a substitute for traditional military means to achieve military objectives.").

149. *See* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 730 (2004) ("[E]ven the battles of the nineteenth century rarely fit this paradigm, and modern conflict fits this paradigm still less well."); Gabriel Swiney, *Saving Lives: The Principle of Distinction and the Realities of Modern War*, 39 INT'L LAW. 733, 743 (2005) ("Wars between powerful states, those conflicts that prompted the development of humanitarian law, are increasingly rare. Instead of large-scale combat between organized militaries, modern warfare is becoming asymmetrical. Insurgencies, not armies, are the norm.").

150. *See* John J. Romjue, *The Evolution of the AirLand Battle Concept*, AIR U. REV. (1984), *available at* http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/may-jun/romjue.html.

151. *See The Contemporary Operational Environment (COE)*, OPERATION ENDURING FREEDOM TACTICS, TECHNIQUES AND PROCEDURES HANDBOOK NO. 02-8, STRATEGYPAGE.COM, *available at http://www.strategypage.com/articles/operationenduringfreedom/chap1.asp* (last visited Apr. 2, 2006).

152. *See* Official Website of the United States Air Force, *http://www.af.mil/bios/bio.asp?bioID=5293*
(Showing that at the time of this writing, MG Charles Dunlap, Jr. had recently been promoted to the rank of Major General and assigned as Deputy Judge Advocate General of the Air Force).

strengths; it is an approach that focuses whatever may be one sides comparative advantages against their enemy's relative weaknesses."[153] In this type of conflict, the disadvantaged party is unlikely to succeed by squaring off with its opponent in a typical force on force military struggle. Instead, the disadvantaged party must seek to use the comparatively low-tech tools at its disposal to gain the comparative advantage.[154] One of the most tempting and potentially successful low-tech tools in this fight is international law, particularly the principle of distinction.[155]

The use of law as a tool of warfare is not inherently good or bad. The laws of war have generally had a mitigating effect on warfare. But, like any tool of warfare, "it is how the law is used that defines its nature and value."[156] As David Rivken and Lee Casey argue, "international law may become one of the most potent weapons ever deployed."[157] In this form of warfare, a group or state that is facing a nation committed to comply with the laws of war will choose to openly violate the law not only for the tactical advantage gained but for the strategic benefit that arises.[158] The compliant nation, still committed to law of war compliance, is thus disadvantaged.

This form of asymmetrical warfare has come to be known as "lawfare," or "the use of law as a weapon of war."[159] It takes many forms but is always pointed at striking where a more superior but legally bound military force is more constrained than a less superior but legally unconstrained force.[160] The recent war in Iraq illustrates many examples of this,[161] including attacking from protected

153. Charles J. Dunlap, Jr., *A Virtuous Warrior in a Savage World*, 8 USAFA J. Leg. Stud. 71, 72 (1997/1998). *See also* W. Chadwick Austin and Antony Barone Kolenc, *Who's Afraid of the Big Bad Wolf? The International Criminal Court as a Weapon of Asymmetric Warfare*, 39 VAND. J. TRANSNAT'L L. 291, 293-94, 301-02 (2006).

154. Michael N. Schmitt, *The Impact of High and Low-Tech Warfare on the Principle of Distinction*, 1, 2, 12-13, Harvard Program on Humanitarian Policy and Conflict Research, International Humanitarian Law Research Initiative Briefing Paper (2003), *reprinted in* INTERNATIONAL HUMANITARIAN LAW AND THE 21ST CENTURY'S CONFLICTS: CHANGES AND CHALLENGES (Lausanne: Editions Interuniversitaires Suisses, Roberta Arnold & Pierre-Antoine Hildbrand eds., 2005), *available at* http://www.michaelschmitt.org/Publications.html.

155. *See* Michael N. Schmitt, *The Principle of Discrimination in the 21st Century*, 2 YALE HUM. RTS. & DEV. L.J. 143, 157 (1999) (discussing the effects of technology on the principle of distinction and arguing that as the gap widens between the "haves and have-nots," the asymmetrical disadvantage of the have-nots will tempt them to abandon the principle of distinction).

156. Colonel Kelly D. Wheaton, *Strategic Lawyering: Realizing the Potential of Military Lawyers at the Strategic Level*, 2006 ARMY LAW. 1, 7 (2006).

157. Colonel Charles J. Dunlap, Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts* 4, 5 (2001), *available at* http://www.ksg.harvard.edu/cchrp/Web%20Working%20Papers/Use%20of%20Force/Dunlap2001.pdf (last visited June 28, 2004).

158. *See* Reynolds, *supra* note 2, at 102-03 (stating, "[P]ublic support can be lost based on the number of civilian casualties. A March, 2003 Gallup poll indicates 57 percent of those surveyed would oppose a war in Iraq because 'many innocent Iraqi citizens would die.'").

159. *See* Dunlap, Jr., *supra* note 157; Schmitt *supra* note 154, at 17. *See also* Austin & Kolenc, *supra* note 153, at 306-310.

160. *See* William Bradford, *Barbarians at the Gates: A Post-September 11th Proposal to Rationalize the Laws of War*, 73 MISS. L. J. 639, 673-74 (2004).

161. *See Announcing the Inaugural Combined Arms Center Commanding General's 2006 Special*

places and using protected places or objects as weapons storage sites,[162] fighting without wearing a proper uniform,[163] using human shields to protect military targets,[164] using protected symbols to gain military advantage,[165] and murdering of prisoners or others who deserve protection.[166] In each of these cases, an inferior force used the superior force's commitment to adhere to the law of war to its tactical advantage.

Unfortunately, the most typical and also most damaging form of lawfare in recent conflicts has been the decision of disadvantaged combatants to not distinguish themselves from the local populace.[167] And it appears that this trend is on the rise, even amongst major military powers.[168] As MG Dunlap has written, "If international law is to remain a viable force for good in military interventions, lawfare practitioners cannot be permitted to commandeer it for malevolent purposes."[169] Regrettably, the aforementioned ICJ decisions have made it much easier for practitioners of lawfare to use the law of war against compliant nations. Rebecca Kahan highlights this point: "For years, the international community has embraced the idea that targeting civilians violates principles of international

---

Topics Writing Competition: "Countering Insurgency," HEADQUARTERS GAZETTE (Society for Military History, Leavenworth, KS), Winter 2006, at 12, *available at http://leavenworth-net.com/lchs/12658%Headquarters.pdf* (highlighting the U.S. Army's recognition of the seriousness of the use of lawfare in Iraq. In a recent announcement from the Combined Arms Center at Ft. Leavenworth, Kansas, the Military Review is sponsoring a writing competition seeking articles specifically on issues dealing with counter insurgency, including "lawfare." The announcement begins by stating that "The Army absolutely needs to understand more about counterinsurgency—nothing less than the future of the civilized world may depend on it.").

162. *See* Tony Perry & Rick Loomis, *Mosque Targeted in Fallouja Fighting*, L.A. TIMES, April 27, 2004, at A1.

163. *See Coalition Forces Continue Advance Toward Baghdad*, CNN LIVE EVENT/SPECIAL, March 24, 2003.

164. *See The Rules of War are Foreign to Saddam*, OTTAWA CITIZEN, March 25, 2003; David Blair, *Human Shields Disillusioned with Saddam, Leave Iraq after Dubious Postings*, NATIONAL POST (CANADA), March 4, 2003, *available at* http://www.FPinfomart.ca.

165. Rivkin & Casey, *supra* note 27, at 65.

166. *See* Robert H. Reid, *South Korean Hostage Beheaded in Iraq*, TORONTO STAR, June 23, 2004, at A1, *available at* WL 6081419; *See also* Michael Sirak, *Legal Armed Conflict*, JANE'S DEFENSE WEEKLY, Jan. 14, 2004, at 27 (listing a number of violations of the law of war committed by Iraqi military and paramilitary forces).

167. *See* Gabriel Swiney, *Saving Lives: The Principle of Distinction and the Realities of Modern War*, 39 INT'L LAW. 733, 735 (2005) (stating, "[t]he Principle of Distinction is violated across the world, often openly so, and that problem is getting worse." The author then argues for replacing the principle of distinction with the Principle of Culpability which is based on each individual's actions rather than his status as a noncombatant).

168. *See* Col Wang Xiangsui, Chinese Air Force, *as quoted by* John Pomfret in *China Ponders New Rules of 'Unrestricted Warfare,'* WASH. POST, Aug. 9, 1999, at 1, *quoted in* Dunlap, *supra* note 158, at 36 (where a senior member of the Chinese Air Force recently stated "War has rules, but those rules are set by the West . . . if you use those rules, then weak countries have no chance . . .We are a weak country, so do we need to fight according to your rules? No.").

169. Dunlap, *supra* note 157, at 36; *See also* Colonel Kelly D. Wheaton, *Strategic Lawyering: Realizing the Potential of Military Lawyers at the Strategic Level*, 2006 ARMY LAW. 1, 16 (2006) (arguing that strategic lawyering can be a force to fight the effects of lawfare).

law."[170] She then contrasts the actions of those who practice lawfare; "terrorist organizations have adopted this strategy [of violating international law] as part of their policy."[171] The fact that terrorists and others find sympathy for the use of their tactics from the ICJ and others only emboldens them. It also emboldens state leaders who cannot otherwise use the military instrument in their aggressive designs for fear of military retribution.

As a result of the Wall and Uganda decisions by the ICJ, state leaders have incentive to "use" other armed groups to accomplish their military attacks on neighbors rather than their official uniformed armed forces because the latter would trigger the target nation's right of self-defense. On the other hand, if they maintain their support to armed groups below a standard that the ICJ will attribute to the state, the state can effectively work toward the destabilization of a neighboring country without fear of a legal response in self-defense. If an illegal response does come, the nation cannot only respond in self-defense, though the original aggressor, but also claim to be the legally compliant state. The clear result of this is more fighters on the battlefields of the world who are not distinguished or distinguishable from the local populace. This can only result in more civilian casualties and greater derogation from the laws of war.

V. THE NEED FOR A RETAINING WALL TO STOP THE EROSION

The erosion of the principle of distinction poses a danger too great for the international community to sit idly. Steps must be taken to incentivize all battlefield fighters to comply with the laws of war, particularly with those rules that distinguish them from the local populace. Some such incentives have already been proposed.[172] However, incentives on an individual basis need to be augmented by institutional incentives that remove the incentives of states to derogate from this fundamental rule.

The first remedial action that must be taken is for the ICJ to reverse its misapplication of the concept of armed attack. Regardless of whether customary international law ever recognized armed attack as restricted only to states, it does not and should not now.[173] As clearly implied by the UN Security Council in resolutions 1368 and 1373[174] and confirmed by Judges Kooijmans and Simma in their separate opinions,[175] armed attacks invoke a state's right of self defense

170. Kahan, *supra* note 110, at 827-28.

171. *Id.*

172. *See generally* Jensen, *supra* note 12 (proposing five incentives to encourage combatants to distinguish themselves from civilians).

173. *See* Schmitt, *supra* note 146, at 536-540.

174. *See* Kathleen Renee Cronin-Furman, *The International Court of Justice and the United Nations Security Council: Rethinking a Complicated Relationship*, 106 COLUM. L. REV. 435, 463 (2006) (arguing that the conflict between the ICJ and Security Council is not new and that "[t]he ICJ's failure to conform its reasoning to international political realities, as evinced in the Wall Opinion, seriously threatens the ICJ's credibility." The author proposes, "According the Security Council's pronouncements primacy in the consideration of customary law would be an effective way to resolve this issue. It would preserve the ICJ's judicial discretion while at the same time recognizing the Security Council's paramount importance to the maintenance of international peace and security.").

175. *See* Dem. Rep. Congo v. Uganda, *supra* note 16 (separate opinions of Judge Simma and Judge

whether they are generated by a state or not. Armed attack should be understood as a quantum requirement, not a source requirement.[176] Any other reading would incentivize the use of irregulars to do what regular forces could not, striking at the heart of the fundamental principle of distinction in international law and significantly degrade fundamental protections currently afforded to civilians.

Secondly, the Security Council must issue a more explicit and definitive statement on the quantum nature of armed attack. As the Security Council is increasingly confronted with threats to international peace and security by the onslaught of terrorism and similar multinational non-state actors, it is in the Security Council's interest, and the interest of all United Nations' member states, to have a definitive statement on this issue. As such, the Security Council should recognize a state's inherent right to defend itself against attack so long as the response is proportional and necessary. The Security Council could easily reconfirm these bedrock principles and apply them in the light of the current international system.

Finally, organizations such as the ICRC that identify protection of noncombatants and civilians as part of their charter[177] ought to encourage the enactment of laws that will advance this vital interest. As Professor Reisman has pointed out,[178] those who have advocated for GPI should now reflect on its results. In an effort to give protections to certain battlefield actors, they have dramatically degraded the principle of distinction. A better approach is to insure that noncombatants and civilians are protected, even if it means that some battlefield actors who choose to participate without meeting the requirements of GPW Article 4, are not given combatant privileges. It is not an overly arduous requirement that all battlefield actors distinguish themselves to be viewable at a distance in some way. This does not even require a uniform, merely a distinguishing marking that sets battlefield fighters apart from civilians.[179] The ICRC should take the lead on revisiting this issue amongst NGOs and work toward reestablishing the safety wall around civilians as opposed to eroding those protections.

While these three recommendations will certainly not prevent any future civilian casualties, they would help establish a clear legal standard for state actions that would remove the existing incentives to "use" armed groups to avoid giving

---

Kooijmans).

176. *See* Schmitt, *supra* note 121, at 750-52 (discussing the effects basis for understanding the right of self-defense in the ICJ's decision in Nicaragua).

177. See the ICRC Mission Statement, *available at* http://www.icrc.org/HOME.NSF/060a34982cae624ec12566fe00326312/125ffe2d4c7f68acc1256ae300394f6e?OpenDocument, which states:

> The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of war and internal violence and to provide them with assistance. It directs and coordinates the international relief activities conducted by the Movement in situations of conflict. It also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles.

178. Reisman, *supra* note 17, at 856.

179. Ferrell, *supra* note 13, at 106-09.

rise to the right of self-defense. Such a move would enhance the principle of distinction and reinvigorate the protections provided to civilians on the battlefield.

VI. CONCLUSION

The recent erosion of the principle of distinction has certainly been one of the factors leading to an increasing number of noncombatant deaths on modern battlefields. The international law principle that makes this conduct illegal is firmly rooted in the law of war but has been weakened by provisions of GPI that are designed to provide greater protections to battlefield fighters. As history has borne out, trying to widen the group who gain combatant protections has inevitably weakened the protections provided for noncombatants and civilians and brought more innocent bystanders within the hostile fire of warring parties.

The recent decisions of the ICJ have taken this derogatory step even further. In the Wall Advisory Opinion, the ICJ held that "numerous indiscriminate and deadly acts of violence against its civilian population"[180] by a non-state actor from within its own territory did not give Israel the right to respond in self-defense, even if that response was non-lethal. The ICJ went a step further in the Congo v. Uganda ruling when it immunized any action from raising the right of self-defense, regardless of the scale, as long as it was committed by a non-state entity or group. This holding gives tremendous incentive to states that are aggressive toward their neighbors to support and even assist armed groups who are carrying out significant attacks, attacks which would give rise to the right of self-defense if done by government armed forces.

These decisions, taken despite prior UN Security Council resolutions proclaiming otherwise, dramatically erode the principle of distinction. They not only remove the incentive to comply with the law of war, but they actually give a disincentive to do so because it gives the target state a legal right to respond with proportional armed force. The result will be fewer and fewer marked combatants on modern battlefields and greater and greater civilian casualties who get inadvertently mixed in with those who are engaging in hostilities by relying on the protections of the noncombatant identity to pursue their militant goals.

These unfortunate erosions of the law of war aggravate the asymmetrical warfare approach of lawfare, or using the law of war as a weapon against a compliant enemy. Lawfare is a growing methodology to warfare, contemplated not only by small nations and groups, but also by large armies. Sadly, the ICJ's decisions add a false legal gloss to these actions. If this trend is allowed to continue, the principle of distinction will soon dwindle into a meaningless rule.

The Security Council must take the lead on more clearly and explicitly stating the quantum nature of armed conflict rather than reliance on the source of the action for qualification. The ICJ must follow the Security Council's lead and reverse the direction in which the Court is heading by redefining armed attack to be an effects-based test, rather than a claim that can only be invoked if the attacker is a state actor. Finally, the ICRC must take the lead in reevaluating its advocacy

180. Advisory Opinion No. 131, *supra* note 15, at para. 141.

of a principle that supplies greater protections to all battlefield fighters but has the practical effect of endangering civilians. The principle of distinction must remain the foundational principle of the law of war. The Israeli Wall must be torn down and the entry point for lawfare blocked. In its place, a bridge should be built, allowing civilians to cross back into a realm where they are protected and their safety is legally enshrined.

3

LEVERAGING EMERGING TECHNOLOGY FOR LOAC COMPLIANCE

By Eric Talbot Jensen[1] and Alan Hickey[2]

I. INTRODUCTION

The International Committee of the Red Cross (ICRC), in conjunction with the government of Switzerland, has recently introduced an initiative on strengthening compliance with the law of armed conflict (LOAC).[3] According to the ICRC, the lack of compliance with the LOAC is "probably the greatest current challenge to . . ."[4] and the "principal cause of suffering during armed conflict."[5] A major effort of the initiative is to create a forum for exchanges between States on compliance issues,[6] hoping that open discussion will lead "to enhancing and ensuring the

---

[1] Professor, Brigham Young University Law School.

[2] JD, Brigham Young University Law School

[3] *See generally* Jelena Pejic. *Strengthening Compliance with IHL: The ICRC-Swiss Initiative*. 98 INT'L REV. OF THE RED CROSS 315, 315–30 (2016).

[4] *Id.* at 316.

[5] *Status of additional protocols relating to the protection of victims of armed conflicts: ICRC statement to the United Nations, 2016*, ICRC.ORG, https://www.icrc.org/en/document/status-additional-protocols-relating-protection-victims-armed-conflicts-icrc-statement-0 (last visited May 1, 2018).

[6] Peter Maurer, Pres. of the ICRC, Establishing a Dedicated IHL Compliance System, Opening

effectiveness of mechanisms of compliance with IHL."[7]

Resolution 2 of the 32nd International Conference of the Red Cross and Red Crescent called for called for

> the continuation of an inclusive, State-driven intergovernmental process based on the principle of consensus after the 32nd International Conference and in line with the guiding principles enumerated in operative paragraph 1 to find agreement on features and functions of a potential forum of States and to find ways to enhance the implementation of IHL using the potential of the International Conference and IHL regional forums in order to submit the outcome of this intergovernmental process to the 33rd International Conference."[8]

Speech at the Third Meeting of States on Strengthening Compliance with International Humanitarian Law (June 30–July 1, 2014), https://www.icrc.org/eng/resources/documents/statement/2014/06-30-compliance-ihl-maurer.htm; Emanuela-Chiara Gillard, *Promoting Compliance with International Humanitarian Law*, CHATHAM HOUSE 2, 1–8 (2016), https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-10-05-promoting-compliance-ihl-gillard.pdf.

[7] Claudia McGoldrick, *The future of humanitarian action: an ICRC perspective*, 93 INT'L REV. OF THE RED CROSS 965, 985 (2011).

[8] 32nd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT, Geneva, Switzerland 8-10 December 2015. Strengthening compliance with international humanitarian law: Resolution 2, http://rcrcconference.org/wp-content/uploads/2015/04/32IC-

Efforts in this area continue in preparation for the 33rd International Conference.

Concurrent with the recognition of the need for greater compliance with the LOAC is a vibrant discussion on the role of emerging technologies in modern warfare.[9] While many have raised a cautionary voice about the ability of the LOAC to constrain advanced weapons systems,[10] there is a clear recognition that all emerging technologies that are weaponized must comply with the LOAC.[11]

This focus on constraining emerging technologies has caused the unfortunate result of limiting attention on the ability of emerging technologies to increase LOAC compliance. In fact, advanced weapon systems provide significant opportunities for armed forces to dramatically improve LOAC compliance and substantially increase the protection for civilians during armed conflict. Increased use of emerging technologies, applied in ways focused on protection of civilians and civilian objects, would undoubtedly increase LOAC compliance.

AR-Compliance_EN.pdf.

https://www.eda.admin.ch/content/dam/eda/en/documents/aussenpolitik/voelkerrecht/32IC-AR-Resolution_EN.pdf

[9] https://www.icrc.org/en/document/asia-new-weapons-international-humanitarian-law;

https://www.icrc.org/en/war-and-law/weapons/ihl-and-new-technologies

[10] https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war

[11] https://www.icrc.org/eng/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm

However, many of the current issues with LOAC compliance are rooted in the limitation that parties to an armed conflict are only required to do what is "feasible" to protect civilians and civilian objects during hostilities. This would, of course, apply to the employment of emerging technologies. An understanding of feasibility that is enlightened by the use of emerging technologies will dramatically increase the effectiveness of steps parties to an armed conflict can take to protect the civilian population. Further, the effectiveness and ease of application of these emerging technologies should be reflected in what the international community accepts as feasible actions by the parties to an armed conflict.

Part II of this article will briefly describe the principles of the law of armed conflict that apply to lethal military operations. Part III will identify the role of "feasibility" in non-compliance and note its role as an escape valve by which parties to the armed conflict justify inaction in protecting civilians. Part IV will identify emerging technologies that are to varying degrees both ubiquitous and inexpensive that could be feasibly used to assist in the protection of civilians. This Part will further argue that the international community's understanding of "feasible" should include the employment of these emerging technologies, requiring both States and commanders to consider their use as part of the legal obligation to apply feasible precautions in both the attack and in defense. The paper will conclude in Part V.

II. PRINCIPLES OF THE LOAC

The law of armed conflict is a historic and evolving set of rules based on a mixture of moral

and ethical concerns and perceived reciprocal benefits. Underlying the entire scheme are several foundational principles that provide the intellectual and practical basis for the modern rules. The two foundational principles most important for consideration of the current topic of the value of emerging technologies for increasing LOAC compliance are the principles of distinction and proportionality. Additionally, the more modern application of those principles is found in the rules on precautions, both in the attack and in the defense. A brief analysis of these four principles, including examples of non-compliance, will allow a more in-depth review of the doctrine of feasibility in Part III.

A. Distinction

The principle of distinction has a long history in the LOAC and has been referred to as the "grandfather" of all LOAC principles. It was codified as early as the Lieber Rules,[12] confirmed in the Hague Rules,[13] and its most current formulation comes from Article. 48 of API which states

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian

[12] Instructions for the Government of Armies of the United States in the Field, General Orders No. 100, art. 19 (1863) *reprinted in* Schindler & Toman, THE LAWS OF ARMED CONFLICTS 315 (Dietrich Schindler & Jiri Toman eds., 2004).

[13] Hague Convention (IV) Respecting the Laws and Customs of War on Land, art. 25, Oct. 18, 1907, 36 Stat. 2277

population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[14]

To facilitate this distinction between civilians and military objectives, individuals are generally grouped into two categories—civilians and combatants[15]—and combatants are obligated to distinguish themselves from the civilian population.[16] Civilians and civilian objects are then protected from the dangers of military operations[17] and "shall not be the object of attack"[18] as long as civilians don't "take a direct part in hostilities."[19]

These rules are generally accepted as customary international law in both international

[14] Protocol Additional to the Geneva Convention of August 12, 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977, art. 48, 1125 U.N.T.S. 3 [hereinafter AP I].

[15] *Id.* at art. 50.

[16] *Id.* at art. 44.

[17] *Id*. at art. 51.1; The ICRC *Commentary* adds, "The term 'military operations' should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat." Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, at 680 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter AP Commentary].

[18] AP I, *supra* note 14, at art. 51.2.

[19] *Id*. at art. 51.3.

armed conflicts (IACs) and non-international armed conflicts (NIACs).[20] Further, the US Department of Defense Law of War Manual embraces distinction as one of the core LOAC principles, defining it as an obligation to "distinguish principally between the armed forces and the civilian population, and between unprotected and protected objects."[21]

In other words, it is fundamental to the LOAC for those engaged in armed conflict to distinguish themselves from the civilian population and to only direct their military operations against other fighters. Concurrently, if civilians want to enjoy the benefits of this protection, they must refrain from taking a direct part in the hostilities. These mutually reinforcing obligations are designed to protect non-fighters from the effects of armed conflict to the maximum extent possible.

B. Proportionality

Complementary to the principle of distinction is the rule of proportionality. The rule is often defined as requiring commanders to "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military

[20] *See generally* 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: RULES, PART I (2005) [hereinafter CIHL STUDY]

[21] U.S. DEP'T OF DEF. OFFICE OF GEN. COUNSEL, DEPARTMENT OF DEFENSE LAW OF WAR MANUAL ¶ 2.5 (2015) (updated Dec. 2016) [hereinafter DoD LOWM].

advantage anticipated."[22] The rule of proportionality recognizes that it is likely impossible to prevent all civilian deaths, even when correctly applying the principle of distinction during an armed conflict. However, excessive civilian casualties are prohibited.

Like the principle of distinction, proportionality is accepted as customary international law in both IACs and NIACs.[23] The DoD Law of War Manual defines the rule of proportionality as the obligation to "refrain from attacks in which the expected loss of civilian life, injury to civilians, and damage to civilian objects incidental to the attack would be excessive in relation to the concrete and direct military advantage expected to be gained."[24] The Manual further points out that this rule

---

[22] AP I, *supra* note 14, at art. 57.2(a)(iii). The Commentary notes that

> The concept of proportionality occurs twice in Article 57: in the sub-paragraph under consideration here and in sub-paragraph (b) following it. However, it is also found in Article 51 *(Protection of the civilian population),* paragraph *5(b).* It occurs again in Protocol II (Article 3, paragraph 3(c)) annexed to the 1980 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, with regard to land mines laid outside military zones. In these four cases the wording used is deliberately identical.

AP Commentary, *supra* note 17, at 683.

[23] *See* CIHL Study, *supra* note 20, Rule 14.

[24] DoD LOWM, *supra* note 21, at ¶ 5.10.

does not provide any protection to military objectives, but only to "persons and objects that may not be made the object of attack."[25]

The rule of proportionality, then, in contrast to the principle of distinction which protects civilians from attack, protects civilians who are not the direct object of attack but may be incidentally injured due to the effects of an otherwise lawful attack. Applying the rule of proportionality may result in a commander deciding to cancel or suspend an attack.[26]

C. Precautions in the Attack

Listed alongside the rule of proportionality in the DoD Law of War Manual is the duty those military operators who are conducting attacks to apply feasible precautions. The Manual states the obligation as requiring combatants to "take feasible precautions in planning and conducting attacks to reduce the risk of harm to civilians and other persons and objects protected from being made the object of attack."[27]

Article 57 of Additional Protocol I (API) states eight specific precautionary requirements, two of which are restatements of the proportionality rule. All eight precautionary measures obligate Parties through the use of the term "shall." Even Article 57.1 which imposes the least

[25] *Id.* at ¶ 5.10.1.

[26] AP I, *supra* note 14, at art. 57.2(b).

[27] DoD LOWM, *supra* note 21, at ¶ 5.10.

defined requirement of taking "constant care" to spare the civilian population uses the mandatory language of "shall." Other precautions in Article 57 include verifying that targets are neither civilians nor civilian objects,[28] selecting means and methods that will avoid or at least minimize civilian casualties and damage,[29] refraining from attacks that violate the rule of proportionality,[30] canceling or suspending on-going attacks if it is discovered that they will violate the rule of proportionality,[31] providing warnings to the civilian population,[32] selecting the target that will cause the least incidental civilian injury and damage in cases where there is more than one target that provide similar military advantage,[33] and applying the LOAC rules to attacks at sea or in the air."[34]

These precautions are generally accepted to be customary international law and are binding on nations in both IACs and NIACs.[35]

D. Precautions Against the Effects of Attacks

[28] AP I, *supra* note 14, at art. 57.2(a)(i).

[29] *Id.* at art. 57.2(a)(ii).

[30] *Id.* at art. 57.2(a)(iii).

[31] *Id.* at art. 57.2(b).

[32] *Id.* at art. 57.2(c).

[33] *Id.* at art. 57.3.

[34] *Id* at art. 57.4.

[35] *See* CIHL Study, *supra* note 20, Rules 15-21.

In addition to precautions when attacking, defending forces also have precautionary obligations.[36] As Bothe, Partsch and Solf said in discussing the "precautions" provisions of API:

> The obligation to take precautions to protect the civilian population and civilian objects against the collateral effects of attacks is a complementary one shared by both sides to an armed conflict in implementation of the principle of distinction. . . Article 58 is the provision applicable to the party having control over the civilian

[36] As Queguine has argued,

> Contrary to what is sometimes maintained, Additional Protocol I does not introduce a fundamental imbalance between the precautions required of the defender and those required of the attacker. Responsibility for applying the principle of distinction rests equally on the defender, who alone controls the population and objects present on his territory, and on the attacker, who alone decides on the objects to be targeted and the methods and means of attack to be employed. Consequently, only a combination of precautions taken by all belligerents will effectively ensure the protection of the civilian population and objects.

Jean-Francois Queguiner, Precautions Under the Law Governing the Conduct of Hostilities, 88 IRRC 793, 820-21 (2006).

> population to do what is feasible to attain this goal. It is complementary to, and interdependent with, Art. 57 which implements, in somewhat more mandatory terms, the obligations of the attacking Party in this regard.[37]

Infusing the role of the defender with even more importance, Hays Parks argues that "[i]f the new rules of Protocol I are to have any credibility, the predominant responsibility must remain with the defender, who has control over the civilian population."[38]

---

[37] Michael Bothe, Karl Josef Partsch & Waldemar A. Solf, New Rules for Victims of Armed Conflicts 413 (2013). Long-time US DoD Law of War expert Hays Parks agrees and states:

> the reason behind the requirement for warning stated in Hague Conventions IV and IX, and in article 57(2)(c) of Protocol I: it enables the Government controlling the civilian population to see to its evacuation from the vicinity of military objectives that might be subject to attack; it also permits individual civilians to remove themselves and their property from high-risk areas. There is little else that an attacker can do to avoid injury to individual civilians or the civilian population as such. Any attempt to increase an attacker's responsibility - particularly where a defender has failed or elected not to discharge his responsibility for the safety of the civilian population - will prove futile.

W. Hays Parks, Air War and the Law of War, 32 Air Force Law Review 1, 158 (1990).

[38] Parks, *supra* note 37, at 153-54 (1990). Law of War expert, Matthew C. Waxman

This view is echoed in the U.S. DoD law of War Manual which states "[t]he party controlling civilians and civilian objects has the primary responsibility for the protection of civilians and civilian objects. The party controlling the civilian population generally has the greater opportunity to minimize risk to civilians."[39]

Given this logic, Article 58 endeavors to properly place responsibility on the defender by focusing on two main obligations. The first is to segregate military objectives from civilians

---

demonstrates the logic of this when he argues:

> First, the defending force often has substantial control (whereas the attacker has none) over where military forces and equipment are placed in relation to the civilian population. Second, the defending power often has better information than the attacker about where civilian persons and property actually are, and is therefore better positioned to avoid knowingly leaving them in harm's way. And, third, the defender's actions—including its proper efforts to protect itself by resisting attack—may contribute to the danger facing noncombatants. The defender's choice of strategy, too, will significantly determine the extent to which civilians are vulnerable to possible attack.

Matthew C. Waxman, International Law and the Politics of Urban Air Operations, 16 (2000).

[39] DoD LOWM, *supra* note 21, at 187.

(paragraphs (a) and (b)). This includes not placing military objectives near civilians and removing any civilians from areas where military objectives are located. The second obligation is to protect civilians and civilian objects under the military control from the dangers inherent in military operations (paragraph (c)). These specific obligations will now be discussed in further detail.

This specific provision is not echoed in NIAC rules and is binding, therefore, only on Parties to the Protocol and only in IACs.[40] However, the ICRC has argued that it is considered part of customary international law[41] as an application of the principles of distinction and

[40] The DoD LOW Manual also does not accept Article 58 as customary international law but does argue that:

> Outside the context of conducting attacks (such as when conducting defense planning or other military operations), parties to a conflict should also take feasible precautions to reduce the risk of harm to protected persons and objects from the effects of enemy attacks. In particular, military commanders and other officials responsible for the safety of the civilian populations must take reasonable steps to separate the civilian population from military objectives and to protect the civilian population from the effects of combat.

DoD LOWM, *supra* note 21, at 271-72. This use of the word "must" reflects the United States' understanding of the obligations set out in Article 58.

[41] CIHL Study, *supra* note 20, at Rules 22-24; Michael, N. Schmitt, Charles H.B. Garraway &

proportionality. Additionally, in 2003, at its 28th International Conference, the ICRC identified the requirements of the defender to protect the civilian populations as one of the areas that needed greater emphasis.[42]

E. Summary

These are just a few of the foundational principles of LOAC that apply most directly to the law of targeting and, coincidentally, that are most modified by what is "feasible." It is to this doctrine of feasibility that this article now turns.

III. FEASIBILITY

Four of the eight provisions discussed above with respect to "Precautions in the Attack" and the entirety of the "Precautions Against the Effects of Attacks" are not absolute in their application. Rather, the attacker or defender need only apply these rules when it is "feasible."[43] It

---

Yoram Dinstein, *The Manual on the Law of Non-International Armed Conflict with Commentary*, ¶ 2.3.7 (2006), *reprinted in* 36 Isr. Y. Hum. Rtx. (special supplement) (Yoram Dinstein & Fania Domb eds., 2006).

[42] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2-6 December 2003, at 14 *available at* https://www.icrc.org/eng/assets/files/other/ihlcontemp_armedconflicts_final_ang.pdf.

[43] Articles 57.2(a)(i), 57.2(a)(ii) and 58 of AP I expressly use the term feasible as a limitation on

seems obvious then, that understanding the meaning of "feasible" will give important insight into the obligations to which it applies.[44]

A. Negotiating History

During the course of the negotiations of API, the national representatives were anxious to set a standard that would require diligence on the part of the commander but would not be one with which it was beyond his capability to comply. As a result, the use of the term "feasible" began to appear in several sections of proposed language, acting as a limitation on specific obligations during armed conflict.[45] It became clear that the repeated use of the term required some common understanding of its meaning and application.[46]

John Redvers Freeland, head of UK delegation during several of the sessions, clarified that

---

the requirement of the corresponding rule. Article 57.2(c) using the language "unless circumstances do not permit," and Article 57.4 requires Parties to "take all reasonable precautions." *See* AP I, *supra* note 14.

[44] See generally The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare, 93 Int'l L. Stud. 322, 373-88 (2017) (hereinafter Challenges).

[45] *Id.,* at 373 (2017) where the authors state "The [Study Group] noted that the general understanding of feasibility is the same for both precautions in attack and precautions against the effects of attacks."

[46] *Id.,* at 210.

the words "to the maximum extent feasible" related to what was "workable or practicable, taking into account all the circumstances at a given moment, and especially those which had a bearing on the success of military operations."[47] S.H. Bloembergen, representing the Netherlands, was in agreement, stating that "feasible" should be "interpreted as referring to that which was practicable or practically possible, taking into account all circumstances at the time."[48] According to the Official Record of the Conference, at least eight other states joined with the UK and Netherlands on this interpretation with respect to the meaning of the term feasible in Article 58 as well as the numerous other articles that use that term.[49]

This interpretation is also reflected in the ICRC commentary to Article 57 which states:

The words "everything feasible" were discussed at length. When the article was

[47] VI OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS, GENEVA 1974-77 (1978) at 214, http://www.loc.gov/rr/frd/Military_Law/RC-dipl-conference-records.html (hereinafter VI Official Records). *See also* Challenges, *supra* note 44, at 374-76 (2017) for additional uses of the term and their definition.

[48] Official Records, *supra* note 47, at 214.

[49] Julie Gaudreau, The Reservations to the Protocols Additional to the Geneva Conventions for the Protection of War Victims, International Review of the Red Cross, No. 849, March 2003, pp. 143, 156-57 (2003); Eric Talbot Jensen, *Article 58 and Precautions Against the Effects of Attacks in Urban Areas*, 98 INT'L REV. OF THE RED CROSS 147, 163-66 (2016).

> adopted some delegations stated that they understood these words to mean everything that was practicable or practically possible, taking into account all the circumstances at the time of the attack, including those relevant to the success of military operations. The last-mentioned criterion seems to be too broad, having regard to the requirements of this article. There might be reason to fear that by invoking the success of military operations in general, one might end up by neglecting the humanitarian obligations prescribed here. Once again the interpretation will be a matter of common sense and good faith. What is required of the person launching an offensive is to take the necessary identification measures in good time in order to spare the population as far as possible. It is not clear how the success of military operations could be jeopardized by this.[50]

With respect to the use of "feasible" in Article 58, there was discussion concerning to which portions of Article 58 the use of the term should apply. Initially, there was disagreement on this issue. Brigadier General Wolfe, the Canadian representative, proposed that the limiting language of "to the maximum extent feasible" be applied to the entire provision.[51] The proposed amendment

---

[50] AP Commentary, *supra* note 17, at 681–82.

[51] 14 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS, GENEVA 1974-77 (1978) at 199, http://www.loc.gov/rr/frd/Military_Law/RC-dipl-conference-records.html (hereinafter XIV Official Records).

was eventually accepted by consensus.[52]

B. Post API Commentary

Since the formulation and ratification of API, States and commentators have discussed the meaning of feasibility, particularly with respect to precautions. For example, the U.S. DoD Law of War Manual lists five examples of "circumstances" which may impact the feasibility of a precaution. They are:

- The effect of taking the precaution on mission accomplishment;

- Whether taking the precaution poses risk to one's own forces or presents other security risks;

- The likelihood and degree of humanitarian benefit from taking the precaution;

- The cost of taking the precaution, in terms of time, resources, or money;

- Whether taking the precaution forecloses alternative courses of action.[53]

[52] *Id.*, at 304; Jensen, *supra* note 49, at 166.

[53] DoD LOWM, *supra* note 21, at 190.

These examples, while not meant to be exclusive, provide insight into how at least one State expects its commanders to determine what is feasible.

Writers in the area have also consider such factors and tend to advocate for a strong application of the rules and that such action would significantly strengthen the practical protections for civilians. For example, Kalshoven and Zegveld argue that:

> It is a truism that effective separation of civilians and civilian objects from combatants and military objectives provides the best possible protection of the civilian population. It is equally obvious that in practice, this may be very difficult, if not impossible, to realise. This much is certain, however, that parties must, "to the maximum extent feasible", endeavour to bring about and maintain the above separation.[54]

Bloembergen's reference to "taking into account all circumstances at the time"[55] mentioned above has been understood to allow for the fact that a State's or commander's decisions are limited by his circumstances and knowledge at the time, and therefore such decisions should not be subject to subsequently informed analysis. This expression stems from the WWII prosecution of German

[54] Frits Kalshoven and Liesbeth Zegveld, Constraints on the Waging of War, at 117 (2011, 4th ed.).

[55] VI Official Records, *supra* note 47, at 214.

General Lothar Rendulic.[56] General Rendulic anticipated a swiftly advancing Russian force and conducted a scorched earth policy in Finnmark to inhibit troop movement. In adjudicating Rendulic's responsibility for wanton destruction of property without military necessity, the Court determined that the legal standard was "consideration to all factors and existing possibilities" as they "appeared to the defendant at the time."[57] This same standard is understood to apply to the feasibility of precautions in the defense.

The general consensus is that there has been an increasing focus on precautions since the codification of API, but there has been general acceptance of the application of feasibility and of its understanding of what is practical in the course of armed conflict.

C. Conclusion

Both at the time precautions were codified in API, and in application since, feasibility has presented a limiting factor to the requirements of both the attacker and defender with respect to applicable precautions. States recognized the practical difficulties some precautions might present

[56] *See* United States v. Wilhelm List, et. al, XI Trials Of War Criminals Before The Nuernberg Military Tribunals Under Control Council Law No. 10, 1295 (1950) [hereinafter Hostage Judgment]; *See also* Eric Talbot Jensen, *Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 Am. U. Int'l L. Rev. 1145, 1181-83 (2003).

[57] Hostage Judgement, *supra* note, 56, at 1296.

and have continued to embrace feasibility as the test for the implementation of the obligation. The article now turns to how emerging technology might influence the understanding of feasibility and its application in armed conflict.

IV. LEVERAGING EMERGING TECHNOLOGIES

There is no need to devote effort to describing the ever-increasing development of technology across the world. These emerging technologies have dramatically influenced the conduct of warfare in the past and will continue to do so in the future.[58] In many cases, the emergence of technology has led to increasing destructiveness of weapons systems. It has also led to enhanced precision of lethal weapons.[59]

Little has been written about non-lethal technologies and their potential to provide meaningful additional protections for civilians and civilian objects. Importantly, the effectiveness and ease of application of many of these emerging technologies make them extremely feasible to incorporate by both the attacker and defender. In fact, as will be demonstrated below, these

[58] *See generally* Eric Talbot Jensen, *The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots*, 35 Mich. J. Int'l L. 253 (2014).

[59] *See* Christopher B. Puckett, *In This Era of Smart Weapons, is a State Under and International Legal Oblication to use Precision-Guided Technology in Armed Conflict*, 18 EMORY INT'L. L. REV. 645 (2004).

emerging technologies are so accessible, and will only become more so with the passage of time, that their employment should be reflected in what the international community accepts as feasible by the parties to an armed conflict.

A. An Evolving Standard

The clarity of the standard of feasibility does not mean that the requirements to meet the standard are static. In fact, the commonly accepted understanding that feasible means "that which was practicable or practically possible, taking into account all circumstances at the time"[60] implies that the standard might change over time and in different circumstances. The evolving nature of the "feasible" standard is especially important in light of emerging technologies. As forces participate in armed conflict, advanced technology will provide increased capabilities to comply with precautionary measures that are feasible, even if they weren't feasible months or years prior. In other words, though "feasibility" is absolutely an important standard that must be maintained in assessing compliance with precautions in both the attack and the defense, it is also an evolving standard that must take account of developing technology.[61]

Bill Boothby, writing with respect to new technology and the LOAC, has already reflected this idea. He argues:

[60] VI Official Records, *supra* note 47, at 214.

[61] Jensen, *supra* note 49, at 173-75.

> In considering the legal implications of futuristic new technologies, it is important to bear in mind that the law of targeting, for example, is replete with relative language: . . . and so is the "maximum extent feasible" in Article 58 of Additional Protocol I. Those relative notions seem likely to be capable of adaptive interpretation as technological development improves.[62]

An example illustrates Boothby's point. Targeting mobile enemy positions in WWII that were deep behind enemy lines often had to be done on limited and potentially stale intelligence. The emergence of satellite imagery has revolutionized the accuracy of targeting through real-time intelligence.[63] For States that have ready access to such intelligence, it seems likely that the international community would consider the use of such intelligence in targeting decisions to be feasible. Similarly, when a defender uses indirect fire against an enemy that has counter-battery radar, that defender should anticipate counter-fire in response to its attack and endeavor to segregate or protect civilians and civilian objects in accordance with Article 58 of API.

The ICRC has agreed with this approach, stating "[a]s access to advancing technology that could assist the defender in applying precautions becomes more pervasive, the expectation that defenders will make use of those technologies should increase."[64] In fact, the ICRC has recently

---

[62] William H. Boothby, The Legal Challenges of new Technologies: An Overview 25 *in* New Technologies and the Law of Armed Conflict (H. Nasu and R. McLaughlin, eds.) (2014).

[63] *See* Puckett, *supra* note 59.

[64] Jensen, *supra* note 49, at 174.

published a commentary on the implications of new technologies in armed conflict, where the author concludes,

> [e]Examining legal issues such as these will only become increasingly relevant to situations of armed conflict, as it is reasonable to assume that parties to the conflict will use all available means at their disposal—including new information and communications technologies—to interact with civilians. It is therefore worth emphasising that IHL could and should be applied also to operations using these new technologies.[65]

While counter-battery radar and real time satellite imagery are only available to sophisticated and well-financed forces, there are a number of emerging technologies such as the communication capabilities discussed by the ICRC that are readily available and relatively inexpensive that could be purchased and used by the vast majority of armed forces currently involved in armed conflict. The accessibility and potential effectiveness of these technologies in protecting civilians and civilian objects should demand that the armed forces incorporate them in

---

[65] Ponthus Winther, Military Influence Operations & IHL: Implications of New Technologies October 27, 2017, available at http://blogs.icrc.org/law-and-policy/2017/10/27/military-influence-operations-ihl-implications-new-technologies/?utm_source=ICRC+Law+%26+Policy+Forum+Newsletter&utm_campaign=51edbd5bb7-EMAIL_CAMPAIGN_2017_10_27&utm_medium=email&utm_term=0_8eeeebc66b-51edbd5bb7-69070909&mc_cid=51edbd5bb7&mc_eid=423dc3b81a

their military operations as feasible precautionary measures. Examples of these emerging technologies are discussed below.

B. Examples of Emerging Technologies

A host of advanced technologies already exist or are near production that could feasibly be used during armed conflict to better protect civilians and civilian objects. The following examples will be loosely grouped into three categories: sensors, communication devices and markers.

1. Sensors

One of the emerging technologies that is becoming more affordable and more pervasive is the use of sensors. Though the following sections will highlight specific types of sensors, they will work best in combination with both other sensors and other advanced technologies. DARPA is already very interested in the possibilities combinations of such sensors provide. In discussing the new Squad X Core Technologies program, DARPA states:

> To succeed in their missions, military units must have a robust, multi-faceted picture of their operational environments, including the location, nature and activity of both threats and allied forces around them. Technology is making this kind of rich, real-time situational awareness increasingly available to airborne and other vehicle-assigned forces, along with a capacity to deploy precision armaments more safely, quickly and effectively. Dismounted infantry squads, however, have so far

> been unable to take full advantage of some of these highly effective capabilities because many of the technologies underlying them are too heavy and cumbersome for individual Soldiers and Marines to carry or too difficult to use under demanding field conditions.
>
> DARPA's Squad X Core Technologies (SXCT) program aims to develop novel technologies that could be integrated into user-friendly systems that would extend squad awareness and engagement capabilities without imposing physical and cognitive burdens. The goal is to speed the development of new, lightweight, integrated systems that provide infantry squads unprecedented awareness, adaptability and flexibility in complex environments, and enable dismounted Soldiers and Marines to more intuitively understand and control their complex mission environments.[66]

This desire to provide better situational awareness, even at the lowest levels of tactical actions, is indicative of not only the market for these types of emerging technologies, but also the benefit that is seen to be gained. As sensors increase the battlefield awareness of fighters, it will allow both attackers and defenders to use that greater situational awareness to not only control their own fires but also (particularly in the case of the defender) direct their combat actions away from civilians.

[66] https://www.darpa.mil/program/squad-x-core-technologies

a. Acoustic

Acoustic sensors have been used on the battlefield since World War I.[67] Modern battlefield applications include small (4.25" DIA X 6.5" tall) acoustic ground sensors[68] as well as vehicle-mounted sensors.[69] Recent work has been done on mounting acoustic sensors to small balloons and then networking the data into a larger sensor network for provide the military with real-time intelligence on both enemy and civilian forces.[70] Additionally, work has been done on building robots that can acoustically locate gunfire and identify its source.[71]

Civilian systems that are currently in use, such as acoustic sensors to monitor traffic,[72]

---

[67] B. Kaushik, Don Nance, and K. K. Ahuja, A Review of the Role of Acoustic Sensors in the Modern Battlefield (2005), available at https://ccse.lbl.gov/people/kaushik/papers/AIAA_Monterey.pdf

[68] http://www.signalsystemscorp.com/3DASU_brochure.pdf

[69] http://www.signalsystemscorp.com/asu.html

[70] C. Reiff, T. Pham, M. Scanlon, and J. Noble, A. Van Landuyt, J. Petek and J. Ratches, ACOUSTIC DETECTION FROM AERIAL BALLOON PLATFORM, http://www.dtic.mil/dtic/tr/fulltext/u2/a432916.pdf.

[71] Battlefield Robot Can Detect Snipers, http://www.nbcnews.com/id/9608603/ns/technology_and_science-innovation/t/battlefield-robot-can-detect-snipers/#.WeDUl2iPK70.

[72] Barbara Barbagli, Gianfranco Manes, and Rodolfo Facchini, Acoustic Sensor Network for

could also be employed to provide protections for civilians. Such systems could not only be used to monitor the potential movement of enemy vehicles and provide early warning to civilians but also be used to monitor civilians traffic, providing armed forces with situational awareness as to civilian vehicular movement.

b. Seismic

Seismic sensors are also an area where fighters can readily produce increased situational awareness in an effort to better protect civilians. Civilian uses already include seismic sensing tied to cell phones to provide early warning of potential earthquakes in California.[73] Military applications of seismic sensors have been around since the early 1980s and have been steadily improving.[74] A host of new systems are now being used[75] both on ground and underwater.[76]

Vehicle Traffic Monitoring (2012), https://www.researchgate.net/profile/G_Manes/publication/260385445_Acoustic_Sensor_Network_for_Vehicle_Traffic_Monitoring/links/556713fa08aeccd777377ff0/Acoustic-Sensor-Network-for-Vehicle-Traffic-Monitoring.pdf.

[73] (http://seismo.berkeley.edu/blog/2016/02/11/seismic-sensors-by-the-million.html)

[74] https://fas.org/man/dod-101/sys/land/rembass.htm

[75] http://www2.l3t.com/cs-east/pdf/bais.pdf

[76] Alain Lemer and Frederique Ywanne, Acoustic/Seismic Ground Sensors for Detection, Localization and Classification on the Battlefield (2006), available at

Many of these systems are inexpensive and have relatively long battery life. They could easily be placed in areas of regular civilian traffic to provide situational awareness of civilian movement, allowing the military commander to avoid military operations in those areas or to track the movement of civilians out of areas that could then be used for military operations with lower risk to civilians.

c. Visual

Though more expensive than some of the previously mentioned sensors, visual sensors provide another excellent method for fighters to increase protections for civilians and civilian objects. There are a large number of options that provide a wide array of capabilities. For example, there are mobile vehicle cameras[77] as well as cameras that can be static.[78] These cameras can be

https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA479047.xhtml.

[77] https://www.amazon.com/OldShark-Dashboard-Recorder-G-Sensor-Recording/dp/B01DLWBPCA/?tag=aboutcom02lifewire-20&ascsubtag=4062264%7Cgoogle.com%7C%7C%7C%7C2%7C)

[78] Bastian Leibe, Konrad Schindler, Nico Cornelis, and Luc Can Gool, *Coupled Object Detection and Tracking from Static Cameras and Moving Vehicles*, available at https://www.vision.ee.ethz.ch/publications/papers/articles/eth_biwi_00556.pdf (last accessed June 8, 2018).

connected to the internet and then operated from mobile phones or other devices.[79] Some rely on batteries or direct power, while others operate on solar power.[80]

One of the most intriguing use of visual sensors in modern conflict has been demonstrated by very small drones that provide excellent situational awareness for combat forces. Personal drones that cost less than $2,000 and have a 4-mile flight radius have been used quite effectively in the fight against ISIS, for example.[81]As recently reported in the Wall Street Journal:

> The latest advance in Mosul was aided in part by the drones, quadcopters that are small enough to carry in a backpack, sell for about $1,500 commercially and are rigged with cameras on the underside.
>
> Iraqi counterterrorism forces have said they used quadcopters to supply aircraft with the U.S.- led coalition with some of their first targets in the Old City.
>
> Iraq's federal police say they do the same.
>
> Islamic State terrorized Iraqi forces earlier in the battle for the city by using their

[79] (http://thewirecutter.com/reviews/best-wireless-outdoor-home-security-camera/)

[80] (https://www.eyetrax.net/solar-powered-motion-activated-cellular-camera-how-it-works)

[81] (https://store.dji.com/product/mavic-pro?set_country=us&gclid=CLOazZ_BjNQCFceLswodr9EOaw)

own drones rigged to drop grenades. Now, Iraq's security forces have turned the technology against the militants.

At a command post near the front lines, American combat advisers huddled days ago around stacks of high--tech communications equipment and screens with feeds from multimillion-dollar aircraft while they waited patiently for an Iraqi quadcopter to give them the battlefield intelligence needed for an airstrike.

"Using the Iraqi drones is something new," said Brig. Gen. Walid Khalifa, deputy commander of the Iraqi Army's 9th Division. "We see the enemy and we decide its location and we give the coordinates of targets. It's faster than before."[82]

---

[82] Ben Kesling and Ghassan Adan, "Low-Tech Gadgets Steer Battle to Retake Rest of Mosul," *The Wall Street Journal* (Europe Edition), pg. A3, 21 June 2017. The article continued:

When Iraqi drone pilots fly a quadcopter over a target—and bring that target up on screen, showing militants fighting Iraqi troops in high definition—Col. Browning said he gets what he needs to authorize a strike in seconds.

"We're able to deliver joint fires essentially at their command," he said, referring to airstrikes, artillery and other weapons.

Iraqi troops have been tinkering with quadcopters to make it possible for them to

d. Thermal

The last example in the area of sensors is thermal sensor. Though generally more expensive than simple visual sensors, they provide the same kind of clarity on civilian movements, even in darkness. The availability of thermal mapping services[83] may be limited in areas of armed conflict, but the tools to conduct thermal surveillance are available on the open market and can be purchased and employed in a number of effective ways.

As with the vast majority of sensors currently available, thermal sensors can be connected to the internet and the data can be live-streamed in a way that provides real-time intelligence. Such data would be invaluable to fighters who were endeavoring to avoid targeting civilians or who were trying to segregate military operations from places where civilians were present.

---

fly farther and still provide real--time video feeds in dense parts of Mosul.

> Col. Browning said Iraqi drone technicians had fitted drones with bigger batteries, giving them extended range. If one falls from the sky or gets shot down, they launch another at little cost, he said.

Ben Kesling and Ghassan Adan, "Low-Tech Gadgets Steer Battle to Retake Rest of Mosul," *The Wall Street Journal* (Europe Edition), pg. A3, 21 June 2017.

[83] (http://www.resourcemappinggis.com/app_aerial.html)

e. Conclusion

In conclusion, the effectiveness and ease of acquisition and application make sensors an extremely important capability with respect to protecting civilians on the battlefield. Because of their ease of application and effectiveness, militaries should consider them in conducting military operations, and nations should seriously consider them when determining what precautions are "feasible".

2. Communication Devices

Sensors are generally passive collectors that can provide important data concerning civilian locations and movements. In contrast, communication devices are generally active devices that allow fighters to send and receive messages from the civilian population. The devices are roughly categorized below as one-way devices and devices that allow two-way communication.

a. One-Way

One-way communication systems are used widely as part of emergency response systems.[84] They also have been used to notify individuals of certain criminal activity, such as child kidnappings.[85] These systems can communicate in any number of ways, but the most often used

[84] https://www.ready.gov/alerts; (http://www.emergencyalert.gov.au/)

[85] https://www.amberalert.gov/

methods appear to be email[86] and cell phone.[87]

The benefits of these systems have been widely accepted and have promoted their widespread use. Similar systems have already been used in armed conflict, with the most publicized use probably being the use by the Israeli Defense Forces (IDF) to warn civilians of impending attacks.[88] The IDF has also used one-way warnings to let civilians know that the IDF was going to conduct military operations in the area where they currently were located and instructing them to leave the area or to stay in shelter where they currently were.[89] Prepositioned or mobile loudspeakers could also provide effective warning devices.[90]

Though not embraced widely in other armed conflicts, one-way cell phone and other messages could be a great source of feasible precautions designed to protect civilians and civilian objects. The effective use by Israel is an example of the feasibility of such programs and the accessibility and relatively low cost make these methods feasible for almost all fighting forces.

---

[86] (https://www.alertmedia.com/emergency-mass-notification)

[87] https://www.nap.edu/read/15853/chapter/2#9

[88] https://www.haaretz.com/idf-to-experiment-with-informing-the-public-via-text-messages-1.305621.

[89] https://www.nytimes.com/2014/07/09/world/middleeast/by-phone-and-leaflet-israeli-attackers-warn-gazans.html.

[90] (https://www.fedsig.com/product/modulator%C2%AE-ii-electronic-siren-series); (http://www.sentrysiren.com/warning-sirens-products/outdoor-warning-sirens/)

b. Two-Way

Of course, many of the previously mentioned one-way communication methods can also be two-way methods. For example, when an amber alert is sent concerning a kidnapped child, a phone number is provided to call if the person who received the notification has important information.[91] Similar methodologies could be employed more generally in appropriate circumstances.

In cases where fighters were attempting to protect civilians, two-way communications may raise risks of civilians directly participating in hostilities, an issue that commanders would have to be cognizant of. However, in the right circumstances, two-way communication systems would provide an excellent way for fighters to not only warn civilians but also gather information concerning their location and movements. For example, the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo established a Community Alert Network where locals can use UN distributed mobile phones to provide warning of imminent attacks.[92]

Of course, as with all of these emerging technologies, a nefarious fighting force could use these same technologies to facilitate attacks on civilians, but that possibility should not prevent

[91] https://www.amberalert.gov/

[92] New Technology for Peace & Protection: Expanding the R2P Toolbox by Lloyd Axworthy and A. Walter Dorn - http://www.mitpressjournals.org/author/Dorn%2C+A+Walter

legitimate fighting forces from introducing them as feasible options to comply with their precautionary obligations.

3. Markers

Other emerging technologies that impact what is feasible with respect to precautions include various forms of markers or marking systems. The systems are categorized below as visual, olfactory, and aural, but, of course, many effective markers will use elements of all three.

a. Visual

Visual markers are as old as armed conflict itself. They have been used to identify affiliations as well as signal battle commands. For purposes of this article, visual markers can also be used to mark areas where civilians might find safe refuge, direct civilians away from danger, or provide mobile signals of civilian movements, among other possible uses.

Colored smoke has a long history in armed conflict and continues to present simple, cheap, and easy methods to mark, direct, and protect civilian populations.[93] The use of flares or smoke producing agents can be tied effectively to colors, such as green smoke denoting a safe area and red meaning danger. Products that could be used for these purposes are used broadly in a large

[93] http://www.orionsignals.com/products/smoke-flares.html

number of forums and are easy to acquire.[94]

Similar to smoke or flares, simple paint or chalk could also serve these purposes. For maximum flexibility, such markings could be delivered by drone or vehicle. Ideally, markings systems would be widely published so that the civilian population would understand clearly what each marking meant, but basic use of red as danger and green as safe may be effective in emergency situations.

b. Olfactory

In addition to visual markings, olfactory markings could be an effective, feasible precaution. There are a large number of options for both smell and delivery system. A maloderant known appropriately as "Skunk" has been used both in law enforcement and LOAC scenarios.[95] Potential use of pleasant smells, either alone or as a contrast, might also be used to help in the protection of civilians.

Potential complications with the prohibition on the use of chemical agents[96] would need to

[94] http://www.enolagaye.com/wire-pull-smoke-grenades/

[95] http://www.defenseone.com/technology/2015/04/americas-police-will-fight-next-riot-these-stink-bombs/111430/

[96] Convention on the Prohibition of the Development, Production, Stockpilling and Use of Chemical Weapons and on Their Destruction Chemical Weapons Convention (CWC), Jan. 13,

be considered if olfactory signals were to be used widely on the battlefield, but just as the U.S. has reserved its ability to use riot control agents in certain circumstances, states could distinguish its use of such olfactory markers from conduct that would equate to a violation. Additionally, as the use of olfactory markers becomes more prevalent, its potential for misidentification will decrease.

c. Aural

Loud bangs or other audible signals are also a feasible precaution that is easily accessible and can be very effective in protecting the civilian population. Flash bang grenades are already widely used both by law enforcement[97] and by militaries.[98] They are also relatively easy to construct from normal household items.[99] Their combination of visual and aural signal makes them especially effective.

As mentioned above, the use of loudspeakers as a one-way communication device also doubles as an aural marking system. Either mobile or static speakers could be used to send warnings to the civilian population or provide direction as to where or whether to move.[100] These

1993, 1974 UNTS 45.

[97] http://www.npr.org/2015/01/18/378200407/investigation-reveals-rampant-use-of-flashbang-grenades-by-police

[98] https://www.defensemedianetwork.com/stories/tools-of-the-trade-the-flash-bang-grenade/

[99] http://www.instructables.com/id/How-to-make-a-Flash-Bang-Flash-grenade/

[100] https://www.fedsig.com/product/modulator%C2%AE-ii-electronic-siren-series;

speakers could have specific pre-recorded messages that triggered in combination with other sensors or that just played upon remote command.

C. "All Circumstances at the Time"

This list represents a small sampling of the technologies that are available or under development. The passage of time will only provide more capabilities and a more diverse range of capabilities and platforms. Further, all of these technologies are reasonably inexpensive, and the costs are lowering as research and development continue. They provide easily accessible and easily employable means that could provide dramatically increased situational awareness, which could easily be utilized to provide greater protections for civilians and civilian objects.

Despite the ubiquity of many of these technologies and ease of purchase and employment, the principle of feasibility applies both to encourage use of advancing technology and recognize that legitimate constraints exist. The argument above, that considering all circumstances at the time might condemn states and commanders who don't apply readily available and extremely effective technologies in order to protect civilians and civilian objects, also recognizes that accessibility and ubiquity are relative terms. For example, the fact that many of these technologies are available at local electronics stores in the military's nation does not mean they are accessible to the commander at the time he or she needs them. Many militaries will only allow employment of weapons and other systems that can be purchased through the general acquisition system and

---

http://www.sentrysiren.com/warning-sirens-products/outdoor-warning-sirens/

are in the logistics inventory. While this does not undermine the argument of applying feasible precautions, it does recognize that until the State has conducted the analysis at a national level and determined such tools should be purchased and provided to commanders, those commanders may not have them "available" to employ.

Similarly, as with the use of advanced lethal weapons, many States, including the United States, remain clear that the LOAC does not require the use of the most advanced possible weapons in every case. For example, the United States is clear that the LOAC does not require the use of precision guided munitions every time they are available.[101] Rather, the commander must consider the availability and quantity of those weapons, along with other potential missions when considering the proper application of precautions.

In other words, in arguing for an evolved standard of "feasibility" that includes emerging technologies that could have a significant benefit to the protection of civilians and civilian objects, it must be clear that whether a particular option is available to a commander will need to be a detailed analysis including more than simply pointing to a website where a specific technology is generally offered for sale.[102] On the other hand, States should be on notice that these technologies are available and, recognizing their LOAC obligations, begin to take steps to make such technologies truly available in "the circumstances at the time."[103]

---

[101] DoD LOWM, *supra* note 21, para. 5.2.3.2.

[102] Challenges, *supra* note 44, at 377.

[103] See UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*,

D. Conclusion

The use of these types of emerging technologies was dramatically illustrated recently when North Korea launched a missile over the Japanese island of Hokkaido. The Japanese government used a number of systems similar to those addressed above to warn its people of the launch and the potential danger it posed.[104] Similar usages are very feasible in modern conflict as precautions in both attack and defense. In fact, the understanding of the feasibility limitation on precautions required in military operations should include a recognition of the value of emerging technology and its potential to significantly protect civilians in armed conflict.

On the other hand, as stated in the US DoD Law of War Manual,

---

16 December 1966, United Nations, Treaty Series, vol. 993, at p. 3. Art. 2 states: "Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures." The use of "maximum of its available resources" provides an example of the international community agreeing to a very high standard with respect to resource commitment.

[104] http://www.independent.co.uk/news/world/asia/north-korea-missile-launch-japan-millions-warning-messages-hokkaido-take-cover-alarm-sirens-shinzo-a7917511.html

> The obligation to take feasible precautions is a legal requirement. However, the determination of whether a precaution is feasible involves significant policy, practical, and military judgments, which are committed to the responsible commander to make in good faith based on the available information.[105]

In many cases, the commander can only make that determination once his State has made such systems available to him or her. As the international community continues to consider and evolve the understanding of what is "feasible," States should make these technologies available to commanders and build doctrine and tactics to encourage their employment. Such actions have the potential to dramatically increase the protection of both civilians and civilian objects in modern armed conflict.

V. CONCLUSION

Compliance with LOAC is a continual problem that nations and other international actors such as the ICRC struggle to reinforce. Some excuses for non-compliance are rooted in the limitation that parties to an armed conflict are only required to do what is "feasible" to protect civilians and civilian objects during hostilities. An understanding of feasibility that is enlightened by the use of emerging technology will dramatically increase the effectiveness of steps parties to an armed conflict can take to actually protect the civilian population. Further, the effectiveness and ease of application of these emerging technologies should be reflected in what the international

[105] DoD LOWM, *supra* note 21, at para. 5.2.3.3.

community accepts as feasible by the parties to an armed conflict.