TARGETING CYBER ARMS DEALERS WHO DIRECTLY PARTICIPATE IN HOSTILITIES

*Collin Allan**

* Captain, Offutt AFB, U.S. Air Force. B.A., Brigham Young University (2010); J.D., Brigham Young University (2013). The views expressed in this article are those of the author, not the Judge Advocate General's Corps, the United States Air Force, the Department of Defense, or its elements.

I. INTRODUCTION

The threat of cyber attacks has occupied an increasingly prominent position in the media over the past several years.[1] This is due, in part, to both the United States' perceived vulnerability to a cyber attack[2] and the increase in the number of cyber attacks.[3] Cyber arms dealers are often overlooked in cyber security discussions. Nevertheless, they are playing an increasingly active role in cyber operations by developing tools for governments, groups, and individuals.[4]

Cyber arms dealers encompass a wide range of potential participants in armed conflicts, including independent civilians, organized crime groups, members of a state's armed forces, and corporations.[5] Their involvement in recent and ongoing cyber activities ranges from creating a cyber tool for carrying out cyber operations to providing technical support in the employment of a cyber tool.[6] Existing cyber tools created by cyber arms dealers enable the purchasers of such tools to "automate hacking" and carry out "espionage, fraud, and much more."[7] Some cyber tools sold include "12 months of technical support and updates to ensure the kits stay up to date on the latest web vulnerabilities."[8] Many of these tools are made available by organized crime groups like the Russian Business Network (RBN), a non-state actor comprised of civilians.[9]

Cyber arms dealers are increasingly making their wares more available, and the low cost of many of the tools enables individual

1. *See* Paul Szoldra, *Hacker Reveals How Devastating A Cyberattack On The Stock Market Could Be*, BUS. INSIDER, (Aug. 21, 2013, 8:56 AM), http://www.businessinsider.com/hacker-reveals-how-devastating-a-cyberattack-on-the-stock-market-could-be-2013-8 (discussing the implications of an attack on the United States stock market); *see also* Marie Szaniszlo, *Cyber Attack Danger Grows*, BOS. HERALD, Aug. 14, 2013, at 16 (discussing recent cyber-attacks on business and the Boston Police Department); *Cyber Attack Gits Istanbul Airports*, XINHUA (July 26, 2013, 5:15 PM), http://news.xinhuanet.com/english/world/2013-07/26/c_132577334.htm (China) (reporting an attack on the passport control system at the Istanbul International Airport);

2. *See* Leon E. Panetta, Sec'y of Def., Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012) (transcript available at the Department of Defense).

3. *See* Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BLOOMBERG BUS. (July 20, 2011), http://www.bloomberg.com/bw/magazine/cyber-weapons-the-new-arms-race-07212011.html.

4. *See id.*

5. *See id.*

6. *See* Ward Carroll, *Professional Cyber Arms Dealers*, DEF. TECH (Apr. 24, 2008), http://defensetech.org/2008/04/24/professional-cyber-arms-dealers.

7. *Id.*

8. *Id.*

9. *See id.*

civilians to launch devastating attacks against a broad spectrum of targets such as individuals, businesses, and states.[10] In 2008, it was estimated that "68,000 cyberattack tools" were in existence and "available for download."[11] The number of these tools "is growing fast," with an estimated "underground market for cyber attack tools [ ] in the hundreds of millions of dollars worldwide."[12] In 2008, the cost for these tools ranged from "less than $100 and up to $50,000."[13] In 2007, one tool "was used by a single person to attack and compromise over 10,000 websites in a single assault."[14]

One of the truly disconcerting aspects of cyber arms proliferation is the effect that civilians can have on battlefields located hundreds of miles from where the civilian is located. For example, in 2008, organized crime groups, including the RBN, made cyber attack tools available to hundreds of Russian hacktivists, allowing the civilian hackers to participate in the conflict between Russia and Georgia.[15] In some instances these tools aided Russian forces in their attacks against Georgian targets.[16] Given the United States' declaration that it will use kinetic force in response to cyber attacks, it is crucial to determine when a civilian participant in a cyber attack may be legally targeted.[17]

In some circumstances, it may make sense to use force against the creator of the cyber tools in order to prevent their dissemination or to prevent further interaction with the creator's customers. The United States may better obstruct the proliferation of harmful cyber tools by focusing on the genesis of the tools. If the United States chooses to use kinetic force against cyber arms dealers, it must use care in deciding when to use kinetic force to target civilians even when the civilians are creating and disseminating tools that are potentially harmful to the United States. The United States, of course, must be mindful of

10. *See id.*

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

15. *See* Paulo Shakarian, *The 2008 Russian Cyber Campaign Against Georgia*, MILITARY REV., Nov.-Dec. 2011, at 63, 64 (citing Dancho Danchev, *Coordinated Russia vs Georgia Cyber Attack in Progress*, ZDNET (Aug. 11, 2008, 4:23 PM), http://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/#!; Kenneth Corbin, *Lessons From the Russia-Georgia Cyberwar*, INTERNET NEWS (Mar. 12, 2009), http://www.internetnews.com/government/article.php/3810011/Lessons+From+the+RussiaGeorgia+Cyberwar.htm).

16. *See id.* at 63.

17. *See Morning Edition: Pentagon Strategy Prepares for War in Cyberspace* (NPR July 15, 2011) (quoting Deputy Defense Secretary William Lynn as saying, "The United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with proportional and justified military response at the time and place of its choosing.").

the domestic laws governing these situations, but it must also comply with the international laws governing conflicts.

This article discusses a set of scenarios where a cyber arms dealer may participate in an armed conflict that may make them targetable. Each scenario is designed to portray a level of participation in hostilities a cyber arms dealer may undertake that either does or does not render the cyber arms dealer targetable. The various scenarios are designed to elucidate situations where a cyber arms dealer may be legally targeted. All situations will be considered in a *jus in bello* context.

The law's application will be explored through the scenarios by applying the legal analysis provided in two different documents[18] that examine direct participation in hostilities.[19] Where relevant, other documents will be referenced, but this article will focus primarily on the two following documents: the *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (*Interpretive Guidance*), published in 2009, and the *Tallinn Manual on the Internal Law Applicable to Cyber Warfare* (*Tallinn Manual*), published in 2013.[20] While the *Tallinn Manual* was the first comprehensive manual on cyber operations,[21] both documents discuss the necessary analysis used to assess a civilian's actions before a civilian may be legally targeted. Specifically, the *Interpretive Guidance* is a treatment of international law as it applies to civilians who directly participate in hostilities.[22] The *Tallinn Manual* discusses how international law applies to cyber activities as well as those who carry out cyber operations, including civilians who directly participate in hostili-

18. N. ATL. TREATY ORG. COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]; NILS MELZER, INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW (2009).

19. While these are not the only documents addressing direct participation in hostilities, they are documents that have addressed the issue thoroughly. As recognized by the *Law of Armed Conflict Deskbook*, published by the International and Operational Law Department at the United States' Army Judge Advocate General's Legal Center and School, the ICRC's approach to direct participation in hostilities "remain[s] debated by nations, warfighters, and scholars alike." RICHARD P. DIMEGLIO ET AL., INT'L & OPERATIONAL LAW DEP'T, THE U.S. ARMY JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., LAW OF ARMED CONFLICT DESKBOOK 145 (William J. Johnson & Wayne Roberts eds., 2013). This article seeks to be part of that debate.

20. MELZER, *supra* note 18; TALLINN MANUAL, *supra* note 18.

21. Liis Vihul & Michael N. Schmitt, *The Tallinn Manual on Cyber Warfare—A First Tool for Legal Practitioners*, FIFTEEN EIGHTYFOUR, http://www.cambridgeblog.org/2013/11/the-tallinn-manual-on-cyber-warfare-a-first-tool-for-legal-practitioners-michael-schmitt-liis-vihul-nato (last visited Mar. 12, 2015).

22. MELZER, *supra* note 18, at 6.

ties through cyberspace.[23] Differences in language used to describe the direct participation in hostilities (DPH) targeting regime in each document leads to different results in some situations. While the goal of this paper is not to compare the *Interpretive Guidance* and *Tallinn Manual*, it is important to recognize where they agree and where they differ when applying or developing a targeting regime.

The *International Committee of the Red Cross's (ICRC) Interpretive Guidance* outlines the requirements a civilian's actions must meet before a party to the conflict can target that individual.[24] It is not binding on states but attempts to outline the international law obligations that states have in relation to civilians participating in armed conflict.[25] The *Interpretive Guidance* describes two major ways a civilian may become targetable: through assuming a continuous combat function with an organized armed group,[26] or through satisfying the *Interpretive Guidance's* three-part test.[27]

The *Tallinn Manual* was published by a group of international law experts (Tallinn Experts) in 2013.[28] Like the *Interpretive Guidance*, the *Tallinn Manual* is not a binding document[29] but provides a number of rules that describe how, according to the experts, international law applies to cyber operations and cyber warfare.[30] Several rules apply to situations where civilians may become targetable, including a section on civilians directly participating in hostilities.[31]

A. Introduction to Targeting[32]

Generally, individuals are targetable in three circumstances: (1) when they are a combatant; (2) when they are a member of an organized armed group who has assumed a continuous combat function; and (3) when they are an individual whose actions constitute direct

23. See Tallinn Manual, *supra* note 18, at 4, 118.

24. MELZER, *supra* note 18, at 46.

25. *See id.* at 9-10.

26. *See id.* at 31-34.

27. *See id.* at 46.

28. TALLINN MANUAL, *supra* note 18, at 9-11.

29. *Id.* at 1.

30. *See id.* at 1, 4.

31. *See id.* at 118-22. For an in-depth analysis of the differences in DPH targeting regimes between these two documents, see Collin Allan, Note, *Direct Participation in Hostilities from Cyberspace*, 54 VA. J. INT'L L. 173 (2013).

32. The author understands that a discussion of targeting assumes a lot in the cyber context. It is extremely difficult to locate the source of an attack, much less the creator of a tool. However, as technology develops it will likely become easier to perform these tasks, and a legal framework should be in place to guide the actions of states before technology reaches such a point.

participation in hostilities.[33] Parties to an armed conflict are legally obligated to distinguish between lawful targets and unlawful targets, and there is a presumption against targeting civilians.[34] This presumption can be overcome in certain circumstances explained below.

1. Combatant

In an International Armed Conflict (IAC), states engage in armed conflict through their respective armed forces.[35] The individual members of the armed forces are generally labeled combatants and are targetable in most situations.[36] They are not targetable when they are *hors de combat*.[37] This means that they are not targetable when they are out of combat. The Geneva Conventions outline when someone is *hors de combat*: when a soldier is sick, wounded, or surrenders.[38] It is legally impossible for an individual to be both a civilian and a combatant at the same time.[39] As long as the cyber arms dealer continues to be a member of a government's armed forces, that dealer would always be targetable as a combatant so long as the dealer remained a member of the government's armed forces. In a Non-International Armed Conflict (NIAC) between a state and a non-state party, members of the state's armed forces are still considered combatants in the sense that they are targetable (just as members of a

33. *See* Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1) art. 51, *adopted* June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) art. 13, *adopted* June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II]; Geneva Convention Relative to the Treatment of Prisoners of War art. 4, Aug. 12, 1949-Feb. 12, 1950, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention].

34. Additional Protocol I, *supra* note 33, 1125 U.N.T.S. at 25. While a civilian may not be legally targetable, his or her proximity to those directly participating in hostilities, whether a civilian or a combatant, could result in the civilian's death without the civilian being targeted. *See id.* at 25-26, 29.

35. *See id* at 23.

36. *See id.* at 23, 26. Although this is generally true for states, combatants can also be members of militias or persons belonging to organized resistance groups. *See id.*; Geneva Convention, *supra* note 33, 6 U.S.T. at 3320, 75 U.N.T.S. at 138.

37. Additional Protocol I, *supra* note 33, 1125 U.N.T.S. at 22.

38. Geneva Convention, *supra* note 33, 6 U.S.T. at 3318, 75 U.N.T.S. at 136; *see* Additional Protocol I, *supra* note 33, 1125 U.N.T.S. at 22. For an important discussion on the effects of being rendered *hors de combat* and when that designation should be applied to an individual under international law, see Geoffrey S. Corn et al., *Belligerent Targeting and the Invalidity of a Least Harmful Means Rule*, 89 INT'L L. STUD. 536 (2013).

39. *See* MELZER, *supra* note 18, at 20-21. Although a civilian directly participating in hostilities blurs the lines, this notion is based on the principle of distinction that requires participants to distinguish between civilian and military targets. *See id.* at 12.

state's armed forces are targetable in an IAC).[40] This paper will focus on situations in which cyber arms dealers are civilians—not a member of a state's armed forces—and may only be targetable depending on their level of involvement in the conflict.

2. Continuous Combat Function

Civilians who maintain a continuous combat function in an organized armed group are targetable.[41] This determination is made by examining whether an individual's continuous function aligns with the organization's mission in conducting hostilities in a conflict.[42] A civilian who participates sporadically or on an unorganized basis does not have a continuous combat function.[43] Those who assume a continuous combat function engage in combat-related activities; they are not exclusively engaged in "political, administrative, or other non-combat functions."[44] The *Interpretive Guidance* further clarifies that the "[c]ontinuous combat function requires lasting integration into an organized group acting as the armed forces of a non-State party to an armed conflict."[45] According to the *Interpretive Guidance*, a continuous combat function is not limited to wielding a weapon in combat, making it possible for a cyber arms dealer to be classified as such.[46]

3. Direct Participation in Hostilities (DPH)

A civilian who has not assumed a continuous combat function is protected from direct attack unless and for such time as that civilian directly participates in hostilities.[47] When civilians directly participate in hostilities, they are subject to attack by one of the parties to the conflict.[48]

A civilian's actions in relation to an armed conflict must satisfy the *Interpretive Guidance's* three-part test before that civilian is deemed targetable.[49] These three factors are labeled the threshold of

40. *See* Geneva Convention, *supra* note 33, 6 U.S.T. at 3318, 75 U.N.T.S. at 136.
41. MELZER, *supra* note 18, at 33.
42. *Id.*
43. *Id.* at 33-34.
44. *See id.*
45. *Id.* at 34.
46. *See id.*
47. Additional Protocol I, *supra* note 33, 1125 U.N.T.S. at 26; Additional Protocol II, *supra* note 33, 1125 U.N.T.S. at 615.
48. Additional Protocol I, *supra* note 33, 1125 U.N.T.S. at 26; Additional Protocol II, *supra* note 33, 1125 U.N.T.S. at 615.
49. MELZER, *supra* note 18, at 46.

harm, direct causation, and belligerent nexus.[50] First, in order to satisfy the threshold of harm requirement, a civilian's act "must be likely to adversely affect the military operations or military capacity of a party to an armed conflict."[51] This requirement may also be satisfied if the civilian's act is likely "to inflict death, injury, or destruction on persons or objects protected against direct attack."[52] Second, to satisfy the direct causation requirement, "there must be a direct causal link between the act and the harm likely to result" from that act independent of any other action taking place.[53] This requirement may also be satisfied if there is a direct causal link between the act and the "harm likely to result . . . from a coordinated military operation of which that act constitutes an integral part."[54] Third, for an act to satisfy the belligerent nexus requirement, it "must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another."[55]

B. Introduction to the Scenarios

The scenarios below involve a cyber arms dealer who has created a cyber tool or is helping to employ a cyber tool. The scenarios will explore the consequences of affiliating with certain groups, acting independently of groups, and varying levels of participation in ongoing hostilities between a non-internationally armed group and the armed forces of a state actor. The cyber tool in each scenario will be equipped with two capabilities: (1) the ability to disable communications between drones employed in Afghanistan and drone operators that are members of the NATO Forces in Afghanistan; and (2) the ability to access and disable drone weapons systems on weaponized

50. *Id.*

51. *Id.*

52. *Id.* The idea that individuals and objects are protected from direct attack is reflected in Common Article 3 in the Geneva Conventions and both Additional Protocols that require the humane treatment of people taking no active part in hostilities. *See* Additional Protocol I, *supra* note 33, 1125 U.N.T.S at 26; Additional Protocol II, *supra* note 33, 1125 U.N.T.S at 615; Geneva Convention, *supra* note 33, 6 U.S.T. at 3318, 75 U.N.T.S. at 136. Geneva Convention IV generally applies to the protection of civilians in wartime. Geneva Convention, *supra* note 33, 6 U.S.T. at 3516, 75 U.N.T.S. at 287. Furthermore, the Hague Regulations are a body of international law similar to that of the Geneva Conventions. Regulations Respecting the Laws and Customs of War on Land, annexed to Convention Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631. They provide regulations on the conduct of armed conflict and prohibit the "attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended." *Id.* art. 25.

53. MELZER, *supra* note 18, at 46.

54. *Id.*

55. *Id.*

drones and cameras on surveillance drones.[56] While this tool is non-lethal, its most important quality for the purposes of this paper's analysis is that it is capable of causing military harm.[57]

II. Discussion

A. *Variation 1: The Cyber Arms Dealer Sells the Tool to Al-Qaeda and Walks Away*

In this section, Al-Qaeda requests the cyber arms dealer to design the tool described above and explains to the dealer how the tool will be used. The dealer designs and sells it to Al-Qaeda, having no further interaction with the organization. The dealer does not employ the tool, nor does the dealer assume any role in the tool's implementation.

For the purposes of the *Interpretive Guidance*, because the dealer is walking away after selling the cyber tool, the dealer is not assuming a continuous combat function. The *Interpretive Guidance* states that an "individual[ ] whose function is limited to the purchasing, smuggling, manufacturing, and maintaining of weapons and other equipment outside specific military operations or to the collection of intelligence other than of tactical nature" does not assume a continuous combat function.[58] The *Interpretive Guidance* further explains that while these types of people "may accompany organized armed groups and provide substantial support to a party to the conflict, they do not assume a continuous combat function."[59] This means that for the principles of distinction they cannot be regarded as members of an organized armed group.[60] Because the dealer's main function is as a manufacturer and seller, she does not assume a continuous combat function and is therefore not targetable.

However, the dealer may become targetable if the dealer satisfies the *Interpretive Guidance's* three-part test for DPH.[61] The first ques-

56. The point of this paper is not necessarily to explore the reality or viability of cyber capabilities. Rather, the point is to focus on different scenarios in which a cyber arms dealer may participate in hostilities and accordingly be targeted. Regardless of the type of cyber tool involved, if the participation is the same, the dealer is targetable.

57. *See* Melzer, *supra* note 18, at 47. Melzer's theory does not limit military harm to the "infliction of death, injury, or destruction on military personnel or objects." *Id.* Rather, it includes "essentially any consequence adversely affecting the military operations or military capacity of a party to the conflict." *Id.*

58. *Id.* at 34-35.

59. *Id.* at 35.

60. *Id.*

61. *See id.* at 46. The following analysis is applicable to any subsequent variation where the cyber arms dealer manufactures and sells the tool. Therefore, this discussion will not be repeated in every scenario.

tion that must be answered is whether or not the civilian's act of manufacturing and selling the device satisfies the threshold of harm requirements. While the weapon itself causes military harm, the *Interpretive Guidance* focuses on the civilian's action—not the weapon's operational capacity. The tool disables drone communications and weapons functionality, adversely affecting the military operations or military capacity of a party to the conflict. While the cyber tool itself has the ability to cause harm sufficient to satisfy the threshold of harm requirement, the civilian act in question is one of manufacturing and selling.

Nevertheless, the *Interpretive Guidance* states, "When an act may reasonably be expected to cause harm of a specifically *military nature*, the threshold requirement will generally be satisfied regardless of quantitative gravity."[62] The *Interpretive Guidance*, then, considers situations where the sale of a tool would not satisfy this requirement.[63] For example, the dealer may not reasonably expect the sale of the tool to cause harm of a military nature if the dealer is unaware of his client's identity or is ignorant of how the tool is going to be employed.[64] Because the dealer is aware in this case that he is selling to Al-Qaeda, the dealer can reasonably expect the necessary harm to result. Both the tool's capabilities and how those capabilities are utilized are critical in informing the civilian's reasonable expectations in causing harm of a specifically military nature. If the tool is solely used to disrupt or disable drone communications, selling it to Al-Qaeda would make occurrence of the necessary harm reasonably expected, regardless of the seller's knowledge of his client's identity. This may be negated if the tool requires expertise or training to employ the tool. If a significant level of training would be required to employ the tool, then the sale of the tool to Al-Qaeda would not be reasonably expected to cause the necessary harm. If employment of the tool only required the push of a button, then the necessary harm becomes more of a reasonable expectation. Generally, the reasonable likelihood requirement makes it difficult to determine whether or not the threshold of harm requirement has been met. This determination is especially difficult for the victim of the cyber attack. In this situation, because the dealer knows the client's identity as well as the specific, desired capabilities of the tool,

62. *Id.* at 47.

63. *See id.* at 48.

64. *See id.* The problem here stems from the fact that it is often difficult to determine what an individual reasonably expects—especially when an event is being investigated after the fact. For example, it would be incredibly difficult to determine what the dealer reasonably expected in light of the fact that the tool the dealer created was used to disable drone communications.

and assuming no training or supervision is required, it could reasonably be expected that the necessary harm would result by selling the tool to Al-Qaeda.

Assuming that the threshold of harm requirement is met, the question remains as to whether or not the civilian's act of manufacturing and selling the tool meets the other two DPH requirements for sporadically but directly participating in hostilities. The direct harm requirement is satisfied when there is a direct causal link between the act and the harm likely to result from the act.[65] That is, "direct causation should be understood as meaning that the harm in question must be brought about in one causal step."[66] It may also be satisfied if there is a direct causal link between the act and the harm likely to result from a coordinated military attack.[67]

A civilian may indirectly participate in hostilities and remain legally protected from being targeted by a party to the conflict.[68] Activities that contribute to the general war effort or could be categorized as "war-sustaining efforts" generally do not satisfy the direct causation requirement because they do not qualify as the conduct of hostilities.[69] These types of activities include the "design, production, and shipment of weapons and military equipment," as well as "political, economic or media activities supporting the general war effort," including financial transactions.[70] The *Interpretive Guidance* admits that these types of actions "may ultimately result in harm reaching the threshold required for direct participation in hostilities."[71] However, the general war effort and war sustaining activities include activities that merely maintain or build up the capacity to cause such harm.[72] The main point of distinction between these courses of conduct and conduct of hostilities is that the purpose behind conduct of hostilities is to actually "bring about the materialization of" harm.[73]

---

65. *Id.* at 51.

66. *Id.* at 53.

67. *Id.* at 51.

68. *Id.*

69. *Id. But see* DEP'T OF THE NAVY ET AL., NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 8.2 (2007) ("Only military objectives may be attacked. Military objectives are . . . those objects which, by their nature, location, purpose, or use, effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack.") .

70. MELZER, *supra* note 18, at 51.

71. *Id.* at 52.

72. *Id.*

73. *Id.*

The *Interpretive Guidance* states that scientific research and design do not amount to direct participation.[74] Rather, they qualify as "indirect participation."[75] In selling and even designing the cyber tool, the dealer is participating in activities that are more akin to the general war effort and war sustaining activities than to the conduct of hostilities. Just as civilians who design and manufacture weapons and military equipment used by NATO Forces fail to satisfy the direct causation requirement, a cyber arms dealer who designs and manufactures a cyber tool and sells it to Al-Qaeda would likely fail to satisfy the direct causation requirement even if the dealer knew the weapon's general capacity.[76]

The *Interpretive Guidance* provides several examples on two ends of a spectrum to elucidate the direct participation requirement.[77] The *Interpretive Guidance* explains that a civilian truck driver transporting ammunition to an "active firing position" would satisfy the direct causation requirement.[78] However, a civilian truck driver who transports ammunition "from a factory to a port for further shipping to a storehouse in a conflict zone . . . is too remote from the use of ammunition in specific military operations to cause the ensuing harm directly."[79] These examples demonstrate the importance of the purpose of the action. If the ultimate purpose of the action is to directly cause harm, then it comes closer to satisfying the direct causation requirement. While the *Interpretive Guidance* asserts that geographic proximity is less important than causal proximity,[80] these examples show how geographic proximity can be a factor in determining whether a civilian's action *can* directly cause the required measure of harm.

This requirement, though, becomes difficult to define in the cyber context. Whether or not the manufacture and sale of a cyber tool satisfies the direct causation requirement likely depends on how the tool is employed. For example, if a cyber tool is located on a thumb drive

74. *Id.* at 53.

75. *Id.*

76. The exception to this general rule is implicated when the cyber tool is designed for an "integral part in a specific military operation designed to directly cause the required threshold of harm." *Id.* This is true for many activities related to hostilities; this analysis will be discussed in greater depth during the section of this paper that discusses training. It is also a point to which the *Tallinn Manual* agrees. In short, for the dealer to satisfy this exception, his manufacture and sale of the cyber tool would have to be an integral part of a specific, Al-Qaeda military operation.

77. *See* Melzer, *supra* note 18, at 53-54.

78. *Id.* at 56.

79. *Id.*

80. *See id.* at 55.

that must be placed into a computer before the tool can be employed, then the manufacture and sale of the tool probably would not satisfy the direct causation requirement. However, if the tool could be employed from any computer with a connection to the Internet, then it is more likely that the manufacture and sale of the tool would satisfy the direct causation requirement. The more intermediate steps between the manufacture and sale of the tool, the more tenuous the causal link becomes between the manufacture-sale of the tool and the harm resulting from its employment. If the cyber tool requires a closer geographic proximity to be employed, the causal connection becomes more tenuous, as the tool is moved from the seller (the factory) through a series of locations (the storehouse) to the conflict zone. However, if the tool can be employed immediately upon its purchase from the cyber dealer, then the sale could be akin to transporting ammunition to an active firing position and thus allow the dealer's sale to satisfy the direct causation requirement.

Assuming that both the first and second requirements are met, the third factor to be satisfied is the belligerent nexus requirement. In order for a civilian's action to satisfy this requirement, the "act must be specifically designed to cause the required threshold of harm in support of a party to the conflict and to the detriment of another."[81] The *Interpretive Guidance* admits that "[n]ot every act that directly adversely affects the military operations and military capacity of a party to an armed conflict . . . necessarily amounts to direct participation in hostilities."[82] This requirement focuses on the objective purpose of the act, not the subjective intent of the civilian actor.[83] So, if the purpose of an action is to cause harm to one party to the conflict—regardless of the underlying reason for doing so—that action will satisfy the belligerent nexus requirement.

Whether or not the act of selling and manufacturing a cyber tool satisfies the belligerent nexus requirement turns on the civilian's actions in relation to the tool. If the dealer manufactures a tool with a multitude of capabilities that includes the ability to disrupt drone communications and functionality, the dealer probably would not satisfy the belligerent nexus requirement. However, if the dealer knew the buyer was interested in only those two capabilities in addition to the buyer's ability to employ the tool during a present engagement in armed conflict with the United States, the dealer should probably

81. *Id.* at 58.
82. *Id.*
83. *Id.* at 59.

know that the objective purpose of the act would be to employ it in such a way. The belligerent nexus becomes easier to demonstrate if the tool's sole capabilities disable drone communications and functionality regardless of the dealer's personal intent.

The *Tallinn Manual* uses the same three factors identified by the *Interpretive Guidance* in determining whether or not a civilian's action qualifies as direct participation in hostilities, rendering that civilian a targetable candidate.[84] However, the *Tallinn Manual* takes a more expansive view on when the dealer is targetable under a DPH model. Most importantly, the *Tallinn Manual* states that "*any* action that makes possible specific attacks" would qualify as direct participation in hostilities.[85] This distinction between actions that are intended for specific missions and actions intended to support the general war effort is similar to that made by the *Interpretive Guidance.* However, the *Tallinn Manual* states that *any* action that makes a specific attack possible renders the civilian targetable, rather than any action that is "integral" to a specific attack.[86] This is a distinction with broad implications. The types of actions that make a specific attack possible are much more inclusive than actions integral to a specific attack.

The *Tallinn Manual* provides several "unambiguous" examples of civilian actions that may make a specific attack possible.[87] They include identifying vulnerabilities in a targeted system, creating a cyber tool to take advantage of particular vulnerabilities, collecting information on enemy operations by cyber means and passing it to one's own armed forces, and conducting DDoS operations against enemy military systems.[88] The *Tallinn Manual* also provides several examples that would not make a specific attack possible.[89] The act of "designing malware and making it openly available online, even if it may be used by someone involved in the conflict to conduct an attack, does not constitute direct participation," according to the Tallinn Experts.[90]

The middle ground between these two sets of examples caused some of the Tallinn Experts to hesitate when it came to defining the direct causation requirement.[91] They were conflicted on how this requirement would play out "when malware is developed and provided

84. TALLINN MANUAL, *supra* note 18, at 119.
85. *Id.* at 120 (emphasis added).
86. *Id.*
87. *Id.*
88. *Id.*
89. *See id.*
90. *Id.*
91. *Id.*

to individuals in circumstances where it is clear that it will be used to conduct attacks, but where the precise intended target is unknown to the supplier."[92] In essence, while the dealer understands how the tool will be used, he or she may not be aware as to whom the tool will be used against. Some of the experts doubted the causal connection between the act of providing malware and the subsequent attack would, in such a situation, be sufficiently direct to qualify as direct participation.[93]

In summary, for the Tallinn Experts, designing a tool to take advantage of particular vulnerabilities qualifies as direct participation in hostilities.[94] Making a tool openly available online does not qualify as direct participation in hostilities.[95] Making a tool that is clearly for cyber attacks but where the intended target is unknown *may* not qualify as direct participation in hostilities.[96] The difference between the first and third examples seems to be that the first example deals with a cyber tool created for a specific target, whereas in the third example, the cyber tool is created with a known capability but without knowledge of specific targets. The main point here is that the more specific a target for which a tool is designed, the more concrete the causal connection for the *Tallinn Manual*, and the more likely that the direct causation element will be satisfied.

This is similar to the *Interpretive Guidance's* example of transporting ammunition.[97] The transportation of ammunition in and of itself is a benign act—while a bullet has the ability to cause death and damage, merely transporting that ammunition is not a causal step in bringing about any eventual death or damage. Rather, it is an action that supports the general war effort.[98] But the transportation of ammunition to an active firing position implies that targets have already been identified, so the transportation of the ammunition constitutes a crucial step in causing further death or damage in that specific, ongoing attack.[99]

In Variation 1, Al-Qaeda asks the dealer to design a specific tool with the capability to take advantage of particular vulnerabilities. The target has already been specifically identified, so Variation 1 fits

92. *Id.*
93. *Id.*
94. *See id.*
95. *See id.*
96. *Id.*
97. MELZER, *supra* note 18, at 56.
98. *See id.*
99. *See id.*

squarely within the *Tallinn Manual's* example. Here, the dealer also knows that the tool will be used to target specific vulnerabilities. Specifically, the dealer is creating the tool to take advantage of vulnerabilities unique to a drone's operating and communications system. Because the dealer is creating the tool with the specific purpose of taking advantage of these particular vulnerabilities at the request of a specific party to a conflict, this action would fulfill the direct causation requirement under the *Tallinn Manual.* If the dealer is uncertain as to what harm is intended or against which targets the tool will be applied, and if the dealer does not specifically intend to cause any harm, then the sale of the tool may not satisfy the direct causation requirement.

If, however, the purpose of the tool was changed, and the tool was created only to discover vulnerabilities in the drone operating and communications system so that a different cyber tool could be created to take advantage of those vulnerabilities, the dealer would likely satisfy the direct causation requirement. The *Tallinn Manual* states that one unambiguous example of an act that qualifies as direct participation occurs when a civilian "gather[s] information on enemy operations by cyber means."[100] While the *Tallinn Manual* limits the unambiguity of this example to the gathering of information on enemy operations, the *Interpretive Guidance* describes this qualifying act as the "gathering of intelligence" but only when the act is "carried out with a view to the execution of a specific hostile act,"[101] or if the information is "tactical targeting information for an attack."[102] The *Interpretive Guidance* elucidates the meaning of "tactical targeting information for an attack" with the example of a civilian woman who repeatedly peeked into a building where troops had taken cover in order to indicate their position to the attacking enemy forces.[103] The *Interpretive Guidance* clarified that the "decisive criterion for the qualification of her conduct as direct participation in hostilities was held to be the importance of the transmitted information for the direct causation of harm and, thus, for the execution of a concrete military operation."[104] The key for the *Interpretive Guidance's* analysis is how important the information passed by the civilian was to the direct causation of the requisite harm.

100. TALLINN MANUAL, *supra* note 18, at 119.

101. MELZER, *supra* note 18, at 66.

102. *Id.* at 48.

103. *Id.* at 48 n.103.

104. *Id.*

While the Tallinn Experts were concerned about a direct causal link, the creation of an unsolicited cyber tool and subsequent sale of such a tool may also fail the belligerent nexus requirement. The *Tallinn Manual's* conception of the belligerent nexus is that a civilian's actions must "be directly related to the hostilities."[105] According to the *Tallinn Manual*, this "rules out acts of a purely criminal or private nature that occur during an armed conflict."[106] If the tool was a special request from a customer who was a party to a conflict (as is the case in this variation), the belligerent nexus requirement is satisfied because of the harm to one party at the request of another party. If the dealer designed and sold the tool merely for private, pecuniary gain but the tool made its way into Al-Qaeda's hands, the dealer would not have satisfied this requirement. It is harder to determine if the dealer was acting solely for personal, pecuniary gain if the tool is openly available and sold to multiple customers without regard to whether or not the customers were involved in an armed conflict. Then the belligerent nexus becomes strained, and it becomes less likely that the dealer can be targeted. If the dealer sought out Al-Qaeda or designed the tool with Al-Qaeda in mind, and sold it to other groups to make extra money, the belligerent nexus would probably be satisfied. In this variation, because the dealer knows that he is preparing a tool for Al-Qaeda with the capability of disabling drones' important functions, the design and sale of the tool are directly related to hostilities even if the dealer is profiting from the transaction.

In the practical application of this analysis, the dealer is likely targetable under the *Tallinn Manual* but not under the *Interpretive Guidance* unless the tool was designed and sold with a specific operation in mind. The victim party is likely to impute the requisite intent to the dealer for each requirement and thus come to a determination that for such time as the dealer was directly participating in hostilities, the dealer was targetable. While it would be more difficult to determine that the design and sale of the tool would satisfy the *Interpretive Guidance's* objective likelihood test, the dealer would be targetable under both perspectives if the tool was developed with a specific military operation in mind.

105. TALLINN MANUAL, *supra* note 18, at 119.
106. *Id.* at 120.

B. *Variation 2: The Cyber Arms Dealer Trains Al-Qaeda Members to Employ the Cyber Tool*

In this variation, Al-Qaeda requests the dealer to train some of its members on how to employ the cyber tool. The dealer knows the customers are from Al-Qaeda and that they generally want to employ the tool against drones.

The *Interpretive Guidance* states that while individuals may "continually accompany or support an organized armed group," they will not assume a continuous combat function as long as their "function [with the group] does not involve direct participation in hostilities."[107] Rather, "they remain civilians assuming support functions. . . . Thus, recruiters, trainers, financiers, and propogandists may continuously contribute to the war effort of a party" to a conflict and do not become targetable "unless their function additionally includes activities amounting to direct participation in hostilities."[108] The *Interpretive Guidance* notes that while these individuals may render significant aid to a party to a conflict, that aid does not necessarily result in the civilian assuming a continuous combat function.[109] Continued targetability may not necessarily be established based solely upon a spontaneous, sporadic, or temporary role for the duration of a particular operation.[110]

According to the *Interpretive Guidance*, the presence alone of the dealer with the party to a conflict does not, in and of itself, render the dealer targetable.[111] The dealer may train the Al-Qaeda operatives but will not be targetable unless the dealer also assumes a continuous combat function. If the dealer's training is accomplished through a single meeting and is not ongoing, it is highly unlikely that the dealer would be targetable under the *Interpretive Guidance* because the dealer would not assume a continuous combat function by training only once. Furthermore, in this variation the dealer is not assuming a combat function but rather a training function that is limited to the support of an organized armed group. Even if the dealer trained members of the group multiple times, as long as the dealer's activity was limited to training, the dealer would not assume a combat function.

The dealer may be targetable under the three-pronged analysis for sporadic, direct participation if the dealer is training the Al-Qaeda

107. MELZER, *supra* note 18, at 35.
108. *Id.* at 34.
109. *See id.* at 35.
110. *Id.*
111. *See id.*

operatives for a specific mission.[112] For the *Interpretive Guidance* this question hinges on the direct causation requirement because the dealer is only training members of one party to the conflict and that training is directly resulting in military harm.[113] This action also satisfies the other two prongs of the DPH analysis. If the dealer was only engaged in general training, the dealer would not be targetable under the *Interpretive Guidance* because there would not be a sufficient causal link between the training and the resulting harm to satisfy the direct causation requirement.[114] The *Interpretive Guidance* states that "although the recruitment and training of personnel is crucial to the military capacity of a party to the conflict, the causal link with the harm inflicted on the adversary will generally remain indirect."[115]

However, similar to the specific-mission analysis in Variation 1 where a cyber tool was designed and sold for an integral part in a specific mission, if the dealer was training Al-Qaeda members for a specific mission, he would satisfy the direct causation prong. In this variation, regardless of whether or not the cyber tool was designed and sold in order to play an integral part in a specific operation, if the dealer provides "instruction and assistance . . . to troops for the execution of a specific military operation," the dealer would be targetable.[116] Training qualifies as direct participation in hostilities "[o]nly where persons are specifically recruited and trained for the execution of a predetermined hostile act."[117] This would likely occur where the dealer walks the Al-Qaeda operatives through a planned, specific mission and instructs the operatives on when and how to employ the cyber tool. Assuming the threshold of harm and belligerent nexus requirements are met, if the dealer trains Al-Qaeda operatives on the employment of the cyber tool for a specific military operation, under the *Interpretive Guidance* the dealer would be targetable for the length of time that the dealer provided such training.

While the *Tallinn Manual* does not directly address the subject of training, the three-pronged DPH analysis employed by the *Tallinn Manual* still applies. Specifically, the *Tallinn Manual's* characterization of the direct causation prong is implicated. As with the design and sale of a cyber tool from Variation 1, the only time a dealer would be

112. *See id.* at 54-55..
113. *See id.* at 53.
114. *See id.*
115. *Id.*
116. *Id.* at 54-55.
117. *Id.* at 53.

targetable is if the training "makes possible specific attacks."[118] Training Al-Qaeda members on how to employ the cyber tool certainly makes specific attacks possible, especially if the training is not merely helpful but necessary to the employment of the tool. The question remains as to whether this means any training on employing the tool satisfies the direct causation requirement.

The direct causation requirement is satisfied when there is a direct causal link between the civilian's action and the harm intended or inflicted.[119] In this variation, there must be a direct causal link between the training and the eventual harm that is a result of the training. The harm is more likely to be a direct cause of the training if the training was for a specific mission. If the training is conducted to allow the Al-Qaeda members to "take advantage of particular vulnerabilities" regardless of whether a specific mission has been organized, this would qualify as an action that made possible a specific attack. Thus, it would qualify as an act of direct participation in hostilities.[120] Even if the dealer is unaware of when the specific mission will occur, if the dealer is training people to take advantage of particular vulnerabilities on a specific platform, the intended harm is clear and is made possible because of the dealer's training. In this situation, the dealer is training the Al-Qaeda members on how to take advantage of particular vulnerabilities of a drone's communication system and functionality. This renders the dealer targetable not only in situations where there is a specific mission in mind, but in *all* training situations for this tool.

For the *Tallinn Manual*, the direct causation requirement hinges on *either* the intended or actually inflicted harm resulting from the civilian's act.[121] Under this regime, the victim state does not have to wait until the actual harm occurs, so long as the civilian's act is accompanied by the intention of causing the requisite harm.[122] Once the dealer trains the Al-Qaeda members on how to take advantage of particular vulnerabilities on a specific platform, it is clear what harm is intended by the dealer. At this point, the dealer is likely targetable.

However, if the dealer is training the Al-Qaeda members on how to deploy a tool that takes advantage of generalized vulnerabilities, it is less likely the dealer would be targetable during or after the training. Similarly, if the dealer provides general training on creating

118. TALLINN MANUAL, *supra* note 18, at 120.

119. *Id.* at 119.

120. *Id.* at 120.

121. *See id.* at 119.

122. *See id.*

malware or using a computer, then the dealer would not be targetable. This is because the training is not making a specific mission possible but rather it is making possible many different missions. This is tantamount to training an individual on how to use a machine gun or a radio. While the training makes it more likely the necessary harm will result, the training itself is not designed to bring about necessary harm in one causal step. Whereas the dealer's participation in providing training on particular vulnerabilities is crucial in bringing to pass a specific mission, in providing training on how to implement a basic tool that takes advantage of general vulnerabilities the dealer's causation of the eventual harm becomes more diffuse. Therefore, in situations where the dealer provides training on how to take advantage of general vulnerabilities, the dealer would likely not be targetable.

C. *Variation 3: Al Qaeda Asks the Dealer to Supervise Employment of the Cyber Tool*

Where in the previous variation the dealer provided training on how to implement the tool, this variation has the dealer supervising the employment of the cyber tool. Here, different levels of supervision must be analyzed. Nevertheless, in all levels of supervision the dealer does not actively participate in the mission other than to provide supervision of employing the tool. While neither the *Interpretive Guidance* nor the *Tallinn Manual* directly addresses supervision, principles can be drawn from each to determine when either document would render the dealer targetable. This variation explores the type of participation required to render the dealer targetable in a collective operation.

The *Interpretive Guidance* addresses supervision in a general manner through an example—the execution of a drone strike.[123] This example also outlines targetability requirements for a collective operation.[124] The *Interpretive Guidance* observes that a successful drone strike requires a number of people working together.[125] The example demonstrates that not everyone who participates in a collective operation is necessarily targetable by virtue of their participation in such a collective operation.[126]

Multiple individuals are involved in the *Interpretive Guidance's* example, including "computer specialists operating the vehicle

123. *See* Melzer, *supra* note 18, at 54.
124. *See id.*
125. *See id.*
126. *See id.*

through remote control, individuals illuminating the target, aircraft crews collecting data, specialists controlling the firing of missiles, radio operators transmitting orders, and an overall commander."[127] For the *Interpretive Guidance*, direct causation is the key to targetability in a collective operation. In collective operations such as the drone strike above, the *Interpretive Guidance* recognizes that "all of these persons are integral to that operation and *directly participate* in hostilities."[128] However, it argues that "only few of them carry out activities that, in isolation, could be said to directly cause the required threshold of harm."[129] It does not explain which individuals from the example would satisfy the direct causation requirement. Rather, it explains that if an individual's act in isolation does not meet the direct causation threshold, that for the direct causation requirement to be satisfied in a collective operation an act must constitute an "integral part of a concrete and coordinated tactical operation that directly causes" the necessary level of harm.[130] Based on this, the *Interpretive Guidance's* targetability analysis for civilians in a collective operation has two factors. First, the participation must be integral to the operation. Second, the operation must be concrete, coordinated, *and* a tactical operation.

In this variation, whether or not the dealer is targetable under the *Interpretive Guidance* regime depends on how integral of a role the dealer plays in the operation. Further, in this variation the employment of a tool that disables drone communications is a concrete, coordinated, and tactical operation regardless of whether it is directed at all drones or drones within a specific geographic area. The question is whether the dealer's supervision constitutes an integral part of that operation. If the Al-Qaeda operatives employing the tool have the requisite training and expertise to employ it, and if the dealer is acting only to confirm that the tool is being employed effectively, the dealer's actions would not be considered integral. Thus, it is unlikely that under the *Interpretive Guidance* the dealer could be targeted. On the other hand, if the dealer's supervision is necessary to effectively employ the tool, the dealer's technical supervision would be integral to the operation, rendering the dealer targetable for such time as the dealer is supervising.

Similar to the *Interpretive Guidance*, the *Tallinn Manual* does not specifically discuss supervision. Rather, it provides the same general

127. *Id.*

128. *Id.* (emphasis added).

129. *Id.*

130. *Id.* at 54-55.

rule that "any actions that make possible specific attacks" qualify "as an act of direct participation."[131] This rule leaves room for certain levels of supervision that would and would not make the dealer targetable—in some circumstances the dealer's supervision would not be making a specific attack possible. If the dealer's supervision is necessary to effectuate the cyber tool's effective employment, the dealer would be targetable. However, if the dealer's participation amounted only to confirming the tool was effectively employed and was not necessary to the tool's employment, it is more likely that this level of supervision would not make possible a specific attack. While the supervision would no doubt be helpful to the tool's employment, it would not rise to the level of making possible the specific attack. Because of this, the dealer's detached supervision would not satisfy the direct causation requirement. Thus, in this case it is unlikely the dealer would be targetable.

D. Variation 4: Al Qaeda Hires a Cyber Arms Dealer to Employ the Tool

In this variation the dealer is hired by Al-Qaeda to employ the tool against coalition forces. This variation explores what actions are necessary for the dealer to assume a continuous combat function. It also examines the starting and stopping points of the dealer's participation.

The issue in this scenario is whether or not the dealer has assumed a continuous combat function or is directly participating in hostilities for a limited period of time by employing the tool, or if the dealer is merely performing an action that amounts to neither one. As previously discussed, the tool is designed to meet the required threshold of harm for the DPH analysis, so employing the tool rules out the third option. Furthermore, employing it against the United States in this scenario would satisfy the other two requirements. The difference here from previous variations is the combat function. While the dealer may have assumed a training function or a supervisory role in previous variations, in this variation the dealer assumes a combat function. Another key issue for this variation is whether the dealer is targetable for the entire time the tool is in effect or only for the duration of the actual employment of the tool. This turns on whether or not the

131. *See* TALLINN MANUAL, *supra* note 18, at 120. The goal of the *Tallinn Manual* is to provide general rules; it was not created to address every variation.

dealer has assumed a continuous combat function for Al-Qaeda's organized armed group.[132]

The *Interpretive Guidance* defines a continuous combat function as "a continuous function assumed by an individual" that amounts to the "conduct of hostilities on behalf of a non-state party to the conflict."[133] If the dealer has assumed a continuous combat function for an organized armed group, the dealer is considered a member of that group and becomes targetable for as long as the dealer retains that function.[134] If the dealer has not assumed a continuous combat function but is only directly participating in hostilities on a sporadic basis, the dealer is only targetable for such time as the dealer directly participates in hostilities.[135] One way the *Interpretive Guidance* describes the assumption of a continuous combat function is when "[a]n individual [is] recruited, trained and equipped by such a group to continuously and directly participate in hostilities on its behalf," so that individual can be considered to assume a continuous combat function even before he or she first carries out a hostile act.[136] That is, an individual becomes targetable even before executing any hostile act by assuming a continuous combat function; the individual is targetable for as long as he or she assumes a continuous combat function for an organized armed group belonging to a non-State party.[137] If the dealer was hired to carry out only one attack, the nature of the dealer's involvement in that attack would need to be examined to determine if she has assumed a continuous combat function. In any case, once the dealer has been recruited (or hired) to continuously carry out multiple attacks for Al-Qaeda, the dealer would assume a continuous combat function and would be targetable continuously.

On the other hand, if the dealer is hired to participate only sporadically in hostilities and does not assume a continuous combat function, the dealer is not generally targetable.[138] Rather, the dealer would be targetable only for such time as he or she is directly participating.[139] If the dealer was hired to carry out one short attack that required little more than the press of a button, the dealer could not be said to have assumed a continuous combat function. The dealer would

132. *See* Melzer, *supra* note 18, at 38-40.
133. *Id.* at 33.
134. *See id.* at 39.
135. *See id.* at 71-72.
136. *Id.* at 34.
137. *Id.* at 39.
138. *See id.* at 71-72.
139. *See id.*

be targetable only for the duration of the direct participation. Questions of course arise over the space in time between either end of the spectrum.

The Tallinn Experts agreed that an individual who assumes a continuous combat function is generally targetable.[140] They were, however, divided on when an individual would assume that function in different scenarios.[141] Some experts asserted that the assumption of a continuous combat function was not necessary at all but that membership in an organized armed group was sufficient to render the individual targetable.[142] The experts did agree that an individual would become targetable after joining the military wing of an organized armed group.[143]

In this variation, the dealer has been hired to employ the tool. Employment of the tool clearly causes the requisite harm to the detriment of one party to the conflict. If Al-Qaeda hires the dealer on a long-term basis to carry out attacks over the course of the dealer's employment, the dealer would have assumed a continuous combat function and would generally be targetable. If, however, the dealer is hired only to employ the device, the dealer would be targetable only during this brief employment.

This variation also raises questions about the starting and stopping points of participation if the dealer has not assumed a continuous combat function. The variation where the dealer does not assume a continuous combat function, but only sporadically participates in hostilities, highlights the need to know the duration for which the dealer may be targeted. If the dealer is hired to employ the tool only once, the question arises as to when the victim of the dealer's attack may start to target the dealer and when the victim is legally obligated to cease targeting. This question is particularly tied to this variation because it is the dealer carrying out the attack. Some of the foregoing variations focused on specific acts that were preparatory to execute the tool. This variation is different—here the actor carrying out the actual attack is the dealer.

The *Interpretive Guidance* states that the "concept of direct participation in hostilities . . . include[s] measures preparatory to the execution of such an act, as well as the deployment to and return from the location of its execution, where they constitute an integral part of such

140. *See* TALLINN MANUAL, *supra* note 18, at 116.
141. *Id.*
142. *See id.*
143. *Id.*

a specific act or operation."[144] The key for the *Interpretive Guidance* is whether a preparatory action or transit to and from the location where the qualifying act takes place constitutes an integral part of the qualifying action. The *Interpretive Guidance* lists preparatory actions that may qualify, including actions "carried out with a view to the execution of a specific hostile act."[145] These actions are listed as "equipment, instruction, and transport of personnel; gathering of intelligence; and preparation, transport, and positioning of weapons and equipment"; "loading of bombs onto an airplane for a direct attack on military objectives in an area of hostilities"; and deployment if it constitutes "an integral part of the act in question."[146] Participation ends when the individual has "physically separated from the operation."[147]

The *Interpretive Guidance* notes that in cases such as "computer network attacks or remote-controlled weapons systems," where a hostile act does not necessarily "require geographic displacement . . . the duration of direct participation in hostilities will be restricted to the immediate execution of the act and preparatory measures forming an integral part of that act."[148] The *Interpretive Guidance* expressly excludes transit to and from the place where a civilian directly participates in hostilities through cyberspace. It is unclear why it asserts that transit to and from the location of the computer used to launch a computer network attack would not qualify as an integral act even though the dealer would be traveling with a view to the execution of a specific hostile act. While it may be impractical to target a civilian located outside of a conflict zone,[149] the fact that a civilian is targetable only after walking down the street to an internet cafe in Kandahar to launch a cyber attack against drones based in Kabul should be no different than a civilian who walks down the street in Kabul to plant an IED along a transit route.

144. MELZER, *supra* note 18, at 65.

145. *Id.* at 66.

146. *Id.* at 66-67.

147. *Id.* at 67.

148. *Id.* at 68.

149. There are other questions that this analysis inherently raises, including the question of sovereignty and consent. If a target civilian is located in a state that is not victim to the crime but the location of the attack, the victim state must obtain consent from the other state to comply with international law. *See* U.N. Charter art. 2, para.4 (noting the requisite principle of territorial sovereignty); Ashley Deeks, *The Geography of Cyber Conflict: Through a Glass Darkly*, 89 INT'L L. STUD. 1, 10 (2013) ("In the ideal situation, a victim State will approach the territorial State and inform the latter of the fact of the imminent or actual armed attack and its reasons for believing that the attacker is employing the victim State's infrastructure to commit the attacks.").

Under the *Tallinn Manual*, a dealer in this variation would be targetable in more situations than he or she is under the *Interpretive Guidance*. The Tallinn Experts agreed that a civilian is targetable during "actions immediately preceding or subsequent to the qualifying act" as long as the preparatory or subsequent actions are undertaken while the civilian is "engaged in the qualifying act of direct participation in hostilities."[150] The *Tallinn Manual* expands the scope of targetability in preparatory and subsequent actions to include any action where the civilian is still *engaged* in the qualifying act, not just where the preparatory or subsequent actions are *integral* to the qualifying act. For example, a civilian is targetable while traveling "to and from the location where a computer used to mount the operation in question is based."[151] Unlike the *Interpretive Guidance* analysis, the *Tallinn Manual* renders targetable a civilian traveling to and from the place where the computer used to launch an attack is located.

Differences in a civilian's targetability also depend on which DPH regime a victim state employs. If the dealer is a member of a Russian organized crime group, and if the tool may only be employed in Afghanistan, the dealer would be targetable en route from Russia to Afghanistan. Furthermore, if the dealer needed to procure any equipment in order to employ the tool, the dealer would be targetable during that time. It becomes more difficult to determine targetability if, on the way to Afghanistan, the dealer travels to Uzbekistan for nothing more than to visit family. Under the *Interpretive Guidance*, it is clear that the dealer would not be targetable while with family because the family visit is not integral to his qualifying act. However, depending on how long the dealer stayed with family, the dealer may remain targetable under the *Tallinn Manual*. Similarly, if the dealer did not have a home computer but worked out of an office, the dealer would be targetable under the *Tallinn Manual* while walking or driving to the office, as well as during the time the dealer was en route to return home after the attack's execution.

E. Variation 5: Al-Qaeda Hires Cyber Arms Dealers to Watch and Maintain the Tool Until They Are Ready to Deliver the Payload

This variation is the same as the previous variation but with the important distinction that the tool is not effective immediately upon employment. Here, the tool's effects are delayed until a point in the

150. TALLINN MANUAL, *supra* note 18, at 120.
151. *Id.*

future instead of assuming harm realization at the moment the tool is employed. A close geographic proximity is now unnecessary to the tool's employment. Because the main payload will not be delivered until a point in the future, this variation focuses on the delayed effects of the tool. The eventual effect is the same: Employment of the tool results in a disruption of the drones' communications and functionality. However, once the tool has been placed, it may be triggered by some future condition occurring on the platform in which the tool has been installed, often referred to as a logic bomb, or by the dealer herself. The dealer monitors the tool from outside the immediate zone of conflict until the necessary conditions are achieved on the platform or until asked to deliver the payload.

In addressing weapons systems with delayed effects, the *Interpretive Guidance* states that the "causal relationship between the employment of such means and the ensuing harm remains direct regardless of temporal or geographical proximity."[152] The direct causation requirement focuses on the causal proximity, not the temporal or geographical proximity.[153] The *Interpretive Guidance* lists mines, booby-traps, timer-controlled devices, remote-controlled (i.e. geographically remote) missiles, and unmanned aircraft and computer network attacks as examples of weapons systems that have a delayed effect but still satisfy the direct causation requirement.[154] Furthermore, asserting that the causal relationship remains direct regardless of temporal proximity suggests that the civilian is targetable for such time as the civilian participates even though the harm may be realized at some point in the future.[155] Importantly, the *Interpretive Guidance* notes that "where the required harm has not yet materialized, the element of direct causation must be determined by reference to the harm that can reasonably be expected to directly result from a concrete act or operation ('likely' harm)."[156]

If the tool satisfies the threshold of harm and belligerent nexus requirements, the dealer's act of emplacing the tool would satisfy the *Interpretive Guidance's* DPH analysis. As long as the necessary threshold of harm can reasonably be expected to directly result from the tool's emplacement, the dealer is targetable for such time as she directly participates. According to the *Interpretive Guidance*, this

152. MELZER, *supra* note 18, at 55.
153. *Id.*
154. *Id.*
155. *See id.* at 47, 55.
156. *Id.* at 55.

seems to be true even if the direct participation takes place far from the actual conflict.[157] It also suggests that even though harm may be realized at a future date—as could be the case with the emplacement of a logic bomb—the dealer would only be targetable for the period of time he or she was emplacing the logic bomb. If the logic bomb did not require any additional maintenance, the time at which the dealer could be targeted would cease after the logic bomb was emplaced.

The *Tallinn Manual* generally agrees with the foregoing conclusions. In discussions for the manual, a majority of the Tallinn Experts "took the position that the duration of an individual's direct participation extends from the beginning of his involvement in mission planning and ends when he or she terminates an active role in the operation."[158] If one individual, for example, only emplaces the tool and another individual activates it at a later point in time, each would only be targetable for the period at which they participated even though the individual emplacing the tool would directly participate before the harm ever occurred.[159] Similarly, if an individual emplaced a tool and the harm occurred later without any further prompting, the individual would only be targetable for the time during which he emplaced the tool.[160] However, if a single dealer both emplaced and subsequently employed the tool, a majority of the Tallinn Experts agree the dealer would be targetable from the time of emplacement to the time of employment.[161] Only a minority of the experts asserted that each act would qualify as a separate period of direct participation if carried out at different times by the same person.[162] The *Tallinn Manual* acknowledges the difficulties that arise with conflict classification and geographic proximity of actors to the conflict;[163] however, it also recognizes that individuals directly participating in hostilities from a location distant from the conflict would likely be targetable.[164]

157. *See id.* Again, there is debate revolving around targetability outside of a "hot" conflict zone. Section IX of the Interpretive Guidance also discusses alternatives to targeting. *See id.*at 77-82. The purpose of this paper is to discuss when targeting is lawful. The author recognizes that targeting is often not the only option available to armed forces. For an argument restricting targeting to a "hot" conflict zone, see Jennifer Daskal, *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the "Hot" Conflict Zone*, 161 U. PA. L. REV. 1165 (2013).

158. TALLINN MANUAL, *supra* note 18, at 121.

159. *See id.*

160. *See id.*

161. *See id.*

162. *Id.*

163. *See id.* at 78.

164. *See id.* at 86.

If the dealer's action does not satisfy the direct causation or the necessary harm requirement, the dealer may not be targeted. The *Tallinn Manual* asserts that only maintaining computer equipment generally, even if such equipment is subsequently used in the hostilities, is an example of a civilian action that would not satisfy the DPH requirements.[165] Clearly, the dealer must do more than simply maintain the computer equipment. This presents a difficult question for determining when the dealer in this variation would be targetable. While there is no question the dealer is targetable while emplacing the tool and delivering the tool's payload, the nature of maintaining the tool must dictate whether or not the dealer is also targetable while maintaining it. Monitoring the tool in preparation for the delivery of the payload seems to be more than a general maintenance of computer equipment. Therefore, when the dealer initially emplaces the tool and then maintains it in anticipation of delivering the payload until given the order to deliver, the dealer will satisfy the direct participation requirements from the moment the tool is emplaced, while the dealer monitors the tool, and until the dealer delivers the payload.

F. Variation 6: The Dealer Has No Affiliation with Al-Qaeda and Makes the Same Tool Publicly Available.

In this variation, rather than being approached by Al-Qaeda to develop a cyber tool, the dealer independently develops the tool and makes it available online to the general public. This variation is different from the first in that the dealer is operating without any direct interaction with Al-Qaeda. Without the dealer's knowledge, the tool is then discovered and employed by individuals and groups including Al-Qaeda. This variation explores the ramifications of making the tool available in a situation where the dealer does not have any concrete affiliation with an organization that is engaged in an armed conflict. It will explore the targeting consequences of knowing the tool's capabilities but not knowing the client. In short, this variation will examine whether a dealer is targetable solely for making a weapon, and if not, what more is required.

The *Interpretive Guidance* addresses the targeting of weapons makers who are affiliated with a party to a conflict.[166] It asserts that if direct participation renders someone targetable, indirect participation may still be participation in a conflict, but such participation does not

165. *Id.* at 120.

166. *See* MELZER, *supra* note 18, at 51-54.

render an individual targetable.[167] For the *Interpretive Guidance* this is because the causal connection between the weapon production and the resulting harm is too attenuated. Participation that renders a civilian targetable must have a "sufficiently close causal relation between the act and the resulting harm."[168] In the weapons maker's case, the purpose of his activity may be to support the general war effort or engage in war-sustaining activities rather than bring about the actual harm suffered by a party, but this is not clear.[169] For the *Interpretive Guidance*, the difference is that "unlike the conduct of hostilities, which is designed to cause—i.e. bring about the materialization of—the required harm, the general war effort and war sustaining activities also include activities that merely maintain or build up the capacity to cause such harm."[170]

The *Interpretive Guidance* provides examples of indirect participation, including "scientific research and design, as well as *production* and transport of weapons and equipment unless carried out as an integral part of a specific military operation designed to directly cause the required threshold of harm."[171] It uses the assembly and storing of an Improvised Explosive Device (IED), or the purchase and smuggling of its components as an example of participation that does not render an individual targetable because those actions do not cause the harm directly.[172] However, the "planting and detonation of that device" would render the civilian targetable.[173]

An admittedly imperfect approximation of the analysis provided by the *Interpretive Guidance* above would be a civilian located inside or outside of the combat zone making IEDs, leaving them outside his home with a sign that says, "IEDs for sale!" or "Free IEDs." According to the *Interpretive Guidance*, absent a specific military operation, this would probably not render the IED maker targetable because the weapon's production would not directly cause the requisite harm.[174] Rather, for the *Interpretive Guidance*, the planting and detonating of IEDs are acts that would render the civilian targetable because of the direct causal connection between the act of detonating the IED and

167. *Id.* at 51.

168. *Id.* at 52.

169. *See id.* at 51-52.

170. *Id.* at 52.

171. *Id.* at 53 (emphasis added).

172. *Id.* at 54.

173. *Id.*

174. *See id.*

the resulting harm.[175] If an individual made and sold IEDs outside the conflict zone, that individual would clearly be subject to the local laws of the state where that individual was located. However, the individual would not be targetable because the action of making and selling the IEDs would lack both direct causation of any harm to one of the parties and a belligerent nexus to the conflict. Even within the conflict zone, the *Interpretive Guidance* suggests the IED maker would not be targetable.

While the cyber arms dealer may be supporting the general war effort by making the tool available, the tool's availability is not considered directly participating in the hostilities. This is because, for the *Interpretive Guidance*, the direct causation element is too attenuated.

Similarly, the *Tallinn Manual* asserts that "conducting cyber attacks related to an armed conflict qualifies as an act of direct participation, as do any actions that make possible specific attacks."[176] These actions include "identifying vulnerabilities in a targeted system or designing malware in order to take advantage of particular vulnerabilities."[177] However, the *Tallinn Manual* clearly states that "designing malware and making it openly available online, even if it may be used by someone involved in the conflict to conduct an attack," does not render a civilian targetable.[178] For the Tallinn Experts, this is because it is unclear to the dealer how individuals or groups would use the tool.[179] That is, the direct causation and belligerent nexus requirements are not satisfied. The *Tallinn Manual* also provides the example of a "criminal who uses cyber means to steal State funds belonging to a party to the conflict, but with a view to private gain."[180] Such an individual would not be targetable because the action would have no belligerent nexus to the armed conflict.[181] Thus, under the *Tallinn Manual*, developing a cyber tool and making it generally available online does not render the cyber arms dealer targetable.

However, the United States may take a different approach. For example, its *Naval Warfare Publication* describes military objectives as

> combatants and objects which, by their nature, location, purpose, or use, effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture, or

175. *See id.*
176. TALLINN MANUAL, *supra* note 18, at 120.
177. *Id.*
178. *Id.*
179. *See id.*
180. *Id.*
181. *See id.*

> neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack.[182]

The *Naval Warfare Publication* includes warship construction facilities and industrial installations that produce war-fighting products within a list of potential targets that qualify as military objectives.[183] This publication explicitly includes war-sustaining activities, thereby encompassing that which the *Tallinn Manual* and the *Interpretive Guidance* exclude. This analysis states that any object that contributes to the enemy's war-fighting or war-sustaining capabilities is subject to attack. Thus, while a dealer engaging in war-sustaining activities may not be targetable because he or she does not have combatant status, the dealer's computer may be targetable based on its classification as an object, which by its nature, effectively contributes to the enemy's war-fighting or war-sustaining capability, and whose total or partial destruction would constitute a definite military advantage to the attacker under the circumstances at the time of attack. The *Naval Warfare Publication* adds that civilians and civilian objects may not be the subject of an attack.[184] However, it notes that "[c]ivilian objects consist of all civilian property and activities other than those used to support or sustain the enemy's war-fighting capability."[185] Under this reasoning, if an individual uses a personal computer, or if a group of individuals uses a neighborhood Internet club to support or sustain the enemy's war-fighting capability through the development of cyber tools, that individual's computer or the neighborhood Internet club are both subject to attack.

III. CONCLUSION

Although cyber arms dealers potentially play an important role in cyber activities, they have avoided much of the recent discussion surrounding cyber operations, targeting cyber operations participants, and the proliferation of cyber tools. In light of the United States' statement that it reserves the right to respond with force to any cyber attack, it is important to determine when that force can be legally applied. This is especially true as civilians assume a more active role in armed conflicts, and as it becomes easier for individual civilians to assume that role due to increased access to technology.

---

182. DEP'T OF THE NAVY ET AL., *supra* note 69, ¶ 8.2.

183. *Id.* ¶ 8.2.5.

184. *Id.* ¶ 8.1.

185. *Id.* ¶ 8.3.

While the *Interpretive Guidance* and *Tallinn Manual* are non-binding on states, they contain developed legal analyses for this particular question. Both provide important insights into the legality of targeting civilians who directly participate in hostilities. Interestingly, although they generally use the same language in describing when a civilian is directly participating in hostilities, the specific language of each can result in different targeting conclusions. As states develop targeting policies, they should be careful in scrutinizing each document. But fundamental to such policies is careful consideration that must be given to situations in which cyber arms dealers may be legally targeted.