Center on Law, Ethics and National Security

Essay Series
Number 9
July 27, 2021

Cyber Proxies in International Armed Conflicts: Shrinking the Gray Area

By Victoria Morgan

CYBER PROXIES IN INTERNATIONAL ARMED CONFLICTS:

SHRINKING THE GRAY AREA

VICTORIA MORGAN*

INTRODUCTION

Modern audiences can't get enough of the gun-for-hire archetype. Scattered across books, movies, television shows, and video games, mercenaries[1] often face "heart-pounding" and "deadly" drama.[2] And yet, they maintain an air of "coolness."[3] The mercenary character tends to possess one of two personalities. Sylvester Stallone's Barney Ross-type fighter who acts out of loyalty and "an actual moral compass."[4] Or, Antonio Banderas's Miguel Bain-type antihero who does "whatever it takes to get a job done."[5]

Similar to popular culture's dichotomous portrayal of mercenaries, academics have split into two cohorts. Some condemn hired guns as contributing to a "dark and distasteful" trade,[6] while others appreciate them as "vital actors in promoting not only the interests of states, but also humanitarianism worldwide."[7] In his book *The Prince*, Machiavelli famously adopts the former view.[8] He denounces mercenaries as "disu-

*Duke University School of Law, J.D., expected May 2022. A big thank you to Major General Charles J. Dunlap, Jr. USAF (Ret.) for his guidance and support.

1. The term "mercenary" has been used throughout this article to describe any professional soldier hired to serve in an armed conflict. This definition strays from the strict definition of "mercenary" proposed in Article 47.1 of 1977 Additional Protocol I. *See infra* text accompanying notes 193–98. Experts have continued to use the more traditional, layperson-friendly definition of "mercenary" as an umbrella term, regardless of the Additional Protocol I definition. *See generally* TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER (2018) (using the term "mercenary" throughout the book to apply to any professional soldier hired to serve in an armed conflict); SEAN MCFATE, THE NEW RULES OF WAR: VICTORY IN THE AGE OF DURABLE DISORDER (2019) (same).

2. *See* Elijah Watson, *A Definitive Breakdown of "The Expendables" Members*, COMPLEX (Aug. 4, 2014), https://www.complex.com/pop-culture/2014/08/a-definitive-breakdown-of-the-expendables-members/barney-ross-sylvester-stallone (describing Sylvester Stallone's character in *The Expendables*).

3. *Id.*

4. *See* Patrick Sessoms, *The Top 10 Best Movie Mercenaries*, STARS & POPCORN (May 14, 2020), http://starsandpopcorn.com/best-movie-mercenaries/2/ (listing Tyler Rake from *Extraction* as the second best movie mercenary of all time and noting he struggles "with reconciling exactly what kind of man he is" but ultimately "keeps his moral compass"); *Characters / The Expendables*, TV TROPES, https://tvtropes.org/pmwiki/pmwiki.php/Characters/TheExpendables (Apr. 20, 2021, 9:22 PM) (describing the mercenary team in *The Expendables* as being "devoted to each other" even though their occupation has "moral boundaries").

5. *See Characters / The Expendables*, *supra* note 3; Derek Draven, *The 10 Coolest Mercenaries for Hire in Action Movies, Ranked*, SCREENRANT (Dec. 5, 2020), https://screenrant.com/coolest-movie-mercenaries-ranked/ (noting Antonio Banderas's character as a "ruthless" assassin "who exudes a dark charm").

6. JAMES PATTISON, THE MORALITY OF PRIVATE WAR: THE CHALLENGE OF PRIVATE MILITARY AND SECURITY COMPANIES 3 (2014).

7. *Id.*

8. MCFATE, *supra* note 1, at 123.

nited, ambitious, without discipline, unfaithful; gallant among friends, vile among enemies; no fear of God, no faith with men."[9] This outlook seeps into the modern dictionary definition of "mercenary," which refers to "a person whose actions are motivated primarily by personal gain, often at the *expense of ethics*."[10]

Historically, mercenaries have turned on their employers, installed themselves as rulers, and committed human rights abuses.[11] During a particularly publicized event in 2007, employees of Blackwater—a private military and security company (PMSC)—opened fire on civilians in central Baghdad, killing seventeen.[12] Since then, Blackwater has twice changed its name and has attempted to rebrand as "a new company" that clients will find "boring."[13]

In the other cohort, some scholars reject the all-negative view of mercenaries. Sean McFate—a former paratrooper, turned private contractor, turned professor—labels Machiavelli's cynical view of mercenaries as "bunk."[14] He notes that at the time of Machiavelli's disparaging words, mercenaries were thought to participate in an "honorable" and "legitimate trade," often the "main instrument of war."[15] And in McFate's own experience, "[t]he line between soldier and mercenary is hazier than most think."[16] He points out that some contractors refuse jobs on "political grounds."[17] For example, some PMSCs deny money from Iran, China, and Russia: "America's enemies are their enemies."[18] McFate also suggests that in most militaries, reenlisting for monetary reasons is a "common" practice, and thus "every soldier has a little mercenary in him."[19]

If scholars cannot decide whether hired guns are "honorable" or "distasteful," how can they agree on the laws governing them? This article will suggest that the worst response to this question is to leave the legal landscape inconsistent and unclear. And yet, that is the situation in which we find ourselves. The law is particularly murky in the context of cyber. Thus, with the goal of clarifying the law of armed conflict as it pertains to cyber, this article will apply the principle of distinction to real world examples of cyber groups. The article will wade through the vast amounts of legal gray area and suggest the best paths forward. Ultimately, the article will suggest that although we do not need *new rules*, the current law of armed conflict must be *interpreted differently* when applied to cyber operations than when applied to traditional, kinetic warfare.

---

9. *Id.*

10. *Oxford English Dictionary*, https://www.oed.com/view/Entry/116635?redirectedFrom=mercenary#eid (last visited Apr. 25, 2021).

11. MCFATE, *supra* note 1, at 156; Khalid Elhassan, *A Countdown of History's 16 Most Influential and Formidable Mercenaries*, HISTORY COLLECTION (Oct. 20, 2018), https://historycollection.com/a-countdown-of-historys-16-most-influential-and-formidable-mercenaries/15/; *see also* FINABEL, THE ARMY OF TOMORROW: PRIVATE MILITARY AND SECURITY COMPANIES' CONTRIBUTION TO THE MILITARY AND SECURITY LANDSCAPE 4 (2019) ("In the past, mercenaries were considered a moral disgrace and their use was often compared to the practice of slavery, as it was perceived as another form of trade in human lives.").

12. Laura Reddy, *Blackwater Renames Itself, and Wants to Go Back to Iraq*, ABC NEWS (Dec. 12, 2011, 4:15 PM), https://abcnews.go.com/Blotter/blackwater-renames/story?id=15140210.

13. *Id.*

14. MCFATE, *supra* note 1, at 123.

15. *Id.* at 124–25.

16. *Id.* at 125.

17. *Id.*

18. *Id.*

19. *Id.* at 124–25.

The article will proceed in four main parts. Part I will trace the evolution of traditional hired guns and introduce new characters, such as PMSCs and hacktivists. Part II will explore three types of "cyber proxies." "Cyber proxy" is a blanket term covering any intermediary that conducts cyber operations and is enabled knowingly, actively, or passively by a state.[20] The three cyber proxies are classified by their varying levels of connection to their host states. Part III will outline the relevant law of armed conflict, focusing on the principle of distinction. Part IV will analyze how the law of armed conflict applies to these three cyber proxies. Since a cyber proxy has some relationship with its state, the article will concentrate on international, rather than non-international, armed conflicts.[21] Applying the law of armed conflict to actual cyber proxies will expose areas in the law that are desperate for development.

The essay will present three recommendations: (1) A cyber proxy—that is organized, armed, belongs to a party to the conflict, and has directly participated in the conflict—should be considered part of the armed forces; (2) The "for such time" element of direct participation should begin as soon as a cyber proxy plans to commit an act of direct participation; and (3) After directly participating in the conflict, a cyber proxy's direct participation status should continue as long as a harmed foreign state reasonably believes the hacker will again directly participate in the conflict.

I

INTRODUCING THE CHARACTERS

Mercenaries are "as old as war itself."[22] Indeed, mercenaryism is one of the "first professions."[23] Ancient Greece mobilized "huge" armies of hired warriors.[24] And Ancient Rome engaged mercenaries to support the civilization's more than one-thousand-year reign—mercenaries saved Julius Caesar on at least one occasion.[25] During the Middle Ages, King Henry II retained mercenaries to combat a rebellion, realizing the benefit of men loyal to money rather than the ideals of any revolt.[26] In Medieval Europe, even the church trusted mercenaries to wage their wars.[27] Specifically, Pope Innocent III utilized a "mostly mercenary army" against the Cathars.[28] And the Vatican still employs the Swiss Guard—once considered a "fearsome mercenary unit."[29]

Hired guns have lately returned to center stage, often in the form of private military

20. *See* TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 17 (2017) (providing a similar definition).

21. Under the 1949 Geneva Convention common Article 2, an international armed conflict involves any "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." GARY SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 160 (2d ed. 2016). Under Common Article 3, a non-international armed conflict involves an "armed conflict not of an international character occurring in the territory of one of the High Contracting Parties." *Id.* at 163.

22. MCFATE, *supra* note 1, at 125.

23. FINABEL, *supra* note 10, at 4.

24. MCFATE, *supra* note 1, at 126.

25. *Id.*

26. *Id.*

27. *Id.* at 127.

28. *Id.*

29. *Id.*

companies.[30] PMSCs have grown increasingly powerful, with some enjoying well over 10,000 staff.[31] Many PMSCs can "outclass local militaries," and a few can "even stand up to America's most elite forces."[32] In 2010, up to seventy percent of the United States intelligence budget was thought to be spent on contractors.[33] In the recent Iraq and Afghanistan Wars, more than half of all military personnel were contractors.[34] In Afghanistan, the ratio of US-employed contractor per soldier peaked at 1.6.[35] The Middle East "is swimming in mercenaries," explains a former private contractor, "[t]he capital of Kurdistan, Irbil, has become an unofficial marketplace of mercenary services, reminiscent of the Tatooine bar in the movie *Star Wars*—full of smugglers and guns for hire."[36] Some experts assert that it has become impossible for major Western states to wage war without using private military force.[37] Ultimately, private military companies are "here to stay."[38] Renting force, after all, "is cheaper than owning it."[39]

Complicating matters, these companies have recently begun specializing in cyber operations.[40] Alas, the accountability issues already surrounding PMSCs could become even more exaggerated in a cyber context. For one, these cyber proxies might be "more powerful" than state actors.[41] Plus, the nature of cyberspace—which often embraces techniques like anonymization or falsification of identities—makes it difficult to pinpoint the perpetrator of an attack.[42] And concerningly, the law surrounding these actors remains imprecise.

To add yet another wrinkle, a new character has arrived on the cyber scene: hack-

30. *See id.* at 127–28 ("Mercenaries are back . . . .").

31. ICRC, INTERNATIONAL HUMANITARIAN LAW AND PRIVATE MILITARY/SECURITY COMPANIES - FAQ (2013).

32. *See* MCFATE, *supra* note 1, at 132 ("It took America's most elite troops and advanced aircraft four hours to defeat five hundred mercenaries. What happens when they have to face one thousand? Five thousand? More?").

33. JOSE L. GOMEZ DEL PRADO, THE PRIVATIZATION OF WAR: MERCENARIES, PRIVATE MILITARY AND SECURITY COMPANIES (PMSC) (2010).

34. MCFATE, *supra* note 1, at 128.

35. PATTISON, *supra* note 5, at 2.

36. MCFATE, *supra* note 1, at 133.

37. *See* PATTISON, *supra* note 5, at 2; *see also* ICRC, THE MONTREUX DOCUMENT 5 (2009) [hereinafter MONTREUX DOCUMENT] ("Today, PMSCs are viewed in some quarters as an indispensable ingredient of military undertakings.").

38. MCFATE, *supra* note 1, at 141.

39. *Id.* at 125.

40. Andrew Nusca, *Hayden: 'Digital Blackwater' May Be Necessary for Private Sector to Fight Cyber Threats*, ZDNet (Aug. 1, 2011), https://www.zdnet.com/article/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/.

41. MAURER, *supra* note 19, at 8–9.

42. *See* Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 EUR. J. INT'L L. 941, 944 (2020) (listing the traditional challenges of attribution in cyberspace: "the falsification of identities, the multi-stage nature of cyber operations, the dynamic landscape of cyber threats, the undifferentiated nature of cyber tools, the human and technical resources required in performing attribution and the lengthy timescales involved); Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace*, Fletcher Sec. Rev., Spring 2014, at 55 ("Targeted states often find their response options limited in the absence of an identifiable state author of the operations. Moreover, the anonymity of many hostile operations also renders classic deterrence strategies anaemic in cyberspace.").

tivists. "Hacktivism," a blend of hacking and activism, has become increasingly prevalent.[43] In some cases, states support their domestic hacktivism with resources or encouragement.[44] In other cases, states merely turn a blind eye as hacktivists roughly carry out the government's political agenda.[45] Hacktivism is no longer just a "popular means of activism."[46] Hacktivism has become "an instrument of national power" that poses challenging questions for the law of armed conflict.[47]

II

CYBER PROXIES: THREE TYPES

In his 2018 book, *Cyber Mercenaries*, Tim Maurer explores the relationships between states and their cyber proxies.[48] Maurer provides case studies on the relationships that the United States, Iran, and Russia maintain with their cyber proxies.[49] Ultimately, Maurer splits the cyber proxies into three groups based on the closeness of the proxy's relationship with a state.[50] "Tight leash" is the closest relationship, "loose leash" is in the middle, and "on the loose" represents the least connected relationship.[51] This article uses Maurer's classifications as a tool to help explain the current status of cyber proxies and how the law of armed conflict should apply to them. In reality though, cyber proxies fall on a spectrum, and some may not fit neatly into these buckets.

A. The United States: Cyber Proxies on a "Tight Leash"

The relationship between the United States government and its cyber PMSCs is a "classic example" of the "tight leash" relationship.[52] In this relationship, the state has a "close" connection with its cyber proxy, providing guidance and often specific instructions.[53] A PMSC in this category can be thought of as a "digital Blackwater."[54]

The United States generally insists that firms are US-owned and that individuals performing the work are US citizens with security clearance.[55] PMSC personnel "often work physically alongside their government counterparts."[56] And the government prohibits the contractors to work remotely in order to help ensure proper monitoring.[57] Furthermore, the government has shown its willingness to punish contractors for wrongdoing in the form of civil penalties.[58] The government has even arrested a contractor

43. Dorothy Denning, *The Rise of Hacktivism*, GEO. J. OF INT'L AFFS. (Sep. 8, 2015), https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism.

44. MAURER, *supra* note 19, at 87.

45. *See infra* text accompanying notes 95–113.

46. Denning, *supra* note 42.

47. *Id.*

48. *See generally* MAURER, *supra* note 19.

49. *See id.* at 69–106 (detailing the three case studies).

50. *Id.* at 20.

51. *Id* at 20, 71, 81, 94.

52. *Id.* at 71.

53. *Id.* at 126.

54. *See* Nusca, *supra* note 39 ("Let me really throw out a bumper sticker for you: how about a digital Blackwater?").

55. *Id.*

56. *Id.*

57. *Id.*

58. *See id.* (noting a defense contractor paid millions in civil penalties for outsourcing work to Russian

for allegedly stealing and disclosing code used for NSA offensive cyber operations.[59]

U.S. Cyber Command outsources support for offensive and defensive operations to various contractors.[60] As a result of an inventory of contract personnel, the government reinforced its policy regarding contractors.[61] Contractors were prohibited from carrying out "inherently governmental activities" but were employed for "activities such as collection and analysis."[62] What constitutes "inherently governmental activities," however, is unknown.[63]

B. Iran: Cyber Proxies on a "Loose Leash"

The second cyber proxy relationship involves groups on a "loose leash."[64] This relationship involves "individuals" or a "loose group of individuals" that are under a state's "overall control."[65] The state does not necessarily provide specific instruction, but it supports the group in some way.[66] The support may include "financing, providing equipment, supplying weaponry," or other means of "encouragement."[67]

Iran, a country that only recently began focusing on cyberspace, exemplifies this "loose leash" relationship.[68] Over a decade ago, the Stuxnet malware incident resulted in an Iranian shift in policy.[69] In March 2012, Ayatollah Khamenei established the High Council on Cyberspace.[70] In 2014, he delivered a speech urging Iranian students, whom he called "cyber war agents," to prepare for battle.[71] That same year, reports swirled that the Iranian government "host[ed] hacking contests to identify skilled hackers."[72]

Often, the "loose leash" proxies have a "notably extraterritorial dimension."[73] For example, "Cutting Kitten," an Iranian group of about twenty hackers, allegedly has members not only in Iran but also in the Netherlands, Canada, and the United Kingdom.[74]

One Iranian hacking incident fits neatly into the "loose leash" category. In 2016, the United States government unsealed an indictment against Iranian state-sponsored

---

software developers).

59. *Id.*

60. Aliya Sternstein, *Here Are the Companies That Won a Spot on $460M Cyber Command Deal*, NEXTGOV (May 23, 2016), https://www.nextgov.com/cybersecurity/2016/05/cybercom-inks-460m-operations-support-deal-booz-saic-others/128523/.

61. MAURER, *supra* note 19, at 73.

62. *Id.*

63. *Id.* at 73, 77.

64. *Id.* at 81.

65. *Id.* at 127.

66. *Id.*

67. *Id.*

68. *Id.* at 81.

69. *Id.*

70. *Id.*

71. *Id.*; Shahrooz Shekaraubi, *The Wild West of Cyberwarfare*, INT'L POL'Y DIG., Feb. 26, 2014.

72. MAURER, *supra* note 19, at 82.

73. *Id.* at 83.

74. *Id.*; THAI. COMPUT. EMERGENCY RESPONSE TEAM, THREAT GROUP CARDS: A THREAT ACTOR ENCYCLOPEDIA: APT GROUP: CUTTING KITTEN, TG-2889 (2020).

proxy hackers.[75] The seven Iranians indicted were employed by two computer companies: ITSEC and MERSAD.[76] Allegedly, these two companies acted as "front" companies for the Iranian government.[77] The hackers performed an extensive campaign for over 176 days of distributed denial of service (DDoS) attacks.[78] A DDoS attack, which makes a website or computer unavailable due to flooding or crashing, "is one of the most powerful" internet weapons.[79] These DDoS attacks primarily targeted financial institutions (such as JPMorgan Chase and Wells Fargo) and cost victims millions of US dollars in remediation costs.[80]

In addition to the DDoS attacks, the United States accused one of the indicted hackers of gaining unauthorized cyber access to a dam just north of New York City.[81] For almost a month, the hacker repeatedly obtained information about the operation of the dam, such as water levels, temperature, and the status of the gate controlling flow rates.[82] This intrusion concerned White House officials since it demonstrated an "intent to target such systems in the first place."[83]

Just months before these cyber operations, members of the "front companies" boasted about other victories.[84] The hackers posted multiple times on a global repository for Web defacements.[85] These posts generally included pseudonyms of the hackers next to screenshots of defaced websites. One such post read: "special thank[s]" to "Farzad_Ho, rAbiN_hoOd, and R3D.Mind."[86] It is unclear whether the Iranian government already had a relationship with the hackers at that time.[87] The government has never publicly endorsed, let alone admitted to, any of the hackers' cyber operations.[88]

C. Russia: Hacktivists "On the Loose"

The "on the loose" cyber proxy relationship occurs "when a state consciously but indirectly benefits from a malicious activity."[89] The state "could stop" the activity but "chooses not to."[90] Russia fosters an atmosphere conducive to this "on the loose" relationship, which, in turn, "creates a fertile ground for such malicious activity to occur in

75. U.S. DEP'T OF JUST., SEVEN IRANIANS WORKING FOR ISLAMIC REVOLUTIONARY GUARD CORPS-AFFILIATED ENTITIES CHARGED FOR CONDUCTING COORDINATED CAMPAIGN OF CYBER ATTACKS AGAINST U.S. FINANCIAL SECTOR (2016).

76. *Id.*

77. MAURER, *supra* note 19, at 86.

78. *Id.* at 85.

79. Steve Weisman, *What Is a Distributed Denial of Service Attack (DDoS) and What Can You Do About Them?*, NORTON (Jul. 23, 2020), https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html.

80. MAURER, *supra* note 19, at 85.

81. U.S. DEP'T OF JUST., *supra* note 75.

82. *Id.*

83. MAURER, *supra* note 19, at 88.

84. *Id.* at 87.

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.* at 87–89.

89. *Id.* at 94.

90. *Id.*

the first place."[91]

Former Soviet Union states rank as some of the "most literate and educated societies" with many individuals possessing "highly developed technical skills."[92] However, their economies have generally failed to absorb the technically skilled workforce.[93] Accepting a cybersecurity government salary of a few thousand dollars a year seems foolish compared to the thousands, or even millions, that can be made in cyber heist.[94] Consequently, the "legitimate" cyber industry is simply "not big enough to absorb all of the labor."[95]

Notably though, Russian hackers take "great care" to target "victims abroad rather than at home."[96] This strategy seems acceptable to the Kremlin. "[Russian law enforcement has] a very good idea of what is going on and they are monitoring it," one expert remarks, "but as long as the fraud is restricted to other parts of the world they don't care."[97] Indeed, the Russian government does more than merely ignore. When asked by foreign law enforcement to assist in holding its hackers accountable, the Russian government has refused, blocked extradition requests, and protested when its nationals are arrested abroad.[98] A former head of the KGB office in London commented that one hacker caught by the Russian government was offered "the choice of either prison or cooperation with the [Russian Federal Security Service]."[99] The hacker chose the latter.[100] On the other hand, when Russian hackers target domestic victims, "Moscow's response is swift and harsh."[101] One video shows a busted hacker "loudly weeping" following a Russian law enforcement raid on his home.[102] In this atmosphere, cyber operations against foreign victims continue to grow in popularity, and the severity of the operations continues to escalate in nature.[103]

These Russian hackers can possess more than mere financial motives. Often, groups "mobilize themselves and take political action in support of the government."[104] These hacktivists have entered recent Russian conflicts involving Estonia and Ukraine.[105] Although there is generally "no conclusive proof of the Kremlin's direct involvement," there is "considerable evidence" that the government "sanction[s]" the

91. *Id.*

92. *Id.*; *see also* TECH GLOBAL BLOG, RUSSIA RANKED AS TOP COUNTRY IN TECHNOLOGY AND DATA SCIENCE SKILLS (2020), https://tech.global/blog/russia-ranked-as-top-country-in-technology-and-data-science-skills (analyzing recent report by Global Skills Index, which ranked Russia first in technology and data science).

93. MAURER, *supra* note 19, at 94.

94. *Id.* at 94–95.

95. *Id.*

96. *Id.* at 95, 106.

97. *Id.* at 95.

98. *Id.*; *see also Russia Steps Up Efforts to Shield its Hackers from Extradition to U.S.*, Wall St. J., Nov. 5, 2019 (revealing Russian tactics to "keep potential cyber operatives out of U.S. hands").

99. MAURER, *supra* note 19, at 96.

100. *Id.*

101. *Id.* at 95.

102. *Id.*

103. *See id.* at 98–99 (providing examples of escalating conduct and noting that "[i]t remains unclear whether the most significant cyber attack that occurred" during the conflict between Ukraine and Russia "was the result of proxy activity or was carried out by the Russian government").

104. *Id.* at 106.

105. *Id.*

hacktivist activities by doing "very little to stop" them.[106] Thus, without even paying for it, the Russian government can harm its enemies and enjoy plausible deniability.[107]

III

THE PRINCIPLE OF DISTINCTION

The law of armed conflict applies to cyber operations conducted during armed conflicts.[108] In particular, the principle of distinction applies to cyber attacks.[109] While the law of armed conflict does not prohibit "any category of person from participating in cyber operations," "the legal consequences of participation differ."[110] The status of cyber fighters determines the protections and rights bestowed upon the individual.[111] Battlefield status dictates whether an individual is a lawful target and can "determine [one's] life in a literal sense."[112] There are many battlefield statuses. And no one lacks status.[113]

In 1863, Francis Lieber declared that, "all enemies in regular war are divided into two general classes—that is to say, into combatants and noncombatants."[114] Though somewhat more muddled than in Lieber's time, that statement broadly remains true. In an international armed conflict, "there are combatants and there are others."[115]

For international armed conflict, the principle of distinction is codified in Article 48 of the 1977 Additional Protocol I to the 1949 Geneva Conventions ("Additional Protocol I").[116] Additional Protocol I commands that, "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."[117] Furthermore, Article 51.2 states that, "[t]he civilian population as such, as well as individual civilians, shall not be the object of the attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."[118] These requirements represent customary international law.[119] And analogous restrictions apply to non-international armed conflicts.[120]

---

106. *Id.* at 97.

107. *Id.* at 99–100.

108. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 420 (Michael N. Schmitt ed. 2017) [hereinafter TALLINN MANUAL 2.0]; *see also* ICRC, *Cyber Warfare: Does International Humanitarian Law Apply?* (Sep. 3, 2021), https://blogs.icrc.org/new-delhi/2021/03/09/cyber-warfare-does-international-humanitarian-law-apply/ ("IHL applies . . . to cyber operations that are conducted in the context of an armed conflict.").

109. TALLINN MANUAL, *supra* note 114, at 420.

110. *Id.* at 401.

111. SOLIS, *supra* note 20, at 200.

112. *Id.* at 201.

113. *Id.*

114. U.S. Department of War, Instructions for the Government of Armies of the United States in the Field, General Orders No. 100, art. 155, Apr. 24, 1863 [hereinafter Lieber Code].

115. SOLIS, *supra* note 20, at 201.

116. Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

117. *Id.*

118. *Id.* art. 51.2.

119. Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARV. NAT'L SEC. J. 5, 12 (2010).

120. *Id.*

In differentiating between armed forces and the civilian population, the principle of distinction strives "to ensure respect for and protection of the civilian population and civilian objects."[121] And when there is "doubt as to whether a person is a civilian, that person shall be considered to be a civilian."[122] However, the principle of distinction cannot simply protect civilians—it must also consider military necessity.[123] Thus, if certain criteria are met, a civilian is considered a "direct participant" in hostilities and is thus targetable for a certain period of time.[124]

Traditionally, the law of armed conflict did not define "direct part in hostilities."[125] Therefore, in attempt to better define the term, a group of forty international law experts participated in a series of workshops in 2008.[126] The International Committee of the Red Cross (ICRC) culminated the experts' efforts in a publication called the Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (Interpretive Guidance).[127] The Interpretive Guidance is not legally binding and "solely" represents "the ICRC's views."[128] Indeed, some aspects of the Interpretive Guidance are so controversial that a significant number of experts withdrew their names from the publication.[129] Nonetheless, the Interpretive Guidance provides a detailed analysis of direct participation and a starting point for future interpretations and recommendations. This article will evaluate how the Interpretive Guidance would determine the statuses of different types of cyber proxies. Furthermore, it will analyze the various cyber proxies using the second edition of the *Tallinn Manual*, "the most comprehensive analysis of how existing laws of armed conflict apply to cyber warfare."[130]

For international armed conflicts, the Interpretive Guidance defines civilians negatively as: "all persons who are neither members of the armed forces of a party to the conflict nor participants in a *levée en masse* are civilians."[131] The Interpretive Guidance emphasizes that members of the armed forces, *levée en masse*, and civilians are "mutually exclusive."[132] In other words, any person involved in an armed conflict "falls into one of these three categories."[133] The following sections will discuss each of these categories, providing the traditional law of armed conflict plus details noted in the Interpretive Guidance.

---

121. AP I, *supra* note 122, art. 48.

122. TALLINN MANUAL, *supra* note 114, at 424; AP I, *supra* note 122, art. 50.1.

123. Schmitt, *supra* note 125, at 12.

124. SOLIS, *supra* note 20, at 218.

125. Schmitt, *supra* note 125, at 24–25.

126. *Id.* at 5.

127. *Id.*

128. *Id.* at 6.

129. *Id.* at 5–6.

130. Hensey A. Fenton, *Proportionality and Its Applicability in the Realm of Cyber-Attacks*, 29 Duke J. Compar. & Int'l L. 335, 342 (2019).

131. ICRC, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 20 (2009) [hereinafter INTERPRETIVE GUIDANCE].

132. *Id.*

133. *Id.* at 21.

A. Members of the Armed Forces

In international armed conflicts, members of the armed forces of a party to the conflict are combatants and thus "have the right to participate directly in hostilities."[134] For the United States, this category includes the United States armed forces, the Reserved forces, and the National Guard units.[135] These individuals "may attack and be attacked; they may kill and be killed."[136] Under Article 43.1 of Additional Protocol I, members of the armed forces of a party to the conflict are targetable at all times.[137]

Notably, the Interpretive Guidance defines "members of the armed forces" broadly. The Interpretive Guidance supports that decision by noting that any armed forces failing to distinguish themselves from the population should not be granted the protective legal regime afforded to civilians.[138] Therefore, under the Interpretive Guidance, "members of the armed forces" include both the regular armed forces and "all actors showing a sufficient degree of military organization and belonging to a party to the conflict."[139] Put simply, to have status like members of the armed forces, a group must be (1) organized, (2) armed, and (3) belonging to a party to the conflict.

The "belonging" element requires the most explanation. The Interpretive Guidance states that "belonging to" means "at least a *de facto* relationship between an organized armed group and a party to the conflict."[140] According to the Interpretive Guidance, an organized armed group belongs to a party to the conflict if:

- The relationship is "officially declared;"
- The relationship is "expressed through tacit agreement or conclusive [behavior] that makes clear for which party the group is fighting;" or
- The group's conduct is "attributable to that State under the international law of State responsibility."[141]

The "officially declared" criteria poses questions: who would need to "officially" declare the relationship? The armed group? The state? The "state responsibility" benchmark is also unclear. Indeed, the Interpretive Guidance admits that state responsibility is not yet settled in international law.[142]

According to the ICRC, state responsibility for cyber proxies is determined on a

134. AP I, *supra* note 122, art. 43.2.

135. SOLIS, *supra* note 20, at 201.

136. *Id.* at 202.

137. *Id.* at 203; Schmitt, *supra* note 125, at 15.

138. INTERPRETIVE GUIDANCE, *supra* note 137, at 22. This analysis reflects Article 4A(2) of Geneva Convention III, which mandates four conditions for organized armed groups: "(a) be commanded by a person responsible for his subordinates; (b) wear a distinctive emblem or attire that is recognizable at a distance; (c) carry arms openly; and (d) conduct operations in accordance with the law of armed conflict." TALLINN MANUAL, *supra* note 114, at 403.

139. INTERPRETIVE GUIDANCE, *supra* note 137, at 22.

140. *Id.* at 23.

141. *Id.*

142. *Id.*

"case-by-case" basis.[143] In an attempt to clarify state responsibility, specifically in regard to PMSCs, the ICRC developed the *Montreux Document*.[144] The *Montreux Document* is "not a legally binding instrument" but simply provides foreign states with "good practices."[145] The *Montreux Document* stipulates that "entering into contractual relations" with a PMSC "does not in itself engage the responsibility" of the contracting state.[146] The state responsibility guidelines in the *Montreux Document*, *The Tallinn Manual*, and the International Law Commission's *Draft Articles on Responsibility of States for International Wrongful Acts* embrace similar language: "Cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own."[147] One way the state can acknowledge the operation is by "publicly endors[ing]" it.[148] The *Montreux Document* also adds that a PMSC's conduct may be attributable to a Contracting State if the PMSC was "empowered to exercise elements of government authority."[149]

After the Interpretive Guidance lists the elements of "belonging to," the Guidance sneaks in one more line: "In practice, in order for an organized armed group to belong to a party to the conflict, it appears essential that it conduct hostilities on behalf and with the agreement of that."[150] This sentence seemingly adds another element of "belonging to"—the organized armed group must "conduct hostilities."[151] The Interpretive Guidance moves on without an explanation. Yet, if the ICRC meant those words, then that element greatly changes the "belonging to" test. Not only must an organized armed group have a tight relationship with its government, it must "conduct hostilities."

As to what happens when an organized armed group does *not* belong to a party to the conflict, the International Group of Experts was divided.[152] The Interpretive Guidance states that if an organized armed group does not meet the "belonging to" criteria, then its members are civilians.[153] As civilians, they can only be targeted for such time as they directly participate in hostilities.[154] However, other experts argued that there is

143. MONTREUX DOCUMENT, *supra* note 36, at 11, 14.

144. *Id.* at 5.

145. *Id.* at 9.

146. *Id.* at 12.

147. TALLINN MANUAL, *supra* note 114, at 94–95; MONTREUX DOCUMENT, *supra* note 36, at 12; International Law Commission, Report on the Work of its Fifty-Third Session, U.N. Doc. A/56/10, at 47 (2001).

148. ICRC, *Customary IHL Database*, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule149#refFn_EC46E6AE_00034 (last visited Apr. 22, 2021).

149. *See* MONTREUX DOCUMENT, *supra* note 36, at 12 (noting that "government authority" might include being "formally authorized by law or regulation to carry out functions normally conducted by organs of the State").

150. INTERPRETIVE GUIDANCE, *supra* note 137, at 23.

151. *Id.*

152. TALLINN MANUAL, *supra* note 114, at 427. The Interpretive Guidance also suggested that that "organized armed groups operating within the broader context of an international armed conflict without belonging to a party to that conflict *could still* be regarded as parties to a separate non-international armed conflict." INTERPRETIVE GUIDANCE, *supra* note 137, at 24 (emphasis added). But see Schmitt, *supra* note 125, at 18–19, for why that approach "makes little sense" on both a practical and legal level.

153. TALLINN MANUAL, *supra* note 114, at 430.

154. *See supra* text accompanying notes 123–25.

no requirement that an organized armed group belong to a party.[155] Under that second approach, all group members could be targeted based on their status, regardless of whether they are directly participating at the time.[156]

B. Levée en masse

The International Criminal Tribunal for the Former Yugoslavia (ICTY) defines *levée en masse* as "inhabitants of a non-occupied territory who, on the approach of the enemy, spontaneously [take] up arms to resist the invading forces, without having had time to form themselves into regular armed units, and at all times they carried arms openly and respected the laws and customs of war."[157] Given that *levées en masse* are rare on today's battlefields and are not particularly pertinent to the world of cyber,[158] this article spends little time on the topic.

C. Civilians

According to the Interpretive Guidance, if an individual has not fallen into the previous two categories—armed forces members or *levée en masse*—the individual must be a civilian.[159] Generally, civilians shall not be targeted as the object of an attack.[160] However, there are exceptions. In 1977, Additional Protocol I defined one of these exceptions—a civilian who directly participates in an armed conflict.[161] And in 2008, the Interpretive Guidance recommended an addition—civilians who engage in a "continuous combat function."[162]

1. Continuous Combat Function

Somewhat confusingly, the ICRC almost entirely discusses "continuous combat function" in the section of the Interpretive Guidance dedicated to non-international armed conflicts.[163] Some experts have interpreted the term as applying to both international and non-international armed conflicts.[164] Others have interpreted the term as applying only to "non-state organized armed groups in non-international armed conflicts."[165]

According to the Interpretive Guidance, members of an organized group that perform a "continuous combat function" may be attacked on the basis of their membership in that group.[166] In other words, these group members can be attacked even if they are

155. TALLINN MANUAL, *supra* note 114, at 430.

156. *Id.*

157. Prosecutor v. Delalíc et al., Case No. IT-96-21-T, Judgment, ¶ 268 (Int'l Crim. Trib. For the former Yugoslavia Nov. 16, 1998).

158. *See* SOLIS, *supra* note 20, at 214–15 ("[T]he *levée en masse* is uncommon in modern times . . . .").

159. *See supra* text accompanying notes 137–39.

160. AP I, *supra* note 122, art. 51.2.

161. *Id.* art. 51.3.

162. *See infra* text accompanying notes 169–76.

163. *See* INTERPRETIVE GUIDANCE, *supra* note 137, at 27–36 (discussing non-international armed conflict).

164. Schmitt, *supra* note 125, at 21–22 ("This combat function criterion applies to members of organized armed groups in both international and non-international armed conflicts.").

165. LINDSEY CAMERON, THE PRIVATIZATION OF PEACEKEEPING: EXPLORING LIMITS AND RESPONSIBILITY UNDER INTERNATIONAL LAW 153–54 (2017).

166. INTERPRETIVE GUIDANCE, *supra* note 137, at 28.

not presently engaged in hostile activities at the time. A "continuous combat function" involves actions that rise to the level of "direct participation."[167] In fact, it is easier to think of "continuous combat function" as "continuous direct participation."

According to the Interpretive Guidance, evidence of "continuous combat function" may be openly expressed "through the carrying of uniforms, distinctive signs, or certain weapons."[168] In addition, it may be identified based on conclusive behavior—such as, when a person "has *repeatedly directly participated* in hostilities" that indicates a "continuous function."[169] Again, why not just call the term "continuous direct participation?"

The "continuous" nature of this term is what distinguishes this category from the following category. As noted below "direct participants" carry out similar activities as fighters in "continuous combat function," but only do so in a "spontaneous, sporadic, or temporary" way.[170]

2. Direct Participants

The concept of direct participation in hostilities "has vexed . . . students and practitioners" since its inclusion in Additional Protocol I.[171] Direct participation applies to civilians in international and non-international armed conflicts.[172] The "direct participation" status has the following consequences. First, direct participants may be specifically and intentionally targeted.[173] Second, "to the extent that civilians may be attacked under the 'direct participation' rule, their death or injury need not be considered in proportionality assessments."[174] And third, states are not required to consider harm to direct participants when taking "constant care" to "spare" civilians during attack.[175]

Additional Protocol I describes the direct participant status: "Civilians shall enjoy the protection afforded by this Section, [General Protection Against Effects of Hostilities], unless and for such time as they take a direct part in hostilities."[176] Two terms in particular have led to much debate: "direct part" and "for such time."[177] The *Commentary* to Protocol I notes that direct participation refers to "acts of war which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces."[178] Through the Interpretive Guidance, the ICRC sought to provide more clarity.

The Interpretive Guidance notes that "in determining whether a particular conduct amounts to direct participation," one must consider the total "circumstances prevailing

167. *Id.* at 27.

168. *Id.* at 35.

169. *Id.* (emphasis added)

170. *Id.*

171. SOLIS, *supra* note 20, at 217.

172. *Id.*

173. *See* TALLINN MANUAL, *supra* note 114, at 428 ("An act of direct participation in hostilities by civilian renders them liable to be attacked by cyber or other lawful means.").

174. *Id.* at 428–29.

175. Schmitt, *supra* note 125, at 13.

176. AP I, *supra* note 122, art. 51.3.

177. SOLIS, *supra* note 20, at 217.

178. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1679, at 516 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

at the relevant time and place."[179] To aid in this determination, the Interpretive Guidance outlines three criteria that conduct must meet in order to constitute direct participation. First, the act must meet a threshold of harm: "the act must be likely to adversely affect the . . . military capacity of a party to an armed conflict or . . . to inflict death, injury, or destruction on persons or objects protected against direct attack."[180] Second, there must be a "direct causal link between the act and the harm likely to result."[181] And third, there must be a "belligerent nexus:" "the act 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."[182]

The temporal element of direct participation—"for such time"—is "key with regard to targetability."[183] Civilians forfeit their protection against direct attack "for such time" as they directly participate, and thus the beginning and end of that direct participation must be determined with the "utmost care."[184] Attempting to clarify the temporal element, the Interpretive Guidance provides that: "Measures preparatory to the execution of a specific act or direct participation in hostilities, as well as the deployment to and the return from the location of its execution, constitute an integral part of that act."[185] For instance, when the execution of the qualifying act requires "prior geographic deployment, such deployment already constitutes an integral part of the act."[186]

D. What about "Mercenaries"?

Given the frequent use of the layperson definition of "mercenary" in the beginning of this article—as well as the title of Tim Maurer's book, *Cyber Mercenaries*—one might assume that cyber proxies could fit under the "mercenary" description. However, under the law of armed conflict, the "mercenary" term has a strict, narrow definition that generally does not apply to cyber proxies. Mirroring Additional Protocol I, the *Tallinn Manual* denotes "mercenaries" as "unprivileged belligerents," even in cyber operations.[187] Under the law of armed conflict, the following conditions must be fulfilled for an individual to be a "mercenary:" "special recruitment; direct participation in hostilities, desire for private gain as primary motivation; neither a national of a party to the conflict nor a resident of territory controlled by a party; not a member of the armed forces of a party to the conflict; and not sent by another State on official duty as a member of its armed forces."[188]

Even though mercenaries have had a "longstanding role" in armed conflict, "newly independent states had fought against mercenaries in their wars of independence" and "saw little reason" to protect them.[189] These states, particularly including post-colonial

179. INTERPRETIVE GUIDANCE, *supra* note 137, at 41–42.
180. *Id.* at 46.
181. *Id.*
182. *Id.*
183. TALLINN MANUAL, *supra* note 114, at 431.
184. INTERPRETIVE GUIDANCE, *supra* note 137, at 65.
185. *Id.*
186. *Id.* at 67.
187. TALLINN MANUAL, *supra* note 114, at 412.
188. *Id.*
189. Philip Sutter, *The Continuing Role for Belligerent Reprisals*, 13 J. of Conflict & Sec. L. 93, 112 (2008).

Africa, have expressed that unregulated mercenary activity allows "mercenaries to land at an African country in the morning and overthrow the Government by lunch time."[190] Some publications claim that "mercenaryism is now considered illegal by the International Community."[191] However, the *Tallinn Manual* and other experts confirm that while some states have criminalized mercenary activity through conventions, Additional Protocol I "does not criminalize mercenary activity."[192]

IV

ANALYZING THE THREE TYPES OF CYBER PROXIES

Each type of cyber proxy—"tight leash," "loose leash," and "on the loose"—raises its own questions about the principle of distinction and the individual statuses of its members. This section will work through those evaluations and make recommendations regarding how best to interpret the law of armed conflict in this context.

A. Taking "Mercenary" Off the Table

As an initial matter, very few individuals in these cyber proxies would classify as mercenaries. As to PMSCs, the United States places enough regulations on the companies to generally rule out the mercenary label. For example, firms must be US-owned or "possess a favorable National Interest Determination."[193] Plus, "all individuals performing the work must be US citizens" and must have certain security clearances.[194] In placing those restrictions, the United States essentially ensures that personnel will not include non-nationals and thus will not include mercenaries. As to hacktivists, the point in "hacktivism" is to play some part in political activism. Thus, even if paid for their services, hacktivists are unlikely to fall under the definition of mercenary since their "primary motivation" is not a "desire for private gain." Thus, the "mercenary" label applies to very few fighters in the cyber proxy world.[195]

Even if a cyber fighter did qualify as a mercenary, that status would have practically no pertinent legal implications. Mercenaries are neither "part of the armed forces of a party to the conflict" nor are they *levée en masse*.[196] Thus, they are civilians.[197] As with other civilians, depending on their conduct, their status could rise to the level of direct participation or continuous combat function.[198] In other words, for targeting purposes, the analysis would be the same for mercenaries as it is for any other civilian.

---

190. Katherine Fallah, *Corporate Actors: The Legal Status of Mercenaries in Armed Conflict*, 88 Int'l Rev. Red Cross 599, 601 (2006).

191. FINABEL, *supra* note 10, at 5.

192. *See* Fallah, *supra* note 196, at 607–10 ("The major point of distinction is that Protocol I does not criminalize mercenary activity, whereas the mercenary conventions do."); TALLINN MANUAL, *supra* note 114, at 413 (describing mercenaries as "unprivileged belligerents" who lack "combatant status," which "is especially important in light of the criminalization of mercenaries by many States").

193. MAURER, *supra* note 19, at 78.

194. *Id.*

195. Fallah, *supra* note 196, at 610 (analyzing the "narrow scope" of the definition of "mercenary").

196. SOLIS, *supra* note 20, at 132.

197. *Id.*

198. *Id.*

B. Analyzing American PMSCs on a "Tight Leash"

The Interpretive Guidance remarks that the "special role" of PMSC personnel requires that their status be determined with "particular care" due to the closeness of these contractors "to the armed forces and the hostilities."[199] Yet, the Interpretive Guidance provides complicated, conflicting instructions.

As an initial matter, the "tight leash" American PMSCs likely meet the "armed," "organized," and "belonging to" elements. As to being "armed," cyber PMSCs possess the abilities to penetrate target systems and offer a "broad range of services" ranging from defensive to offensive.[200] Experts indicate that carrying a computer with destructive capabilities can qualify as carrying a weapon.[201] As to being "organized," private cybersecurity companies function within a corporate structure and are highly regulated.[202]

And third, a "tight leash" PMSC would likely belong to a party to the conflict under the Interpretive Guidance. These companies sign contracts with the government, sometimes followed by press releases.[203] These actions "officially declare" the agent-proxy relationship. Moreover, the Interpretive Guidance states that "[w]ithout any doubt, an organized armed group can be said to belong to a State if its conduct is attributable to that State under the international law of State Responsibility."[204] The conduct of "tight leash" PMSCs would be "attributable" to the United States under the current law of state responsibility. In a "tight leash" relationship, PMSC personnel physically work side-by-side with the armed forces.[205] Their members are not even permitted to work remotely.[206] Furthermore, the United States government has indicated its ability to punish PMSC personnel for misconduct.[207] For these reasons, the PMSC engages under the State's "instructions" and works "under its direction or control."[208]

American PMSCs, therefore, seem to qualify as "organized," "armed," and "belonging to a party to the conflict." One might assume that the analysis is over and that the PMSC is considered "part of the armed forces." The Interpretive Guidance, after all, asserts that "all armed actors showing a sufficient degree of military organization and belonging to a party to the conflict *must be regard as part of the armed forces* of that party."[209] According to that sentence, as long as a group is armed, organized, and "belonging to" a party, a group member is targetable. That standard is based on membership, not conduct.

---

199. INTERPRETIVE GUIDANCE, *supra* note 137, at 37.

200. MAURER, *supra* note 19, at 74, 77.

201. *See* TALLINN MANUAL, *supra* note 114, at 103 (noting that for the purposes of the Manual, computers can be considered cyber weapons under certain circumstances). *But see* Maurizio D'Urso, *The Cyber Combatant: A New Status for a New Warrior*, 28 PHIL. & TECH. 475, 476 ("[A] computer is not considered a weapon.").

202. MAURER, *supra* note 19, at 78.

203. *See* Sternstein, *supra* note 54 and ("U.S. Cyber Command plans to outsource . . . to a team of six contractors, including Booz Allen Hamilton, SAIC and CACI.").

204. INTERPRETIVE GUIDANCE, *supra* note 137, at 23.

205. *See supra* text notes 65–67 and accompanying text.

206. MAURER, *supra* note 19, at 78.

207. *Id.*

208. MONTREUX DOCUMENT, *supra* note 36, at 9.

209. INTERPRETIVE GUIDANCE, *supra* note 137, at 22.

However, in a different part of the Guidance, the ICRC slips in another element. The Interpretive Guidance remarks that "[most PMSC personnel] have not been incorporated into State armed forces and assume functions that clearly do not involve . . . [a] continuous combat function."[210] The Interpretive Guidance continues: "In practice, in order for an organized armed group to belong to a party to the conflict, it appears essential that it is conducting hostilities on behalf and with the agreement of that party."[211] As an initial matter, this business about "continuous combat function" and "conducting hostilities" is drafted so vexingly that one scholar thought the terms only applied to non-international armed conflict.[212] Nonetheless, given that the terms are woven through a discussion that is neither labelled as "international" nor "non-international" armed conflict, one can assume that they apply to both. Moreover, one can assume—though it's also never clarified—that "continuous combat function" and "conducting hostilities" refer to the same idea. That is, an "organized armed group belonging to a party" must also commit certain continuously hostile acts in order to be "part" of the armed forces.

This fourth "continuous combat function" element adds a temporal dimension. For example, what if a cyber PMSC carried out "hostile conduct" throughout the month of January but then abruptly stopped. Three months later, is the group still considered part of the armed forces? Foreign states trying to target PMSCs would have to sit around discussing whether, at any moment, a company is continuously conducting "hostile conduct" in cyberspace. That mental gymnastics seems identical to the direct participation analysis that is usually done *after* one determines that a group is neither "part of the armed forces" nor *en levée masse*. What is the point in having a status designation for an "organized armed group belonging to a party" if we have to do a continuous combat function analysis anyway? There may be a reasonable answer to this question—but it cannot be found in the Interpretive Guidance.

Nonetheless, the Interpretive Guidance does get one thing right. In determining whether a group is "part of the armed forces," there should be a conduct requirement. Without that element, a PMSC that never attacks the enemy, but simply boosts cyber defense systems, could be targetable at any time during an armed conflict.

But the conduct requirement should not be the Interpretive Guidance's "continuous combat function." That standard puts far too much burden on the harmed state. Cyber operations are often done with anonymization.[213] We cannot expect a commander to have enough evidence to determine that a particular organized armed group has continuously attacked at a level of direct participation. We would be lucky to identify one of those attacks. Thus, if a group is "organized," "armed," "belonging to a party," and has conducted "direct participation" in an armed conflict, that group should be considered part of the armed forces. Under this system, states are disincentivized from allowing PMSCs to conduct inherently government conduct, such as direct participation. Once they do, that group becomes targetable based on membership in the group.

At the moment, the United States maintains the position that it does not delegate

210. *Id.* at 38.
211. *Id.* at 23.
212. CAMERON, *supra* note 171, 153–54.
213. *See supra* note 41 and accompanying text.

inherently governmental activities to its cyber PMSCs.[214] This policy could change since the companies can clearly have the abilities to offer the "full length of the spear," including the "deadly tip."[215] Nonetheless, the original policy is there for a reason. Our military likely has more discipline, legal training, and accountability than a private military company.[216] States should be incentivized to keep inherently government activities within the military. And if they decide to delegate that power to private companies, the personnel in those companies must accept that they are targetable simply based on membership in that group.

C. Analyzing Iran's "Loose Leash" Cyber Proxies

"Loose Leash" cyber proxies probably will not meet the criteria for an "organized armed group belonging to a party." First, they are not particularly "organized." These groups are often comprised of a "loose group of individuals" spread across multiple states.[217] The members of the group have likely spoken only over the Internet, never meeting in person.[218] Moreover, as to the indicted Iranian hackers, some used their own pseudonyms when "publicly boast[ing]" about their Web defacements.[219] A fully organized group probably would not display such individuality.

Moreover, these "loose leash" Iranian hackers likely did not "belong" to the Iranian government, assuming the government did not provide them with specific instructions. The hackers seemed to work for "front" companies coordinated to some extent by the Iranian government.[220] The "belonging to" analysis hinges on how close those "front companies" were to the government. According to the U.S. indictment, the Iranian government provided resources and shepherded the individual hackers into these front companies.[221] However, Iran never "publicly endorsed" the hackers, and there is no evidence that the government provided them with "specific instructions."[222] Thus, based on the evidence in the U.S. indictment alone, these "loose leash" proxy groups would not belong to the Iranian government.

Since the "loose leash" proxies cannot be labelled as "organized armed groups belonging to a party," the members in these groups retain their civilian status. Thus, the members of these groups could qualify as direct participants or even possess a "continuous combat function," depending on their conduct.

---

214. *See* MAURER, *supra* note 19, at 77 (noting that it is difficult to pinpoint what exactly constitutes inherently governmental functions, but that American PMSCs do not partake in the "deadly" part of the spectrum).

215. *Id.*

216. *See* GOMEZ DEL PRADO, *supra* note 32 (considering PSMC-related accountability issues); MCFATE, *supra* note 1, at 138–39 (debating the difficulty of regulating mercenaries).

217. MAURER, *supra* note 19, at 83, 127.

218. *See* TALLINN MANUAL, *supra* note 114, at 404 (noting that organizing a group purely over the Internet could indicate lack of organization).

219. *See* MAURER, *supra* note 19, at 87 (discussing pseudonyms posted next to pictures of defaced websites such as: "special thank[s]" to "Farzad_Ho, rAbiN_hoOd, and R3D.Mind"). Tim Maurer mentions that the public boasting via individual pseudonyms ended a couple of months before the attack on the US financial institutions. *Id.* at 87. Perhaps, the group became more organized at that time.

220. MAURER, *supra* note 19, at 86.

221. *See supra* notes 81–94 and accompanying text.

222. *Id.*

D. Analyzing Russian Hacktivists "On the Loose"

Hacktivists "on the loose" almost certainly cannot constitute "organized armed group[s] belonging to a party." In fact, these groups are even less likely to be "organized" or "belonging to a party" than the "loose leash" groups discussed previously. For these hacktivists, there is no governmental direction, control, or public endorsement—hence, the term "on the loose."

Therefore, the "on the loose" hacktivists retain their civilian status. The next question becomes whether they are "direct participants." Given the steady escalation of hacktivist operations,[223] a hacktivist group could certainly directly participate in a future armed conflict. It should be noted that in order to directly participate, a hacktivist's conduct would need to be "specifically designed" to cause harm "*in support of a party* to the conflict."[224] Although the group has loose ties to the government, the group would still need to meet this "belligerent nexus." Consequently, hacktivists who enter a conflict without any intention to aid the current parties in the conflict would not count as direct participants.

More interesting issues arise if we assume a future hacktivist *does* commit an act of direct participation. In that scenario, the hacktivists may be targetable "for such time" as they directly participate.[225] The question then becomes: when does a hacktivist's direct participation begin? And when does it end? After all, a hacktivist may only be targeted during this period.[226]

Experts disagree on the bounds of this temporal element. According to the Interpretive Guidance, the time period should include "actions immediately preceding or subsequent to the qualifying act."[227] For instance, a hacktivist would be considered a direct participant when "travelling to and from the location" where the individual's computer is being used to mount an operation.[228] Other scholars have proposed extending the time period "as far 'upstream' and 'downstream' as a causal link exist[s]."[229] Under that "causal link" theory, the time period would begin once an individual starts "probing the target system for vulnerabilities."[230]

However, the temporal element should commence earlier than proposed in either of those theories. If the United States gains intel that a Russian hacktivist group is *planning* to directly participate in hostilities, the United States should be able to target that group. Assuming the military has reasonable intel about the planned attack, there is no practical reason to force the military to wait until the hacktivist walks to his computer or begins the process of exploiting system vulnerabilities.

223. *See generally* Denning, *supra* note 42 (outlining the increase in hacktivist activity).
224. INTERPRETIVE GUIDANCE, *supra* note 137, at 46.
225. TALLINN MANUAL, *supra* note 114, at 428.
226. *Id.*
227. *Id.* at 431.
228. *Id.*
229. *Id.*
230. *Id.*

As to when the time period ends, the Interpretive Guidance provides that the participation concludes upon "return from the location of [the act's] execution."[231] That theory, however, is based on kinetic warfare. The theory pertains to the deployment and return of fighters.[232] However, geography has little relevance in cyber operations.[233] Cyber operations are often far removed from the harmed location.[234] Moreover, in the cyber context, it might take months or even years for a harmed state to determine who attacked it.[235] Imagine the following scenario: a Russian hacktivist attacks the United States in January, but the United States is unable to identify its attacker until May. Under the Interpretive Guidance, the United States is out of luck. The United States would not be able to target the individual unless it could connect that same hacktivist to other direct participation attacks between January and April (an unlikely development given it took four months to connect the hacker to the first attack). If the attacks were made with enough frequency, the hacktivist may obtain "continuous combat function" and thus would be targetable.

Likely reacting to this impracticality, a few experts proposed that the period of participation should extend to when the enemy assesses damage to their system.[236] While that timeline makes more sense than the Interpretive Guidance, it also does not suffice. When a state assesses the damage to its system, it still may not know who caused that damage.[237] If a hacktivist is willing to attack at the level of direct participation, we have to believe they are likely to do it again. Thus, if we caught them in the act once, they should not be able to hide behind a veil of legalese. Furthermore, allowing hacktivists complete protection before we can even assess the culprit only incentivizes these "on the loose" cyber proxy relationships. The "on the loose" relationship is grounded in a lack of regulation and a lack of accountability. It is unreasonable to incentivize such an unstable and potentially chaotic structure.

Instead, a hacker's direct participation should continue for as long as the harmed foreign state reasonably believes that the hacker will attack again. If the state has reasonable belief the hacker is planning another attack, then the state may view the hacker as continuing to directly participate in the hostilities. In analyzing whether there is reasonable belief that the hacker will attack again, a state can look at the following factors: the severity of the initial attack, the political condition of the armed conflict, whether the hacktivist's host government took action against the hacktivist, whether the

231. INTERPRETIVE GUIDANCE, *supra* note 137, at 65.

232. *Id.* at 65, 67.

233. Brig. Gen. (ret.) David Wallace et al., *Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines*, 12 Harv. Nat'l Sec. J. 164, 194 (2021).

234. *Id.* at 195.

235. *See supra* note 41 and accompanying text; Neri Zilber, *The Rise of the Cyber Mercenaries*, FOREIGN POL'Y, Aug. 31, 2018 ("[T]he international nature of computer technology . . . makes it hard to ascertain the origin of a cyberattack. That lack of attribution then makes it harder for governments to respond, and the lack of a threat of reprisal makes deterrence difficult, if not impossible.").

236. TALLINN MANUAL, *supra* note 114, at 431.

237. *See* MCFATE, *supra* note 1, at 200 ("Russia has become a disinformation superpower, employing a 'kill 'em with confusion' strategy. And it's working. The evidence is everywhere: making a war in Ukraine invisible, hacking the 2016 US presidential election, stoking the Brexit vote, supporting fringe political groups . . . . Russia is now an empire of lies.").

host government condemned the original attack, whether the hacktivist has directly participated in hostilities at other times.

In reaction to this proposal, a skeptical reader might argue for a more literal interpretation of Additional Protocol I. The skeptic may point out that under this proposal, it is possible that a civilian who is *not* directly participating will be targeted. But isn't that always the case? The law of armed conflict can only expect a commander to look at the facts in front of him. If the total circumstances give the commander reasonable belief that a hacker will again directly participate, the commander should be able to take action. When civilians directly participate in an armed conflict, they must accept that they have opened themselves up to this analysis. Perhaps, this threat will even deter some civilians from entering the battlefield in the first place.

Notably, this proposed analysis would address another "important issue in the cyber context:" cyber operations often have "delayed effects."[238] The *Tallinn Manual* illustrates this phenomenon with the example of a "logic bomb designed to activate at some future point."[239] That "future point" could occur after a predetermined period, on the orders of a particular person, or upon the performance of a specific action by the target system.[240] The Interpretive Guidance experts split in how to determine the beginning and end of "direct participant" status in this situation.[241] The earlier proposal solves this dilemma as well. The hacktivist's direct participation would span until the targeted foreign state has identified the perpetrator and no longer has reasonable belief that the group will strike again. Because of the delayed effects and anonymization so easily employed in cyber, the law of armed conflict must adapt. Moreover, the law should not penalize a state that maintains strict regulations over its proxies, while rewarding one that lets them "loose." Playing this game of hide and seek—where hackers loosely connected to their governments can strike and then immediately hide behind legal status—punishes the regulated and rewards the chaotic.

CONCLUSION

As evidenced by the controversial Interpretive Guidance, experts struggle to apply the principle of distinction to states using proxies to carry out kinetic attacks. Cyber warfare merely complicates this already murky area.

After analyzing the principle of distinction as applied to various types of cyber proxies, this article proposes the following: (1) A cyber proxy that is organized, armed, belonging to a party to the conflict, and has directly participated in the conflict should be considered part of the armed forces. That group's personnel would thus be targetable based on their membership in the group. (2) The "for such time" element of direct participation should begin when a cyber proxy starts planning to commit an act of direct participation. The foreign state looking to target the cyber proxy must undertake that analysis on a good faith basis using the information it has at the time. (3) After directly participating in the conflict, a cyber proxy's direct participation status should continue

238. TALLINN MANUAL, *supra* note 114, at 431.
239. *Id.*
240. *Id.*
241. *Id.*

for as long as a harmed foreign state reasonably believes that the hacker will again directly participate in the conflict.

Scholars have long quarreled over whether mercenary figures are destined to be "dark and distasteful"[242] or whether they can maintain an "honorable albeit bloody trade."[243] There is, however, one way to ensure the worst—allowing these characters to roam through a gray legal landscape.

242. *See* PATTISON, *supra* note 5, at 3 (reviewing the controversial background of mercenaries).

243. *See* MCFATE, *supra* note 1, at 125 (arguing that mercenaries have unfairly garnered a bad reputation).