Summer 2014

The Civilian Cyber Battlefield: Non-State Cyber Operators' Status under the Law of Armed Conflict

Logan Liles

Follow this and additional works at: https://scholarship.law.unc.edu/ncilj

Recommended Citation
Available at: https://scholarship.law.unc.edu/ncilj/vol39/iss4/5

This Note is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of International Law by an authorized editor of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
The Civilian Cyber Battlefield: Non-State Cyber Operators' Status under the Law of Armed Conflict

Cover Page Footnote
International Law; Commercial Law; Law

This note is available in North Carolina Journal of International Law: https://scholarship.law.unc.edu/ncilj/vol39/iss4/
The Civilian Cyber Battlefield: Non-State Cyber Operators' Status Under the Law of Armed Conflict

LOGAN LILES†

I. Introduction .................................................. 1092
   A. Scenario One ............................................. 1093
   B. Scenario Two ............................................. 1094
   C. The Issue of Status ..................................... 1094

II. Combatant Status Architecture Under the Existing Law of Armed Conflict .......................... 1097
   A. The Law of Armed Conflict and Individuals’ Status 1097
   B. Lawful Combatants and Civilians ..................... 1098
   C. Prisoners of War ........................................ 1101
   D. Direct Participation in Hostilities .................. 1103
   E. Spies and Mercenaries ................................ 1105
      1. Spies ....................................................... 1105
      2. Mercenaries ............................................. 1106

III. The Dual Dimensions of Cyber Operations ................. 1108
   A. Physical Domain ......................................... 1109
   B. Systematic ................................................. 1109
   C. Questions Raised By the Dual-Dimensions About
      the Application of the LOAC ............................ 1110

IV. Contractors’ and Hacktivists’ Statuses Under the
    Existing Law of Armed Conflict ......................... 1111
   A. Hacktivists’ Status ..................................... 1112
   B. Contractors’ Status ..................................... 1115

V. Altering the Law of Armed Conflict to Ensure Non-
   State Cyber Operators Incur the Risks of Participating
   In Hostilities ................................................ 1117

VI. Conclusion .................................................. 1120

† B.A., University of North Carolina at Chapel Hill, 2009; J.D., University of North Carolina School of Law, 2014. Thank you to my family and friends, especially my mother and father, for their encouragements and support. Also, my deepest gratitude to the editors and staff of the North Carolina Journal of International Law & Commercial Regulation for their patience and insightful editing.
I. Introduction

“It is not just the fighters with weapons in their hands that pose a threat.”

Brigadier General Kenneth Watkins’ statement, made in the context of discussing an individual approach to determine combatant status, is equally applicable to cyber operations during interstate conflicts. The nature of cyber operations makes it likely that many combatants on cyber battlefields will be civilians. Hacking, writing code, and deploying viruses require a technical sophistication beyond the capabilities of the general public and regular soldier. Governments seeking to strengthen their cyber capabilities have and will rely heavily on civilian contractors. At the same time, to join the cyber fray, all an individual with specialized skills needs is a computer and an internet connection. As the events in Estonia in 2007 and Georgia in 2008 illustrate, nationalistic hackers without formal ties to a country’s armed forces are likely to be a major force on the cyber battlefield.

---


2 See Ellen Nakashima, Pentagon to Boost Cybersecurity Force, WASH. POST (Jan. 27, 2013), http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5f3ec-11e2-b05a-605528f6b712_story.html (detailing the Pentagon’s plans to expand the Cyber Command by 4,000 people, including civilians).


To date, the Russian cyber attacks on Georgia during the 2008 South Ossetia War represent the only instance of massive computer network attacks coinciding with an international armed conflict. But it will not be the last. Together, the increased use of cyber operations in interstate conflicts and the high likelihood of civilian cyber combatants pose a unique challenge to the law of armed conflict (LOAC). Commanders, soldiers, and judge advocates will have to apply the laws of war within the fog of war to completely novel situations. Consider two fictional but plausible scenarios that may arise in the near future.

A. Scenario One

Iran has declared war on the United States, Israel, the United Kingdom, and France for interfering with its “nuclear prerogative.” To halt global oil production, Iran has begun mining the Strait of Hormuz and harassing ships attempting to enter or exit the Persian Gulf.

In addition to mining the Strait of Hormuz, hackers sympathetic to Iran have attempted to access computer systems at the Pentagon, Whitehall, the Hôtel de Brienne, and various U.S. military bases located throughout the Middle East. The relationship between the Iranian Government and the hackers is unclear. Some of the most active hackers, though, use IP

---

5 Id. at 4–5.

6 See Leon E. Panetta, Secretary of Defense Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (“The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country.”). There has been significant debate over whether a purely cyber war will ever actually occur. Compare Richard A. Clarke, Cyber War: The Next Threat to National Security and What to Do About It (2010) (arguing that cyber war is how warfare will be conducted in the future), with Thomas Rid, Cyber War Will Not Take Place (2013) (contending that war will not take place, in the traditional sense, in the cyber realm. Instead, arguing that networks will be used to sabotage, subvert, and spy in ways that replace physical violence). However, this debate should not obscure the notion that future wars will likely involve overt acts in both physical and cyber space.

7 Throughout this Article, the phrase “law of armed conflict” (LOAC) is used interchangeably with the “law of war” and “international humanitarian law.” In all instances, these phrases refer to the body of customary and treaty-based law governing relations among States in armed conflicts.
addresses traced to Bandar Abbas, Iran.

To stop the mining of the Strait of Hormuz, units of the U.S. II Marine Expeditionary Force and the U.K. 3 Commando Brigade have raided Bandar Abbas. You are a lieutenant commanding one of the invading U.S. Marine Corps units. Your primary mission has been to occupy a small section of town and guard against counterattacks while other units permanently disable the port and mining facilities. During the operation, command has traced the same IP address used by the hackers to a building located in your area. You are ordered to take the building and halt the hackers.

On the way, your unit takes small arms fire. A few of your men are injured. At the hackers’ building, though, you encounter no resistance. Instead, you are able to approach quietly and survey what you presume to be the hacker’s room for a few seconds. There is a tangle of ethernet cables, power cords, and USB cables strewn about. Three young Persians in their late-teens to early-twenties share a long table at the far wall. They face away from you as they pound away on their laptops. Two wear headphones. Each is engrossed in their computer’s screen. None wear a uniform. There is a pistol on a table behind the hackers, but it is out of their reach. Your marines raise their weapons. Under the LOAC, though, may you legally open fire?

B. Scenario Two

To assert its right to access the Pacific Ocean, Bolivia has invaded Chile. During a counter-offensive, the Chilean Army captured seven Bolivian contractors as they retook Chilean territory. The contractors confess that Bolivia hired them to create and insert a virus into Chile’s air command systems to disrupt its operation. Even though they gained electronic access to the air command system, the contractors were captured before they could deploy the virus. From the evidence collected, the contractors worked with the Bolivian military but were not under military control. When captured, none of the contractors wore uniforms, but all carried Bolivian-issued identification cards.

You are a Chilean military judge presiding over the hearing to determine the Prisoner of War (POW) status of the seven captured Bolivians. If they are found not to be POWs, Chile will prosecute them as criminal hackers and, possibly, spies. Under the LOAC, are the contractors POWs?
C. The Issue of Status

Even though the two scenarios differ dramatically in terms of specifics, the answers regarding both hackers and contractors turn on the same legal determination: each individual’s status in an Article 2 interstate conflict. This Article applies the framework of international humanitarian law to these scenarios to identify and examine the problems practitioners may face in future international armed conflicts that involve cyber battles.

Contractors, hackers, and other cyber operators without formal connection to a State enjoy the privileges of combatants and civilians without incurring many of the risks each group faces. Simultaneously, they are able to participate in hostilities with minimal loss of their civilian protection and enjoy prisoner of war status due to both the preferences inherent in international humanitarian law’s status structure and the dual physical and systematic dimension in which cyber operations occur. This should not be allowed. Customary international law should require that States either objectively incorporate non-State cyber operators into their armed forces, or allow States to interpret “direct participation in hostilities” more leniently and drop the presumption of prisoner of war status for non-State cyber operators. Such a modification in the LOAC would ensure that non-State cyber operators do not use their status to flaunt the law and its consequences.

To accomplish this analysis, this Article adopts a simple organization. Part II examines the current structure the LOAC employs to determine an individual’s status and the preferences expressed by the law. Part III explores cyber warfare’s physical and systematic nature. Part IV applies the framework of the LOAC to the two scenarios listed above and identifies problems with such an application. Part V proposes a shift in interpretation of the LOAC in instances of cyber operations by non-State...
affiliated individuals to guarantee that non-State cyber operators do not exploit the gray area of unlawful combatancy. This Article concludes that States should either incorporate non-State cyber operators into their armed forces, or States should interpret “direct participation in hostilities” broadly enough to subject non-State cyber operators to the costs of taking up electronic arms.

Before delving into the status of non-State cyber operators, it is important to note two key assumptions of this Article. First, this Article assumes an interstate conflict exists outside of the cyber context. Making this assumption sharpens the Article in three ways. First, it settles any question about the conflict’s status, allowing the analysis to focus exclusively on the status of individuals. Second, assuming the existence of an Article 2 interstate conflict prevents veering into a tangential discussion about whether a cyber attack alone is sufficient to justify a legitimate use of force.9 Third, by expressly excluding consideration of Article 3 intrastate conflicts, there can be a deeper and more thorough analysis of the LOAC under Article 2.

Second, this Article assumes that the LOAC applies to the cyber context. This assumption comports with the opinion expressed by twenty international law scholars and practitioners in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.10

---


II. Combatant Status Architecture Under the Existing Law of Armed Conflict

A. The Law of Armed Conflict and Individuals' Status

The LOAC serves to maintain the standards of civilization despite the necessities of war. In other words, the LOAC attempts to limit the death and destruction inherent in warfare. To achieve this objective, the LOAC restricts who or what a belligerent may kill or destroy lawfully.

One essential way the LOAC constrains war's destructive power is through the creation of individual statuses. An individual's status dictates both one's rights and protections under the LOAC. Everyone in an armed conflict has a status because it is

[a] general principle which is embodied in all four Geneva Conventions of 1949. Every person in enemy hands must have some status under international law: he is either a prisoner of war and, as such, covered by the Third Convention, a civilian covered by the Fourth Convention, or again, a member of the medical personnel of the armed forces who is covered by the First Convention. There is no intermediate status; nobody in enemy hands can be outside the law.

Fundamentally, an individual's status answers two questions. First, whether or not an individual is a lawful military target. Second, whether, upon capture, the detaining force will hold an individual as a POW or prosecute him or her as a criminal. Further, an individual's status plays a significant part in the

---

12 Id. at 160–62.
13 A "belligerent" refers to a State or "power at war . . . protected by and subject to the laws of war." See WEBSTER'S STUDENTS DICTIONARY 75 (G. & C. Merriam Co., 1974).
14 Id.
16 JEAN S. PICTET, COMMENTARY: IV GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 51 (1958).
18 Id. at 28–30.
application of the LOAC’s core principles of distinction\(^\text{19}\) and proportionality.\(^\text{20}\)

B. Lawful Combatants and Civilians

The distinction between combatants and civilians provides the foundation of the LOAC status architecture.\(^\text{21}\) This distinction helps to cabin destructive force by guaranteeing that only the combatants of belligerent nations fight.\(^\text{22}\)

An individual who meets the requirements of lawful combatancy enjoys a bundle of rights known collectively as the “combatant’s privilege.”\(^\text{23}\) Central amongst the rights that make up the privilege is the right to engage in hostilities.\(^\text{24}\) Further, as long as a combatant’s actions comply with the LOAC, the privilege protects him from prosecution for engaging in violence.\(^\text{25}\) Upon capture, a lawful combatant is a prisoner of war (POW).\(^\text{26}\)

There are four categories of lawful combatancy: armed forces, partisans, unrecognized armed forces, and a levée en masse.\(^\text{27}\) With the exception of a levée en masse, lawful combatancy requires individuals to meet four conditions:

1. Command by a person responsible for his subordinates;
2. Having a fixed, distinctive sign recognizable at a distance;

---

\(^{19}\) See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Protocol I, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I]. “In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.” Id. art. 48, 1125 U.N.T.S. at 25 (emphasis added).

\(^{20}\) See Protocol I, supra note 18, arts. 51(5)(b), 57(2)(b), 1125 U.N.T.S. at 26, 29 (capturing the full definition of the concept of proportionality).

\(^{21}\) See DINSTEIN, supra note 17, at 27.

\(^{22}\) Id.


\(^{25}\) Berman, supra note 23, at 9–10.

\(^{26}\) See infra notes 50–72 and accompanying text.

3. Carrying arms openly; and
4. Conducting their operations in accordance with the laws and customs of war.\textsuperscript{28}

The first requirement ensures that individuals do not wage private wars against an enemy State.\textsuperscript{29} Requirements two and three distinguish combatants from civilians.\textsuperscript{30} The fourth requirement recognizes that to be a lawful combatant, a combatant must follow the LOAC.\textsuperscript{31}

Some commentators infer three more conditions for lawful combatancy from the four textual commitments.\textsuperscript{32} Under that approach, lawful combatancy also requires hierarchical organization, non-allegiance to the detaining party, and individual membership to a party to the conflict.\textsuperscript{33} State practice typically does not require the first two extra elements.\textsuperscript{34} Most practitioners concede that belonging to a party to the conflict is an implicit condition of lawful combatancy.\textsuperscript{35}

Even though treaties do not explicitly identify any conditions armed forces and unrecognized armed forces must meet to be lawful combatants,\textsuperscript{36} they still must meet the four conditions that apply to partisans.\textsuperscript{37} The law presumes that military units, by their very nature, will comply with those conditions.\textsuperscript{38}

The only category of lawful combatants that do not have to meet the four requirements for lawful combatancy is a \textit{levée en masse}, which represents a special category of combatants between civilians and members of the armed forces.\textsuperscript{39} A movement rarely

\textsuperscript{28} Geneva III POW, supra note 26, art. 4, 75 U.N.T.S. at 138.
\textsuperscript{29} DINSTEIN, supra note 17, at 37.
\textsuperscript{30} Id. at 37–38.
\textsuperscript{31} Id. at 39.
\textsuperscript{32} Id. at 39–41.
\textsuperscript{33} Id.
\textsuperscript{34} SOLIS, supra note 15, at 197–98.
\textsuperscript{35} Id. at 198.
\textsuperscript{37} DINSTEIN, supra note 17, at 36.
\textsuperscript{38} Id.
supports the determination that a *levée en masse* exists.\textsuperscript{40} The law defines it as when "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, provided they carry arms openly and respect the laws and customs of war."\textsuperscript{41} Treaties necessitate a *levée en masse* to be spontaneous and unorganized.\textsuperscript{42} Basically, the concept eliminates combatancy's requirement for organization and distinction when a belligerent nation invades another nation.\textsuperscript{43}

Anyone who does not fall within the four categories of lawful combatancy qualifies as a civilian.\textsuperscript{44} Thus, the LOAC defines civilians negatively.\textsuperscript{45} Further, the definition is over-inclusive because multiple participants in hostilities are classified as civilians. For example, mercenaries are civilians under this definition.\textsuperscript{46} Moreover, "in case of doubt whether a person is a civilian, that person shall be considered to be a civilian."\textsuperscript{47} The presumption of civilian status and the over-inclusive definition expresses the LOAC's preference for finding individuals to be civilians.

Civilians, like lawful combatants, enjoy a bevy of rights.\textsuperscript{48} Chief amongst the rights of civilians is a "general protection against dangers arising from military operations," including not being objects of attack.\textsuperscript{49}

\begin{itemize}
\item \textsuperscript{40} *Int'l Comm. of the Red Cross, Commentary: III Geneva Convention Relative to the Treatment of Prisoners of War* 57–58 (Jean S. Pictet ed., 1960) [hereinafter *Geneva III Commentary*].
\item \textsuperscript{41} *Geneva III POW*, *supra* note 27, art. 4(A)(6).
\item \textsuperscript{42} *Melzer, supra* note 39, at 840.
\item \textsuperscript{43} Compare *Geneva III POW*, *supra* note 28, art. 4(2), (setting out the requirements of combatancy), with id. art. 4(6), 75 U.N.T.S. at 138 (describing a *levée en masse*).
\item \textsuperscript{44} See Protocol I, *supra* note 19, art. 50(1), 1125 U.N.T.S. at 26.
\item \textsuperscript{45} *Id.*
\item \textsuperscript{46} See infra notes 108-123 and accompanying text.
\item \textsuperscript{47} Protocol I, *supra* note 19, art. 50(1), 1125 U.N.T.S. at 26.
\item \textsuperscript{49} Protocol I, *supra* note 19, art. 51(1)–(2), 1125 U.N.T.S. at 26.
\end{itemize}
C. Prisoners of War

Upon falling into the hands of the enemy, the LOAC entitles lawful combatants and a small, unique section of civilians to POW status.50 "[S]ubject to the condicio sine qua non that he is a lawful combatant[,]" every lawful combatant has an "[e]ntitlement to the status of prisoner of war—upon being captured by the enemy[.]"51 That is why four out of the six categories that Article 4 of the Geneva Convention on the Treatment of Prisoners of War—the core definition of prisoners of war—are the same as the four categories that define lawful combatants.52

Besides members of the armed forces,53 partisans,54 unrecognized armed forces,55 and a levée en masse,56 two non-combatant groups have a right to be POWs. First, non-combatant crewmembers, like merchant marine sailors or civilian aircraft pilots, qualify as POWs.57 This grant of POW status provides a minimum standard when they "do not benefit by more favourable treatment under any other provisions of international law."58

Second, POW status goes to persons accompanying the armed forces who are not members of the armed forces, such as war correspondents and supply contractors.59 The list of individuals is not exhaustive.60 Instead, any individual that accompanies the armed forces may receive POW status if he has authorization from the armed forces and an identity card indicating that

51 DINSTEIN, supra note 17, at 29.
53 Id. art. 4(A)(1), 75 U.N.T.S. at 138.
54 Id. art. 4(A)(2), 75 U.N.T.S. at 138.
55 See id. art. 4(A)(3), 75 U.N.T.S. at 138 (including those armed forces under a power "not recognized by the Detaining Power" or adverse country).
56 See id. art. 4(A)(6), 75 U.N.T.S. at 140 (including those who react to an invading enemy and "spontaneously take up arms to resist" before organizing themselves into customary military divisions).
57 See Geneva III POW, supra note 27, art. 4(A)(5), 75 U.N.T.S. at 140.
58 Id.
60 See GENEVA III COMMENTARY, supra note 40, at 42–43 (stating that service organizations, such as the International Committee of the Red Cross, are also included in the list of individuals granted POW status under art. 4(A)(4)).
authorization.\textsuperscript{61} The identification card serves the same function as a uniform: to distinguish those who deserve POW status from those who do not.\textsuperscript{62}

The LOAC expresses a preference for affording individuals POW status. Protocol I implies that even unlawful combatants receive protections equivalent to POW status.\textsuperscript{63} Further, there is a presumption that anyone who "falls into the power of an adverse Party shall be presumed to be a [POW]."\textsuperscript{64} If there is any dispute over whether or not an individual deserves POW status, a competent tribunal will decide.\textsuperscript{65} During the interim of a definitive determination, the individual enjoys the privileges of a POW.\textsuperscript{66}

POWs receive a number of protections and rights under the LOAC.\textsuperscript{67} These include the right to humane treatment,\textsuperscript{68} maintenance and medical care free of charge,\textsuperscript{69} and exemption from serving as slave labor.\textsuperscript{70} POWs also cannot be prosecuted for participating in hostilities.\textsuperscript{71} For example, a combatant cannot be prosecuted for murder for the deaths he caused during hostilities. This stems from the fact that the purpose of detaining combatants


\footnotesize{62} See \textit{Geneva III Commentary, supra} note 40, at 47 ("The identity card corresponds virtually to a soldier’s uniform or a partisan’s arm-band.").


\footnotesize{64} Protocol I, \textit{supra} note 19, art. 45(1), 1125 U.N.T.S. at 24.

\footnotesize{65} \textit{Id.}; Geneva III POW, \textit{supra} note 27, art. 5, 75 U.N.T.S. at 140-42.

\footnotesize{66} Protocol I, \textit{supra} note 19, art. 45(1), 1125 U.N.T.S. at 24; Geneva III POW, \textit{supra} note 28, art. 5, 75 U.N.T.S. at 140-42.

\footnotesize{67} See generally, Geneva III POW, \textit{supra} note 27 (detailing the basic protections afforded to all prisoners of war).


\footnotesize{69} \textit{Id.} art. 15, 75 U.N.T.S. at 148.

\footnotesize{70} \textit{Id.} arts. 49-57, 75 U.N.T.S. at 172-78.

\footnotesize{71} See Derek Jinks, \textit{The Declining Significance of POW Status}, 45 Harv. Int’l L.J. 367, 376 (2004) (explaining that prisoners of war are entitled to "combat immunity").
as POWs is to keep them out of the fight, not to punish them.  

D. Direct Participation in Hostilities

The last component of the status architecture of the LOAC deals with instances in which civilians join the fight. No general prohibition exists against civilians participating in combat; instead, the LOAC holds that when civilians take an active role in combat, they lose their protected status. Such individuals are neither lawful combatants nor civilians, but occupy the gray area between the two as "unlawful combatants." Lawful combatants may target such unlawful combatants within the parameters of the LOAC. In addition to losing civilian-status protections, unlawful combatants may face criminal liability and cannot claim the privilege of POW status upon capture.

Civilians, though, do not lose their status as such, "unless and for such time as they take a direct part in hostilities." A civilian is deemed to have participated directly in hostilities when three elements are satisfied:

1. [T]he act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm);
2. [T]here must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation);
3. [T]he 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 (belligerent nexus).

---

72 See Berman, supra note 23, at 9 ("The detention of combatants is not punishment, but rather, simply a way of putting combatants hors de combat for the duration of the conflict.").
73 DINSTEIN, supra note 17, at 27.
74 Id. at 29.
75 Id.
76 See, e.g., Ex Parte Quirin, 317 U.S. 1, 31–32 (1942).
78 NILS MELZER, INTERPRETATIVE GUIDANCE ON THE NOTION OF DIRECT
All three elements must be met for a civilian to lose his protected status.\textsuperscript{79}

The threshold of harm may be met either by adversely affecting military operations or by inflicting death or destruction on people or objects.\textsuperscript{80} The International Committee of the Red Cross (ICRC)\textsuperscript{81} found that "electronic interference with military computer networks" may satisfy the adversely affecting military prong of the threshold of harm element "whether through Computer Network Attacks (CNA) or Computer Network Exploitation (CNE), as well as wiretapping the adversary’s high command or transmitting tactical targeting information for an attack."\textsuperscript{82}

To meet the causation requirements, the harm "must be brought about in one causal step."\textsuperscript{83} This excludes an individual from directly participating in hostilities by contributing to the general war effort, such as building tanks; or performing war-sustaining activities, such as completing financial transactions.\textsuperscript{84} Direct causation requires the action to bring about the required harm.\textsuperscript{85} Causation may still exist despite a significant lag in time between the act and the harm or a significant amount of proximal space between the action and the harm.\textsuperscript{86}

The belligerent nexus requirement exists to tie the action to the hostilities between two nations.\textsuperscript{87} It prevents actions of civil unrest or the exercise of self-defense against members of a belligerent’s armed forces from depriving a civilian of his status.\textsuperscript{88} A belligerent nexus exists when "the conduct of a civilian, in conjunction with the circumstances prevailing at the relevant time

\begin{flushright}
\textsuperscript{79} \textit{Id.}
\textsuperscript{80} \textit{Id.} at 47–50.
\textsuperscript{81} The ICRC is a well-regarded corporate publicist. \textit{See SOLS, supra} note 15, at 19–20.
\textsuperscript{82} MELZER, supra note 78, at 48.
\textsuperscript{83} \textit{Id.} at 53.
\textsuperscript{84} \textit{Id.} at 51–52.
\textsuperscript{85} \textit{Id.} at 52.
\textsuperscript{86} \textit{Id.} at 55.
\textsuperscript{87} MELZER, supra note 78, at 58–59.
\textsuperscript{88} \textit{Id.} at 61–63.
\end{flushright}
and place, can reasonably be perceived as an act designed to support one party to the conflict by directly causing the required threshold of harm to another party.\textsuperscript{89}

A civilian that satisfies all three elements, and thus directly participates in hostilities, loses the protection given to civilians only for the duration of the specific qualifying act.\textsuperscript{90} Once the civilian ceases such an act, he regains the protections civilians enjoy.\textsuperscript{91} This stands in direct contrast with individuals who exercise a continuous combat function.\textsuperscript{92} Such individuals are always unlawful combatants and are, therefore, continually lawful targets for direct attack.\textsuperscript{93}

\textit{E. Spies and Mercenaries}

On top of this general framework, the LOAC overlays two unique categories: spies and mercenaries.\textsuperscript{94} If an individual’s actions qualify one as either a spy or mercenary, then the individual’s general status is negated, and the unique rules for those narrow categories apply. This section examines both special categories and the effect they have on an individual’s status.

\textit{1. Spies}

The LOAC permits spying.\textsuperscript{95} Civilians and lawful combatants alike can qualify as spies.\textsuperscript{96} To be a spy, three elements must be present. First, the person must act either clandestinely or under

\textsuperscript{89} Id. at 63–64.
\textsuperscript{90} Id. at 70.
\textsuperscript{91} Id.
\textsuperscript{92} See MELZER, \textit{supra} note 78, at 70–72.
\textsuperscript{93} Id. at 71–72.
\textsuperscript{94} See Protocol I, \textit{supra} note 19, arts. 46–47, 1125 U.N.T.S. at 24-25 (categorizing, describing, and distinguishing spies and mercenaries).
\textsuperscript{96} See Won Kidane, \textit{The Status of Private Military Contractors Under International Humanitarian Law}, 38 DENV. J. INT’L L. & POL’Y 361, 386–87 (2010) (stating the standard used to determine spying depends upon the manner used to collect information, not on the individual’s combatant status). C.f., DINSTEIN, \textit{supra} note 17, at 212 (noting that Article 46 of Protocol I is limited to members of the armed forces, while the Hague Convention relates to both soldiers and civilians).
false pretenses. A lawful combatant acts clandestinely, only if they do so out of uniform. Second, the individual “obtains or endeavors to obtain information in the zone of operations of a belligerent.” The “zone of operations” of a belligerent extends beyond the battlefield into areas controlled by a hostile State. At the same time, “[a] person stationed on his own State’s side of the front line—say, clandestinely monitoring or deciphering enemy radio signals—is not a spy. A spy must be located physically within an area controlled by the enemy.” Third, the individual obtaining the information must intend to communicate it to a party hostile to the belligerent.

Spying affects an individual’s POW status. Civilians and members of the armed forces caught spying do not have the right to be POWs. If caught, a spy may be punished criminally. National law, though, not the LOAC, criminalizes espionage. If a member of the armed forces, wearing his nation’s uniform, meets all of the criteria of spying, he is not a spy. Also, a member of the armed forces only loses his right to POW status if caught in the act of espionage. Otherwise, once he rejoins his unit, a member of the armed forces regains the right to be a prisoner of war.

2. Mercenaries

To qualify as a mercenary under Article 47 of Protocol I, an
individual must meet six specific criteria. First, an individual must be specially recruited to fight in an armed conflict. Second, the person must take a direct part in the hostilities. Third, an individual can be "neither a national of a Party to the conflict nor a resident of a territory occupied by a Party of the conflict." Fourth, a person cannot be a member of the armed forces of a party. Fifth, the individual who is a member of the armed forces of a State that is not a party to the armed conflict may not be sent there on official duty by its State. Sixth, to be a mercenary, an individual’s main motivation must be private gain. Specifically, the state hiring the person must in fact promise compensation, which must be "substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party . . . ." Protocol I provides flatly: "[a] mercenary shall not have the right to be a combatant or a prisoner of war." While mercenaries have been present on the battlefield for at least one thousand years, the flat prohibition on their participation stems only from efforts during the 1960s to stop Europeans and North Americans from profiting and participating in African struggles for independence. Absent the right to participate in hostilities, mercenaries are criminally liable for their actions and, upon capture, may be prosecuted. Despite the strength of the

108 Id. art. 47(2), 1125 U.N.T.S. at 25.
109 Id. art. 47(2)(a), 1125 U.N.T.S. at 25.
112 Id. art. 46(2)(e), 1125 U.N.T.S. at 25.
113 Id. art. 46(2)(f), 1125 U.N.T.S. at 25.
114 Id. art. 46(2)(c), 1125 U.N.T.S. at 25.
115 Id.
118 DINSTEIN, supra note 17, at 52.
international consensus against mercenaries, the United States specifically objects to including it as customary international law because it introduces political factors into the LOAC.120

The prohibition on mercenaries is extremely narrow because all six requirements must be met. Foreign nationals directly incorporated in armed forces—like the French Foreign Legion—foreign advisors, and military technicians, fall outside of the strict definition of mercenaries.121 Countries can subvert the strictures of Article 47 simply by incorporating mercenaries directly into their armed forces.122

III. The Dual Dimensions of Cyber Operations

Cyber operations are unique when compared to their nautical, aerial, and terrestrial counterparts. Unlike the other three, which occur only within the physical environment, cyber actions take place both in the physical and systematic world. Cyber actions’ dual nature complicates attempts to apply the LOAC to determine the individual status of hacktivists and computer contractors. Specifically, it raises two fundamental questions that, regardless of their resolution, permit the preferences inherent in the LOAC to influence strongly the determination of a hacktivist or computer contractor’s status. Using the Stuxnet Virus that destroyed Iran’s uranium enriching centrifuges as an example, this section explains both the physical and systemic dimension of cyber operations and how it complicates application of the LOAC.


120 See Matheson, supra note 63, at 426.


122 DINSTEIN, supra note 17, at 51.

123 Id. at 51–52.

124 A combination of “hack (in the computer sense)” and “activism[,]” the term “Hacktivism” can be defined as “the practice of gaining unauthorized access to a computer system and carrying out various disruptive actions as a means of achieving political or social goals[.]” Hacktivism, DICTIONARY.COM, http://dictionary.reference.com/browse/hacktivism (last visited Feb. 8, 2014).
A. Physical Domain

Clearly, people conduct cyber operations in the physical dimension. The "physical" dimension, for purposes of this Article, means the tangible world where physics, biology, and chemistry govern the battlefield. Created by the forces of nature, the physical domain is where flesh and blood meet keyboard and ethernet cables. The individual creating cyber weapons operates, and the ultimate effect of those weapons occurs, within the physical world. At its most basic, cyber action in the physical domain is the interaction of people and the natural world with computers. The Stuxnet Virus illustrates cyber operations' physical dimension in three specific ways. First, when individuals sitting at computers created the Stuxnet Virus, they acted in the physical environment. Second, when a few individuals pushed thumb drives into USB ports on various Iranian computers, they conducted cyber operations in the physical realm. Third, cyber operations occurred in the physical world when the virus sped up the uranium enriching centrifuges to the point that they shattered.

B. Systematic

In addition to the physical world, cyber actions also transpire in the systematic world. The "systematic" environment, for purposes of this Article, is the network of computers linked together and sustained through self-automation. Processing power, memory, algorithms, and the rules of computer science govern this battlefield. An actual ethernet cable is not part of the systematic environment, but the information and lines of code traveling through it are integral elements. When information breaches a firewall, an actual wall is not penetrated. Instead, breach of a firewall happens when malicious information packets gain access to the defended computer despite the security program. The launching of a virus and its interaction with, and effect on, other computer systems define cyber operation in the systematic

---


126 See id. (indicating that a "new propagation mechanism" of Stuxnet was "the ability to spread seamlessly and invisibly via USB sticks").

127 Id.
dimension. Reduced to its most basic idea, cyber action in the systematic environment is the interaction of computers with other computers.

Events surrounding the Stuxnet Virus demonstrate the systematic dimension of cyber action. After someone inserted the memory stick into a computer, the virus’s insertion of itself within the code of the computer happened in the systematic world.\(^\text{128}\) When the virus sent commands to the controller to alter the speed of the centrifuges, the cyber action took place in the systematic environment.\(^\text{129}\) Cyber operations occurred in the systematic world when the virus spread, through inter-connected systems, to infect computers in India, Indonesia, Europe, and the United States.\(^\text{130}\)

C. Questions Raised By the Dual-Dimensions About the Application of the LOAC

Cyber operations’ dual dimensions make applying the LOAC to determine an individual’s status more complicated. Specifically, they interject two fundamental, intertwined questions about applying the LOAC to cyber operatives.\(^\text{131}\) First, must an individual meet the requirements of a status both in the physical and systematic dimensions? The requirement of distinction demonstrates the implications of this question. If an individual must meet the elements of a particular status in both dimensions, then to qualify as a member of a militia, one would have to distinguish oneself in both worlds. Basically, requiring an individual to adhere to the requirements in both domains doubles the necessary elements one must fulfill to obtain a specific status.

If a person does not have to satisfy the elements of a status in both dimensions, then a second question arises: can evidence from either domain satisfy the requirements of a particular status? Rejecting the need to fulfill the elements in both spheres implicitly considers what evidence is sufficient to determine status. By applying the LOAC in other contexts, it is indisputable that actions

\(^{128}\) Id.

\(^{129}\) Id.

\(^{130}\) See Gross, supra note 125 (indicating that the virus has been found in India, Indonesia, Europe, and the United States).

\(^{131}\) Attempts to answer these questions are beyond the scope of this Article.
in the physical world may justify particular statuses. The practical question thus becomes: can actions in the systematic environment alone satisfy a status element? For example, can malicious code in a Georgian computer system with lines of codes identifying the code's source as Russian, alone fulfill the belligerent nexus requirement of direct participation in hostilities? If such cyber operations in the systematic environment can satisfy status requirements, then the universe of possible evidence doubles. If actions in the systematic world cannot meet the elements for a particular status, then there must be a case-by-case determination of whether the cyber action took place in the physical or systematic dimension. Either answer complicates the application of the LOAC either by expanding the universe of proof or by requiring a distinction in each case between actions occurring in the physical and systematic environments before analyzing status questions.

Regardless of the specific answer to either of these two questions, cyber action's physical and systematic nature complicates status analysis under the LOAC. Those complications create a space in which the preferences inherent in the law can have a determinative influence on status determinations. In situations that are not clear-cut, the added difficulty of cyber operations' dual dimensions makes a status determination even less clear. To navigate such situations, decision makers will rely heavily on the preferences inherent in the LOAC. Thus, in deciding the close case of whether a hacker is a POW or criminal, he will likely be classified as a POW due to the LOAC's preference for affording such a status.\textsuperscript{132}

IV. Contractors' and Hacktivists' Statuses Under the Existing Law of Armed Conflict

Applying the LOAC to specific situations illustrates that the status structure and dual environment of cyber conflicts permit non-State cyber operators to enjoy all the benefits of various statuses while avoiding the risks. This section elucidates this idea by applying the LOAC to answer the questions posed in the two scenarios above.\textsuperscript{133}

\textsuperscript{132} See supra Part II.B.

\textsuperscript{133} See supra Part I.A-B.
A. Hacktivists’ Status

To determine whether the U.S. Marines may lawfully target the Iranian hackers, a Marine would have to go through a two-step process. First, the Marine Lieutenant must decide whether the Iranian hacktivists fit within one of the four categories of lawful combatants. If not, the Marine Lieutenant then decides whether the Iranian hacktivists have committed an act that qualifies as directly participating in hostilities, so as to forfeit their civilian protection from targeting.

The Iranian hackers are not partisans nor members of a recognized or unrecognized armed force because they do not meet the four explicit requirements of lawful combatancy. As Iranians, they are citizens of a party to the conflict. Beyond that, they fail the four formal requirements of lawful combatancy. First, there is no commander responsible for his subordinates. Second, none of the men are uniformed nor in any manner distinguish themselves from civilians. Third, even though there is a gun, none of the individuals are openly carrying weapons. Some may argue that, in this instance, the hacker’s weapon is their personal computer. But computers themselves are not inherently weapons. Only a person’s technical skills transform computers into arms. Finally, since they lack a commander, the Iranian hackers do not comply with the customary LOAC.

Cyber operations’ dual natures make it difficult for non-State cyber operators to meet the requirements of lawful combatancy. Cyber weapons, by their nature, are covert and concealed. It seems impossible for a hacktivist to carry a weapon openly, either in the systematic or physical environment. Even if they could, to do so would negate some of cyber warfare’s advantages. Most hackers will be unable to satisfy the responsible commander requirement because most hacking organizations lack hierarchical organization. Distinction is difficult for non-State cyber operators. The members of a group of hacktivists will not have a physically distinctive indicator because they, most likely, only

---

operate online. Further, in the systematic environment, specific lines of code will likely distinguish groups. Since anyone who knows about that code can copy it, it seems easy for imitators to connect certain groups to certain actions simply by inserting their unique identifying code into that attack. Thus, it is difficult to consider something a distinguishing indicator when it cannot be connected definitely to a unique group of people.

Additionally, the Iranian hackers do not satisfy the definition of a levée en masse. Their cyber activities happened before the Americans and British invaded, not after the approach of enemy belligerents. More broadly, it is difficult to maintain that hackers are defending their physical homeland by attacking the systematic homeland of an adversary. Also, the development and deployment of cyber weapons take time. The planning needed to launch a cyber attack runs counter to a levée en masse’s spontaneity requirement.

Since the Iranian hackers are not lawful combatants, they must fall within the LOAC’s broad definition of civilians. Despite their hostile actions, the LOAC’s preference to consider individuals to be civilians will decisively label the Iranian hackers as civilians. Therefore, whether they may be lawfully targeted depends on whether, because they directly participated in hostilities, they are stripped of their protections from attack.

Scholars recognize a spectrum of cyber actions that may qualify as direct participation in hostilities. On one end of the spectrum, general research into the development of cyber weapons does not qualify as direct participation in hostilities. On the other, there is direct participation in hostilities when a civilian directly enters the commands necessary to commence a cyber action. The tipping point between the civilian retaining his protection and losing it comes when planting a malicious agent that does not immediately cause damage but may do so subsequently. Most cyber actions do not qualify a civilian as

---

135 Id.
137 Id. at 295.
138 Id.
139 Id.
directly participating in hostilities.\textsuperscript{140}

In the case of the Iranian hackers, their actions likely satisfy the harm element but fail to meet the elements of direct causation and belligerent nexus. As Interpretative Guidance\textsuperscript{141} recognizes, cyber attacks, including attempted cyber network exploitation—akin to what the Iranian hackers attempted—meet the threshold of harm.\textsuperscript{142} Showing that the Iranian hackers directly participated in hostilities is difficult because of the strict requirements of direct causation and a belligerent nexus. Direct causation is difficult to prove because it requires only one step from the three individuals typing in the building to the cyber attacks on the various defense networks. The connection between a civilian’s actions and a cyber action takes far more steps than direct causation allows. Also, this example lacks the required belligerent nexus. While it may have caused the threshold of harm to the Americans, French, and English, the connection to the Iranian hackers aiding the Iranians is unclear.

Even if the Iranian hackers meet the elements of direct participation for the previous hacks, after ceasing those cyber attacks, the hackers would once again become civilians. Direct participation in hostilities allows for targeting while individuals directly participate in hostilities. As soon as they stop participating, civilians regain their immunity from attack.\textsuperscript{143} Accordingly, the Iranian hackers in this example are not targetable because they are no longer directly participating in hostilities by hacking into foreign defense departments.

The dual nature of cyber operations greatly hampers assessment of whether a civilian directly participated in hostilities. Since cyber weapons can sit dormant in the systematic realm for long periods of time, it is hard to assess the time frame in which a non-State cyber operator actually participates in hostilities and, therefore, becomes a viable target in the physical world. Also, it is philosophically challenging to maintain that a non-State cyber actor’s systematic actions somehow benefit a specific belligerent in a confrontation in the physical world. Finally, the single-step

\textsuperscript{140} Id.
\textsuperscript{141} See MELZER, supra note 78, at 46.
\textsuperscript{142} See supra notes 79-93 and accompanying text.
\textsuperscript{143} See supra Part II.B.
causation requirement excludes more complex cyber actions, which require more indirect causal actions in the systematic environment, from supporting the conclusion that a hacktivist directly participated in hostilities.

Since the dual dimensions of cyber actions complicates showing that an individual was either a lawful or unlawful combatant, the LOAC’s preference for civilians will make the Iranian hackers unlawful targets. Even though, in this scenario, hacktivists sympathetic to one belligerent have conducted cyber operations against its enemies as if they were combatants, they would retain their civilian protection from lawful targeting.

B. Contractors’ Status

The Chilean judge would go through a two-step process to determine whether the Bolivian contractors are POWs or civilians subject to criminal liability. First, the judge would decide whether the contractors fit within any of the six categories affording POW status under the LOAC. If so, the judge next would determine if their actions placed them in a unique status, like mercenaries or spies, which would strip them of POW status. From capture until the judge reached a decision, the LOAC presumes the Bolivian contractors to be POWs. Accordingly, the Chileans detaining the Bolivian contractors must treat them as POWs.

Although, arguably, they may fulfill more of the requirements, the Bolivian contractors, like the Iranian hackers, are not lawful combatants. For the reasons discussed above, non-state cyber operators will find it difficult to meet the requirements of combatancy. Conceivably, cyber contractors have a better shot at fulfilling the elements than their hacker counterparts. A proponent of such a status may argue that a manager responsible for his employees’ actions equates a responsible commander. Still, contractors working on cyber operations will face the same difficulties that the hackers encountered with distinction and openly carrying a weapon.

The Bolivian contractors are not part of a levée en masse or non-combatant transportation crews. Their country was the invading nation, so the category, meant only for invaded countries,

---

144 See supra Part IV.A.
does not provide the Bolivian contractors with POW status. They do not qualify for POW status as members of non-combatant transportation crews. They are computer specialists, not drivers or pilots.

Under the LOAC, the Bolivian contractors likely deserve POW status because they are individuals accompanying an armed force and carry identification cards issued by the Bolivian Armed Forces. In other situations, though, the dual nature of cyber operations may stretch this notion to its limits. An armed force may credential cyber contractors that do not physically accompany the military. Instead, the contractors may be thousands of miles away conducting systematic actions that affect the physical locale the armed force occupies. If an opposing belligerent captured those remote computer contractors, it is debatable whether they would qualify as POWs under this provision.

Due to the narrow definitions of spies and mercenaries, in conjunction with the dual environment in which cyber operators work, the Bolivian contractors would retain their POW status. The Bolivian contractors are not spies because they were attempting to disrupt an air command system; they were not trying to obtain information and translate it back to a hostile party. Conceivably, any cyber action could meet the requirement for participating in a clandestine act or acting under false pretenses because all cyber actions in the systemic dimension are clandestine. This is true regardless of whether those actions are covert in the physical domain. Further, it is debatable whether a belligerent’s “zone of operation” extends from the physical environment into the systematic. Supporting that conclusion is the idea that a State controls cyber space by providing the infrastructure supporting it. But just because the belligerent controls it does not mean the alleged spy had to invade that space to obtain the information. Thus, similar to someone monitoring enemy radio signals, cyber contractors may never physically invade a zone of operation.

The Bolivian contractors are not mercenaries because they are

145 See supra Part II.C (discussing POW status).
146 Id.
147 Id.
148 See supra notes 108-123 and accompanying text.
citizens of one of the belligerent parties and were not recruited to fight in the conflict.\textsuperscript{149} Cyber operations’ systematic and physical dimensions test whether cyber contractors can be considered mercenaries. Specifically, it questions whether someone hired to conduct specific operations in systematic space was recruited specifically to fight. Ultimately, the Bolivian cyber contractors fail to implicate the narrow definitions of mercenaries or spies that would strip them of their POW status.\textsuperscript{150}

Despite taking part in hostilities as unlawful combatants by creating and attempting to employ a virus that would have had adverse military effect on an enemy party, the Bolivian contractors will enjoy POW status.

V. Altering the Law of Armed Conflict to Ensure Non-State Cyber Operators Incur the Risks of Participating In Hostilities

Presently, under the LOAC, both hackers and contractors that participate in hostilities enjoy protections, such as POW status, without incurring risks, such as continuously being a lawful target. The LOAC should not allow hackers and cyber contractors to exploit this gray area of unlawful combatancy easily and with impunity.

To address this problem, the present LOAC must be altered specifically for non-State cyber operators. States should be offered a choice: incorporate hackers and cyber contractors into their armed forces or force hackers to accept a more lenient application of the direct participation in hostilities standard and discard any presumption of POW status.

Specifically, the direct participation in hostilities standard would be relaxed across the board. For non-State cyber operators, the threshold of harm would be met if a member of a country’s military had to act, in any manner, in response to a cyber action. Thus, it is enough to “likely adversely effect military operations” if a member of the armed forces had to, or will have to, spend time addressing a threat.\textsuperscript{151} With direct causation, the requirement for

\textsuperscript{149} See supra Part II.E.2 (discussing mercenary status).

\textsuperscript{150} See supra Part II.E (discussing spy and mercenary status).

\textsuperscript{151} See supra Part II.D (discussing the “direct participation in hostilities” requirement of combatancy). See Protocol I, supra note 19, art. 75, 1125 U.N.T.S. at 37-
non-State cyber actors will be lowered so that any causation, whether in the systematic or physical domain, is enough to satisfy the element. For example, the requirement would be met if a hacker-created virus infiltrated a firewall. As for the belligerent nexus, non-State cyber operators will fulfill the requirement as long as, in addition to meeting the threshold of harm to one belligerent nation, some articulable connection exists between the hackers and the benefited belligerent. Thus, the fact that the hackers in the first scenario were Iranian would be enough to satisfy the belligerent nexus.

Further, non-State cyber operators will lose the presumption that they are POWs. While still entitled to the general protections of Article 75 of Protocol I, the burden will be on non-State cyber operators to show from the start that they deserve POW status.

This approach ensures that non-State cyber operators cannot abuse the ambiguity of unlawful combatancy without facing consequences. They must either become lawful combatants as members of a nation’s armed forces or continue as unlawful combatants that face the same consequences of foregoing their civilian protection. Forcing non-State cyber actors into the Armed Forces will make them constantly lawful targets but give them POW status. Otherwise, non-State cyber actors will have to deal with always being lawful targets and facing possible criminal liability upon capture.

Also, this approach promotes the LOAC. If a State incorporates cyber operators into their armed forces, those individuals must follow the LOAC. This approach incentivizes incorporation of non-State cyber operators. It may be best understood as rewarding those that follow the LOAC with a guarantee of POW status. By depriving non-adherents of civilian protection from targeting and the presumption of POW status, this approach at least disincentivizes non-compliance with the LOAC.

There are at least two shortcomings to this approach. First, it would expand the number of individuals who lawfully could be

38 (providing the fundamental rights and minimum standards of humane treatment guaranteed to those persons not afforded more favorable treatment under the Geneva Conventions or under Protocol I).

152 See Protocol I, supra note 19, art. 75, 1125 U.N.T.S. at 37-38.
killed. Relaxation of the requirements of direct participation in hostilities would mean more individuals would fall into the category and thus become lawful targets. Increasing the number of individuals who could be targeted legally runs counter to the LOAC’s purpose of constraining the impact and scope of hostilities.

Second, loosely interpreting direct participation in hostilities to allow targeting of hackers and contractors creates a slippery slope. Once the stringency of the direct participation requirements are relaxed for hackers and contractors, nations may be quicker to relax the same rules for other disfavored groups. This process could repeat itself until there were no meaningful distinctions between civilians and lawful combatants and either could be killed freely.

As to the first criticism, the alteration will do more to advance the purposes of the LOAC than to subvert it. Admittedly, in the aggregate, a few more individuals will become lawful targets than previously. At the same time, though, the LOAC will likely be applied more broadly. When nations incorporate hackers and contractors into their armed forces, they will require them, in their operations, to follow the LOAC. Even if nations do not incorporate hackers and contractors into their armed forces, nations seeking to target those individuals will still have to go through the same legal analysis. Rules of proportionality and military necessity will still constrain targeting the hackers. Ultimately, allowing the possibility of armed forces to target a few more individuals within the strictures of the LOAC has to take precedent over permitting contractors and hackers to inflict military harm outside the strictures of the LOAC.

As to the second criticism, a deep descent down a predicted slippery slope misunderstands how nations create international law and would represent a striking reversal of the recent trend in the LOAC. Treaties or customary international practice create the LOAC. Writing treaties and transforming customary international law takes a significant amount of time. It is naïve

154 See, e.g., Michael P. Scharf, Seizing the “Grotian Moment:” Accelerating Formation of Customary International Law, 43 CORNELL INT’L L.J. 439, 446 (2010) (“[T]he process of establishing customary international law can take decades or even
to think this minor alteration in the LOAC would lead to a quick descent into lawless wars. Further, such a decline would represent an astonishing reversal in the recent trend of international law. Since the end of World War II, nations, through international law, have attempted to give civilians greater protection from the destruction of war. Due to both of these facts, it seems unlikely that a slight expansion of direct participation in hostilities for cyber contractors and hacktivists would cause a broader breakdown in the civilian-combatant distinction.

Objections aside, the LOAC must be modified to prevent non-State cyber operators from exploiting the gray area of unlawful combatancy. To accomplish this objective, States should have the option of making non-State cyber operators into State cyber operators by incorporating them into their armed forces or letting those individuals face a more lenient standard for direct participation in hostilities and loss of the presumption of POW status.

**VI. Conclusion**

As cyber warfare increases, non-State cyber operators like civilian contractors and hacktivists will play a larger and larger role in combat. Their presence on the battlefield poses unique challenges to applying the LOAC. The LOAC has a preference for civilian and POW statuses. Along with those specific statuses come protections from targeting and immunity from criminal prosecution. Cyber operations, unlike their nautical, aerial, or terrestrial counterparts, happen in the physical and systemic environments.

These two factors together, the LOAC’s preferences and the dual dimensions in which cyber operations occur, allow non-State cyber operators to enjoy the best of both status worlds. As civilians that enjoy protection from direct attack, they may fight without forfeiting their status due to the difficulty of proving direct

centuries").

155 *See* Aaron Xavier Fellmeth, *Questioning Civilian Immunity*, 43 TEX. INT’L J. 453, 455–57 (2008) (explaining that international law has attempted to limit civilian deaths and property damage related to war but has done an extremely poor job at actually achieving that goal).

156 *See supra* Part II.B.
participation in hostilities. If captured, non-State cyber operators may claim POW status and enjoy immunity from prosecution despite being unlawful combatants. The LOAC must prevent hacktivists and cyber contractors from occupying the gray area of unlawful combatancy by making the law more black and white. States should be given a choice: either directly incorporate them into armed forces or apply to those individuals a broader interpretation of direct participation in hostilities, effectively eliminating the presumption of POW status. This new approach is necessary to ensure that non-State cyber operators face the same risks as other unlawful combatants.