IHL Targeting in Cyberspace: A Hypothetical Case

Terence Check

Terence Check is an attorney and is an LL.M candidate at American University Washington College of Law, specializing in National Security Law and Policy. He graduated magna cum laude in 2014 from Cleveland Marshall College of Law in Cleveland, Ohio, and was Editor-in-Chief of Cleveland State Law Review. He currently lives in Washington, D.C.

Abstract

Cyber-attacks are no longer the stuff of science fiction. Now that cyberweapons have the capability to go kinetic, much of the difficult legal analysis relating to cyberwarfare begins to clear: the physical effects of Stuxnet allow legal scholars to elucidate the evidentiary problem inherent in previous cyberwarfare discussions. This analysis reveals that the permissible list of targets for cyberattacks may be far larger than what would be possible in a traditional conventional armed conflict.

Introduction

Cyber-attacks are no longer the stuff of science fiction. In fact, their use as an instrument of state policy has grown significantly in the past few years. For example, the People’s Republic of China has a top-secret military component known as “Unit 61398” which has “a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.” But cyberattacks have been used for more than mere espionage. The Stuxnet virus, allegedly a product of the United States, was able to destroy dozens of nuclear centrifuges at a nuclear plant in Natanz, Iran. The Stuxnet virus marked a sea change for the discussion of “cyberwarfare” because the physical damage caused by Stuxnet was “not characteristic of most cyber operations.” Now that cyberweapons have the capability to go kinetic, much of the difficult legal analysis relating to cyberwarfare begins to clear: the physical effects of Stuxnet
allow legal scholars to elucidate the evidentiary problem inherent in previous cyberwarfare discussions.\(^5\)

Such a development could not come at a more critical time, as public concern has begun to grow regarding the cyber-security of critical infrastructure.\(^6\) In an age where by “‘using public sources openly and without resorting to illegal means’ . . . it is possible to gather at least 80\% of the information needed to carry out a highly disruptive attack on an infrastructure system”, such public concern is well-placed.\(^7\) And with critical infrastructure defined domestically as “systems and assets . . . so vital to the United States that [their] incapacity or destruction . . . would have a debilitating impact on security,”\(^8\) there is a possibility that components of infrastructure—which are already vulnerable to malware like Stuxnet—could become permissible military targets during an armed conflict. In response to this growing trend, there is an uncomfortable question—in a war where cyberspace is militarized, what is a permissible target under international humanitarian law (IHL)? That is, what sorts of buildings, infrastructure, and information systems may be attacked with a cyberweapon during a period of armed conflict? Are there rules that govern these sorts of questions, and how well do the rules apply to current and potential future scenarios? To briefly foreshadow, this analysis reveals that the permissible list of targets may be far larger than what would be possible in a traditional conventional armed conflict. The article contends that this expansion of the battlefield should prompt jurists, scholars, and policymakers to revisit fundamental assumptions about IHL, targeting, and the scope of civilian protections.

This article folds out in the following parts. After this introduction, Part 1 briefly sets forth the relevant international humanitarian law, including some jus ad bellum provisions. Additionally, Part 1 also reviews the Rome
Statute of the International Criminal Court, in particular, the definition of war crimes and crimes against humanity. Part 2 applies principles of international law to a sample scenario created by the author. In particular, Part 2 will look at major targeting issues, and will consider whether the facts of cyberwar, as a general matter, may necessitate changes to the interpretations of international humanitarian law. Part 3 concludes with some ruminations on the future of international humanitarian law, targeting, and individual criminal responsibility in an age of cyberwarfare.

1. Legal Principles

This section surveys major provisions of international humanitarian law as they relate to the question of targeting. Generally speaking, a targeting analysis falls within the confines of *jus in bello*—the law of war governing what states can do during an armed conflict—rather than *jus ad bellum*, which governs when states may resort to armed force. As a result, there are several threshold questions that precede a targeting analysis. These threshold questions, the legal principles governing targeting, and the Rome Statute are all discussed below.

Before turning to *jus in bello*, one must first classify the type of conflict. Generally speaking, the “law of peace,” or international human rights law, governs the conduct of states. Furthermore, states are prohibited from using “force” in the conduct of their affairs unless one of a few exceptions applies. One such exception, codified in Article 51 of the United Nations Charter, allows states to use force in self-defense “if an armed attack occurs.” For this article, international law defines “armed attack” as sending of armed forces (whether regular military or less-formal groups) across an international border, but mere assistance or provision of support alone does not constitute an armed attack. The contours of an “armed attack” as a legal concept are in flux, and it is not yet clear what an armed attack looks like or who can even commit an armed attack.

But once an armed attack occurs, the question of whether states can respond with armed force depends on whether the armed attack creates or is part of an armed conflict. In theory, an International Armed Conflict
(IAC) arises whenever one state directs armed force against another state. As a practical matter, not every use of armed force triggers an armed conflict, as not every exchange of arms results in an all-out war. For conflicts that involve at least one non-state group—non-international armed conflicts (NIACs)—the status of an armed conflict depends on whether the non-state group meets a minimum level of organization and whether the conflict as a whole meets a minimum threshold of intensity. Once an armed conflict is underway, it is only then that the law of peace makes way for jus in bello—the law of war.

IHL principally consists of the four Geneva Conventions, the two Additional Protocols to the Geneva Conventions, customary international law, and a growing body of international criminal jurisprudence. Together, these provisions provide many specific rules governing the conduct of states during armed conflict, ranging from prohibiting the use of perfidy, targeting medical personnel to honoring the neutrality of third-parties to the conflict. Their use regulates the conduct of states and, to a certain extent, non-state actors, providing fundamental protections for persons not a party to the armed conflict, and determines who can be the permissible target of lethal force.

Permissible targets of lethal force are narrowly limited to the following categories: combatants, civilians that are directly participating in hostilities (DPHers) or civilians that serve a continuous combat function (CCFers), military objectives, and a permissible amount of collateral damage. Combatants are those individuals who are either members of the armed forces of a belligerent party or those individuals that take the orders of a commanding officer, carry arms openly, wear a distinctive emblem or symbol identifiable at a distance, and comply with the laws of war in the course of their operations. Combatants enjoy the “combatant’s privilege,” which prevents the prosecution of combatants for their acts of violence or property damage lawfully committed during active hostilities and entitles them to prisoner-of-war status upon capture.

Additionally, while civilians are generally protected from targeting, those civilians that directly participate in hostilities are targetable for such time
as they are directly participating. Direct participation requires that the civilians directly participate; the conduct must meet a minimum threshold of harm. Furthermore, the civilian’s conduct must have a nexus to the hostilities as a whole. While there is some dispute, customary international law typically holds that ambiguous cases should be resolved in favor of finding non-combatant status so if it is unclear whether or not the civilian’s conduct constitutes directly participating in hostilities, the state should refrain from targeting that civilian.

For those civilians whose involvement in hostilities is so pervasive that they serve a continuous combat function (CCF), they can be targeted at any time they are members of a belligerent force, in contrast to the general rule allowing targeting of DPHers for only the time that they are fighting. The ICRC notes that determining when a CCFer disengages from that continuous combat function is a matter that depends more on political and cultural contexts rather than legal criteria. Additionally, warring parties can also target military objectives, which are defined in Article 52 of Additional Protocol I as: “those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.” It is important to note that warring parties may target military objectives even if it results in collateral damage, so long as the damage is not excessive to the military benefit to be gained. Generally speaking, these individuals and objectives are targetable only on the battlefield, which is the entire territory of the states that are parties to the conflict. The development of unconventional warfare has begun to challenge this conception.

Once a warring party determines that a target falls within a permissible category, additional principles, namely the principles of necessity, proportionality, distinction, and humanity apply to operations taken against that target. Necessity under jus in bello is broad and flexible: any operation that is not otherwise forbidden under international law that is “indispensable for securing the complete submission of the enemy”, is permissible.
Proportionality requires that any incidental loss of civilian life and civilian objects cannot be excessive to the military objective to be gained.\textsuperscript{33} Thus, any act that is \textit{expected} to result in an excessive loss of life is impermissible under Additional Protocol I, and, by extension, customary international law.\textsuperscript{34} Distinction has been implicitly dealt with above: it requires warring parties to distinguish between lawful and unlawful targets (between military and protected objectives).\textsuperscript{35} Importantly, not all operations directed at protected civilian populations are forbidden—psychological and propaganda operations, for example, are allowed under IHL, it is only when those operations rise to the level of an armed attack that the principle of distinction forbids the targeting of civilians.\textsuperscript{36} Furthermore, IHL does not strictly require the use of the most-discriminatory means available, as the Additional Protocols require the taking of “all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life [and civilian injury].\textsuperscript{37} Humanity requires the prevention of unnecessary suffering once a military benefit has been achieved.\textsuperscript{38} This principle forbids the use of devices ranging from blinding weapons to hollow-point bullets, but humanity serves to illuminate all other targeting principles.\textsuperscript{39}

While it is rare for courts or tribunals to second-guess most targeting decisions made in the heat of combat,\textsuperscript{40} there are nevertheless penalties for actions that grossly violate the standards articulated above. Perpetrators may face prosecution in domestic civilian courts or before domestic military tribunals.\textsuperscript{41} If the violations are serious enough, and if the domestic authorities are unwilling or unable to prosecute, the ICC may opt to prosecute, either by referral from the UN Security Council, or by the Chief Prosecutor’s own initiative.\textsuperscript{42} The Rome Statute includes war crimes within its jurisdiction, prohibiting acts ranging from the enlistment of child soldiers to the use of poison gas.\textsuperscript{43} Since crimes against humanity appear in the Rome Statute, the ICC can prosecute acts like deportation, murder, and rape if these acts are part of a widespread, systematic attack directed against a civilian population.\textsuperscript{44} For the purposes of a cyberwarfare targeting analysis,\textsuperscript{45} it is unlikely that jurisdiction over crimes against
humanity would be triggered—but one should not rule out possibility of such an occurrence.

2. Targeting Analysis

Consider the following hypothetical situation: war recently broke out between two neighboring Eurasian countries, Vulgaria and Archenland. Over the past few years, tensions have been high in these two former Soviet republics, but the past eighteen months have been particularly volatile as both countries have militarized their common border. Both countries did experience a period of liberal, democratic, rule shortly after the fall of the Soviet Union, and have ratified every major human rights treaty, the Additional Protocols to the Geneva Conventions, and the Rome Statute of the International Criminal Court. But, difficult economic circumstances have inflamed nationalist movements in each of the two republics, and both nations have taken steps to agitate their countrymen residing in ethnic enclaves within their borders. While the facts are still unclear, a small border incident between Vulgarian and Archenlander military units has escalated into all-out war with each side using the conflict to address a long line of grievances.

While the smaller of the two nations, Archenland has developed a highly sophisticated “Cyber Operations Command,” known colloquially within the country as “Unit 93.” While Unit 93 has engaged in low-level hacking and the defacement of Vulgarian websites, it has also gained the capability to penetrate the networks of the Vulgarian government as well as the networks of Vulgaria’s critical infrastructure. The commander of Unit 93 is eager to employ new viruses and malware to destroy or degrade Vulgarian infrastructure. His list of potential targets include dams, wastewater treatment plants, chemical processing factories, oil refineries, nuclear reactors, communications centers, and a number of “soft targets” like hospitals, power substations, and commercial banks. As the war progresses, Archenland’s Unit 93 prepares to strike.

Under the scenario described above, what kind of targeting analysis must Archenland’s Unit 93 employ? If the commander of Unit 93 directs kinetic
It is still unsettled as to what type of cyber-operation falls within the definition of “armed attack,” as the ICJ Nicaragua opinion is of regrettably little use to the current cyberspace-based scenario. The Tallinn Manual on the International Law of Cyber Warfare, however, provides a useful definition: “A cyber-attack is a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.” While somewhat overly broad, the use of this definition confines the jus in bello targeting analysis to those cyber-attacks, like Stuxnet, that can transcend an electronic medium and create the occurrence of conditions in physical space.
In proceeding with a *jus in bello* analysis, this article makes another critical assumption—namely, that the Vulgarian military would be able to attribute a specific cyber-attack to Archenland. This problem of attribution complicates self-defense and countermeasures, especially if a state will use conventional military weapons against the source of the cyber-attack.\(^{52}\) Because attribution raises doubt not only as to *who* caused an act of destruction, but also as to *what* caused the destruction, it is difficult to identify and respond to a cyber-attack in real-time.\(^{53}\) Thus, the following must proceed on the assumption that the cyber-attacks contemplated in the facts above can be attributed to a belligerent party with an acceptable level of certainty.

In the paragraphs below, the analysis surveys the legal issues first mentioned in Part 1 above. Particular weight is given to the Tallinn Manual on the International Law of Cyber Warfare, and articulates areas where IHL should be revisited in light of the capabilities of cyber-attacks.

### 2.1 Civilian Persons and Objects as the subject of cyber-operations

As noted above, IHL, and in the principle of distinction in particular, forbids the deliberate targeting of non-combatants. The primary exception to this is for those civilians that directly participate in the hostilities. Under IHL, DPHers are targetable for such time that they are directly participating.\(^{54}\) Thus, in the case above, if Archenland’s Unit 93 encourages the involvement of Archenlander civilian hackers in the conduction of cyber-attacks (attacks that can cause death, injury, or property damage), they can be targeted for as long as they participate in the cyber-attack. The Tallinn Manual goes further with its analysis: civilians that identify software vulnerabilities or civilians that gather military intelligence for their national militaries could be considered DPHers.\(^{55}\) While the transmission of tactical intelligence, or the provision of instructive assistance to military forces is “direct” enough for the purposes of DPH status,\(^{56}\) it is doubtful that a defending warring party could definitively determine the difference between tactical intelligence gathering (which is DPH) and strategic intelligence gathering (which is not DPH) *ex ante* when responding to a network intrusion. Such an
approach may open the door for countermeasures directed against the origination points of a cyber-attack, directed by geo-location software.\textsuperscript{57}

If enough civilians take part in cyber-operations, their involvement could constitute a \textit{levee en masse}, in which case, they may be entitled to combatant immunity and prisoner-of-war status.\textsuperscript{58} Importantly, \textit{levee en masse} status is not applicable during NIACs and many legal experts doubt whether civilians participating in a \textit{levee} could meet the openness-of-arms requirement, or whether the concept of a \textit{levee en masse} effectively captures the role of civilian hackers directing a cyber-attack against installations far behind enemy lines.\textsuperscript{59} And for civilians that serve a continuous combat function by virtue of their organizational involvement, they lose their protection from cyber-attacks. Thus, if the civilian commander-in-chief of the Vulgarian military has a pacemaker, that he is a permissible target of a cyber-attack.\textsuperscript{60} But because it is difficult to determine whether a target is a non-combatant, a combatant, or some other belligerent, states directing countermeasures (that is, responding to a cyberattack) should be especially cautious because of the uncertainty of the extent of civilian involvement in cyber-attacks.\textsuperscript{61}

\textbf{2.2 Core principles of targeting}

The four main principles of \textit{jus in bello} constrain cyber-operations in the following ways. First, the principle of necessity does not affect cyber-operations targeting analysis in any substantive way, as the necessity questions pertains to \textit{when} a warring party may attack (when it achieves a military advantage).\textsuperscript{62} As a result, the specific targeting analysis here, as it relates to cyber-operations, is more of a \textit{how} question, which touches on the principles below.

The principles of proportionality and distinction go hand-in-hand. Since distinction prohibits the targeting of any object or person who is neither a member of an armed force/group or someone directly participating in hostilities, the principle of proportionality determines when non-combatants or civilian objects may be targeted during wartime.\textsuperscript{63} In the context of cyber-operations, the proportionality analysis is more or less
unchanged—a cyber-attack that will cause an excessive amount of civilian death or destruction to civilian objects is prohibited.\textsuperscript{64} In circumstances unique to cyber-operations, higher-order consequences of a cyber-attack should also factor into the proportionality analysis. Thus, if malware that targets a military computer alone has a strong likelihood of infecting civilian systems, that potential outcome should be a part of the proportionality analysis. If the commander of Unit 93 seeks to target computer systems belonging to the Vulgarian military, he should also consider whether the malware may leak out into civilian cyberspace. Additionally, consequences further down the causal chain should also be considered. For instance, if an Archenlander cyber-attack takes air traffic control or GPS systems offline (as these can be both military and civilian use technologies) there may be loss of life and damage to property resulting from mistakes or errors made by people relying on that information.\textsuperscript{65} But the proportionality analysis might swing the other way. Consider this: Unit 93 undertakes cyber-attacks that are merely frustrating or irritating to Vulgarian troops and civilians, as in the case of a cyber-attack that intended to take vital systems offline but only succeeded in making the system unusable for a period of time.\textsuperscript{66} In such a case, it would be disproportionate (perhaps under a \textit{jus ad bellum} theory) for Vulgaria to respond to Archenland’s irritating cyber-attack with deadly kinetic force.

The principle of humanity prevents the infliction of suffering that is unnecessary to achieve a military objective, and this principle applies to cyber-operations as well.\textsuperscript{67} Take the case of the commander-in-chief’s pacemaker—if it was just as militarily feasible to kill the Vulgarian commander-in-chief with a gunshot to the head (causing instantaneous death) as it would be for Unit 93 to hack his pacemaker and induce a heart attack (causing a long, painful death through cardiac arrest), the principle of humanity would prohibit the latter course.\textsuperscript{68} Furthermore, the experts who wrote the Tallinn Manual contend that commanders (like those of Unit 93) should take “all feasible measures” to ensure that the methods of their cyber-attacks do not cause needless damage to civilian objects or persons.\textsuperscript{69} This principle may operate in an inverse fashion: the principle of humanity may \textit{compel} the use of a cyber-attack over a traditional armed attack. Consider the case of Archenland’s Unit 93, which seeks to take a
Vulgarian nuclear facility offline—they could use dozens of missiles and bombs or they could use a custom-tailored piece of malware to destroy a specific component in the nuclear facility. The principle of humanity should compel Unit 93 to actually conduct a cyber-attack over a conventional attack. These principles show that the traditional *jus in bello* analysis still constrains cyber-operations just as these principles constrain traditional operations, but it is when cyber-operations are considered as a separate phenomenon in its own right that new problems regarding IHL begin to emerge.

### 2.3 Perfidy, Ruses, and Cyber-operations

Because cyber-operations inherently rely on deception and subterfuge to penetrate a computer system, it is unclear whether this situation could be classified as either an illegal case of perfidy or a legal ruse of war. Additional Protocol I defines perfidy (also known as treachery) as an act “inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with the intent to betray that confidence.” Perfidy historically consists of acts that are meant to wound or kill the enemy, usually by feigning some sort of protected status (incapacitation/sickness, truce negotiators, UN parties, etc). Ruses, on the other hand, are legally permissible deceptions that do not invite the confidence of the enemy regarding the existence of a protected status. The Tallinn Manual illustrates this concept by listing a few cyber-operations that could qualify as ruses, including the transmission of false information or intelligence, the use of false computer identifiers, and the creation of nonexistent computer systems meant to represent nonexistent forces.
Camouflaging the origin of cyber-attacks is permissible in the eyes of experts as long as such camouflage does not constitute perfidy.\(^{73}\) This approach reflects contemporary international law. When one contemplates the specific conditions of cyber warfare, the perfidy/ruse analysis becomes more difficult in practice as multiple issues arise when considering the attribution problems inherent in analyzing cyber-attacks. For example, international law prohibits the use of enemy uniforms, insignia, and emblems when engaging in attacks, but an application to cyber-operations undermines the usefulness of cyberattacks in the first place.\(^{74}\) Consider the case of Unit 93, which could use false computer identifiers to gain access to Vulgarian computer systems. Under the ruse analysis above, the use of false identifiers is permissible. But there could be a few ‘false identifiers’ that could infiltrate an enemy computer network that does not hide the origin of the infiltration. Vulgarians watching their own computer networks would almost always respond to a suspicious infiltration or series of traffic, and would take countermeasures to protect the infiltration. Additionally, Unit 93, as lawful combatants, cannot broadcast their affiliation with Archenland, lest they expose the deception to the enemy.\(^{75}\)

How can Archenland’s Unit 93 disguise its attacks, if not as those of a civilian (forbidden under perfidy rules), a third state (also forbidden),\(^{76}\) or Vulgaria itself? By operation of international law on perfidy, Unit 93 would be relatively limited in what it could do, since the origin of its attacks would be easily determined by Vulgarian military personnel.

### 2.4 Special duties of care in attacking critical infrastructure

Unguarded or unsecure infrastructure poses a tantalizing target to Unit 93—it can wreak significant damage without exposing Archenland’s military forces to potential harm. The Tallinn Manual, however, contends that there is a special duty of care when Unit 93 seeks to target critical infrastructure like dams and nuclear facilities.\(^{77}\) Because the risk of excessive collateral damage is especially acute in targeting installations of this type, it logically follows that the principles of distinction and proportionality require additional caution. Operations designed to reduce the flow of electricity to the war effort must be undertaken with all “feasible precautions” to make sure excessive harm does not result.\(^{78}\)
Therefore, the principle of humanity should prevent the targeting of these types of critical infrastructure generally, as the risk of causing severe environmental damage, loss of civilian life, and damage to protected objects far outweighs any perceivable military advantage to be gained by taking these utilities offline. Thus, in instances where Unit 93 may risk targeting critical infrastructure with an aim towards destroying it or otherwise degrading its military value, the principle of humanity should necessitate the most extreme caution to avoid potential catastrophic losses.

2.5 Liability under the Rome Statute

If the commander of Unit 93 proceeds with his operational plans despite what IHL prescribes above, what potential penalties could he face at the ICC?79 If the commander targets and destroys a dam or nuclear reactor, he could face prosecution for crimes against humanity under Article 7 because his conduct would be widespread (affecting the entire country of Vulgaria) and systematic (the commander conducted these attacks via a military structure).80 In particular, if death results, he could be charged with murder under Article 7.81 If his attacks on critical infrastructure prevent civilians from receiving the necessities of life, he could face prosecution for extermination, but, absent his specific intent to do so, it is unclear whether a cyber-attack directed at a military target would meet the intent requirements.82

The war crimes analysis is somewhat different. The commander could face prosecution for wanton destruction.83 If he acts perfidiously to kill Vulgarian nationals, he could also face prosecution for willful killing.84 If he fails to exercise caution and fails to distinguish between military and civilian targets, the commander could similarly face prosecution for those crimes. If he uses a botnet that includes computers residing in neutral nations or in Vulgaria itself, he could even face prosecution for “compelling nationals” of a hostile party to take part in fighting against their own country.85 These few examples illustrate an important point about the nature of cyber warfare: actions taken behind a computer screen can result in criminal responsibility as much as actions in the field.
3. Conclusion

Faced with constraints from IHL and the possibility of post-war prosecution in the Hague, the commander of Archenland’s Unit 93 aborts many of the more aggressive operations planned for the war and limited operations to gathering intelligence, creating red herrings and diversions, and electronic reconnaissance. Robbed of the ability to clandestinely sabotage key dual-use targets, Archenland opts to engage in a series of air strikes, resulting in extensive damage to the Vulgarian interior. With external debts rising and with a limited capacity to recover from additional damage, Vulgaria calls for a ceasefire, much to the displeasure of its civilians most impacted by the Archenlander offensive.

The IHL cyber-operations targeting analysis reveals that, for the most part, the law treats traditional and cyberspace-based activities the same. But this reflects outcome-determinative thinking: cyberwarfare does not appear dissimilar from traditional warfare because that is the result that many gifted, renowned scholars expect from the analysis. But by looking beneath the surface at the nature of cyber-operations with their more deliberative nature far removed from the exigencies of combat and their inherently deceptive characteristics, it seems that IHL, as applied to certain discrete examples, serves to neuter cyber-operations instead of giving them a place within the scope of permissible military operations. This is unfortunate because cyber-operations, if performed correctly, could enable military operations that allow for force superiority without the long-lasting destructive impacts of conventional weapons. If the resources of an oil refinery or a communications relay could be neutralized for the duration of an armed conflict via a cyber-attack, this would circumvent the long-lasting after-effects of war, including incidental collateral damage to civilians. This ameliorative capacity could be a saving grace of cyber warfare, and it is one that warrants further exploration of these issues.

Endnotes

3 Ibid.
5 Ibid, 115.
8 Executive Order 13636.
10 Ibid.
12 Ibid, article 51.
16 But there are not clear indicators that allow jurists to separate a “border incident” from an armed conflict ex ante. One can only determine that an incident does not become an armed conflict after the hostilities persist or subside. Thus, for the purposes of legal analysis, international humanitarian law is presumed to apply whenever two states exchange fire.
17 Ibid, 76.
19 See e.g., Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 (governing the conduct of parties to a NIAC) (hereinafter Additional Protocol I).
IHL TARGETING IN CYBERSPACE: A HYPOTHETICAL CASE

23 ICRC DPH guidance, 43.
24 Ibid.
25 HCJ 46 I.L.M. 375 Public Committee against Torture in Israel v. Israel [2006] (Isr.).
26 ICRC DPH guidance, 16.
27 Ibid, 72.
28 Ibid.
29 Additional Protocol I, art. 52.
30 Ibid, art. 51(4)(b).
33 FM27-10, para. 41. See also Additional Protocol I, art. 51(5)(b).
34 Additional Protocol I, art. 51(5)(b); Schmitt, 132.
36 Schmitt, 95.
37 Additional Protocol I, art. 57(2)(a)(ii).
39 Ibid.
41 Schmitt, 80-81.
43 Ibid, art. 8(2)(b).
44 Ibid, art. 7.
46 Schmitt, 45-53 (Rules 10, 11, 12, 13).
48 See Nicaragua opinion note 13. The opinion defines an “armed attack” and uses the language of conventional warfare—that matters of armed force would involve the
movement of troops and the firing of weapons in three-dimensional space, namely, violating the sanctity of a national border through a physical incursion.

Ibid, 92 (Rule 30).

The inclusion of “destruction of objects” could bring operations that solely designed to destroy computers or servers within the scope of international humanitarian law (presuming other jus ad bellum requirements are met).

Ibid, 68 (Rule 20).


ICRC guidance at 15.

Schmitt, 102 (Rule 35).

Schmitt, 138.

See e.g., U.S. Patent No. 8825683 B2 (filed Nov. 21, 2008).

Schmitt, 88 (Rule 27).

Ibid, 89.

origin, and thus the intent, of the attack. Thus, by hiding those factors, lawful combatants may lose their combatant immunity because they are not complying with the requirements.

77 Schmitt, 182.
78 Ibid.
79 It is more or less certain that the commander of Unit 93 of our hypothetical scenario could face prosecution for his violations of IHL. See Tallinn Manual at 81 citing Rome Statute, art. 25(3); ICTY Statute, art. 7(1); ICTR Statute, art. 6(1); Sierra Leone Statute, art. 6(1); United Nations Transitional Administration in East Timor, art. 14(3); Prosecutor v. Blaškić, Case. No. IT-95-14-T, Trial Chamber Judgment, paras. 281-282 (Int’l Crim. Trib. for the Former Yugoslavia Mar. 3, 2000); Prosecutor v. Krstić, Case No. IT-98-33-T, Trial Chamber Judgement, para. 605 (Int’l Crim. Trib. for the Former Yugoslavia Aug. 2, 2001).
80 Rome Statute, art. 7.
81 Ibid.
82 Ibid, art. 7(2)(b).
83 Rome Statute, art. 2(a)(iv); 2(b)(iv).
84 Ibid, art. 2(a)(i); 2(b)(xi).
85 Ibid, art. 2(b)(xv).
86 Regrettably and for the sake of brevity, this article did not consider other interesting questions raised by the Tallinn Manual, namely, Rules 44, 52, 56, 58 respectively. These deal with cyber booby-traps (indistinguishable from spear-phishing), constant care in discrimination, the choice of targets, and the giving of warnings. See Tallinn Manual at 122, 137, 141, 144.