Strategy Research Project

Adapting International Law for Cyberspace

by

Lieutenant Colonel Nicole S. Jones
United States Army Reserve

United States Army War College
Class of 2014

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-04-2014	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Adapting International Law for Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Nicole S. Jones
United States Army Reserve

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Brian Gouker
Department of Military Strategy, Planning, and Operations (DMSPO)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5999

14. ABSTRACT

In today's global environment States are increasingly reliant on cyberspace for everything from banking services to infrastructure management. While this environment provides many benefits, reliance on digital systems also leaves us vulnerable. Malicious actions in cyberspace raise multiple legal and ethical questions for States wishing to respond to, or prevent, such actions. The Just War Framework provides an organized way to determine whether the reasons for going to war and the conduct of the war itself are morally justified; however, the international community has not yet adapted laws and international norms to cyberspace. Many questions remain regarding what actions rise to the threshold of armed attack, when a State has an inherent right to self-defense, and how to approach the problem of attribution for cyber attacks. The international community is seeking to clarify norms, most notably through NATO's Cooperative Cyber Defence Centre of Excellence, which published the Tallinn Manual in 2013. The United States must continue to participate in these and other forums and continue to partner with like-minded actors who share our goals of an open and secure cyberspace.

15. SUBJECT TERMS
Law of Armed Conflict, Law of War, Tallinn Manual, Attribution, Use of Force, Cyberwarfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	34	

USAWC STRATEGY RESEARCH PROJECT

Adapting International Law for Cyberspace

by

Lieutenant Colonel Nicole S. Jones
United States Army Reserve

Brian Gouker
Department of Military Strategy, Planning, and Operations (DMSPO)
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title: Adapting International Law for Cyberspace

Report Date: 15 April 2014

Page Count: 34

Word Count: 5999

Key Terms: Law of Armed Conflict, Law of War, Tallinn Manual, Attribution, Use of Force, Cyberwarfare

Classification: Unclassified

In today's global environment States are increasingly reliant on cyberspace for everything from banking services to infrastructure management. While this environment provides many benefits, reliance on digital systems also leaves us vulnerable. Malicious actions in cyberspace raise multiple legal and ethical questions for States wishing to respond to, or prevent, such actions. The Just War Framework provides an organized way to determine whether the reasons for going to war and the conduct of the war itself are morally justified; however, the international community has not yet adapted laws and international norms to cyberspace. Many questions remain regarding what actions rise to the threshold of armed attack, when a State has an inherent right to self-defense, and how to approach the problem of attribution for cyber attacks. The international community is seeking to clarify norms, most notably through NATO's Cooperative Cyber Defence Centre of Excellence, which published the Tallinn Manual in 2013. The United States must continue to participate in these and other forums and continue to partner with like-minded actors who share our goals of an open and secure cyberspace.

Adapting International Law for Cyberspace

> The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just, and peaceful conduct among states and peoples have begun to take hold.
>
> —President Barack Obama[1]

Cyberspace is a dynamic environment that represents immense opportunity for both exceptionally good and exceptionally poor behavior. We increasingly rely on digital backbones for everything from communication to research, banking to commerce, and transportation management to weapons systems controls. Cyberspace affords us the opportunity to connect with people, to purchase goods, and to quickly become aware of world events. However, reliance on cyberspace also makes us vulnerable. Identity theft, denial of services, and much worse can occur through our digital systems.

Consider the distributed denial of services (DDOS) attack against Estonia in 2007 following the Estonian government's removal of a Soviet war memorial from the center of Tallinn to a military cemetery on the outskirts of the city. Specific systems were saturated with millions of requests that targeted media and government websites, infrastructure, and banking applications. While the attack caused no permanent damage, it resulted in overload of the systems and their eventual shutdown, preventing legitimate use of the targeted systems for several weeks.[2] The results were extremely effective since Estonia is a highly networked nation.[3] It is these and other malicious actions that necessitate an international set of normative behaviors and laws in cyberspace. However, determining *that* there should be norms and laws is one thing; determining *what* those norms and laws should be is quite another.

Malicious actions in cyberspace raise multiple legal and ethical questions for nations wishing to respond to, or prevent, actions such as the DDOS attack on Estonia.

Some of the questions surround what actions constitute a cyber attack and what response is appropriate, what right a nation has to defend itself from cyber attack, and how to best deter such attacks. Although the United States clearly confirmed that it has "an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace"[4] and that it will "seek to encourage good actors and dissuade and deter those who threaten peace and stability through actions in cyberspace",[5] many issues remain. One issue is defining cyber attack. Most experts don't agree on what actions constitute a cyber attack, and even within the U.S. government there is no set framework or accepted hierarchy of cyber attacks. However, Director of National Intelligence James R. Clapper recently defined cyber attack as "a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data".[6] His definition is the one used for the basis of this paper.

This paper will present an analysis of international law as it applies in cyberspace, including the *jus ad bellum* and *jus in bello* criteria. It will then present current efforts for adapting international law for cyberspace.

Attribution in Cyberspace

Several of the requirements for both *jus ad bellum* and *jus in bello* relate to the issue of attribution in cyberspace. For example, determining whether a state can use self-defense is tied to knowing who perpetrated an attack. Determining whether another state is responsible for an action depends on whether the attack can be attributed to an actor in that state and then tied to the direction or control by the state itself. U.S. Department of State Legal Advisor Mr. Harold Koh noted that the "ability to mask one’s identity and geography in cyberspace and the resulting difficulties of timely, high-

confidence attribution can create significant challenges for states in identifying, evaluating, and accurately responding to threats."[7]

Analysts can dissect attribution in several ways: by determining the specific machine used in a cyber attack, a specific person or group who launched an attack, the geographic location of the machine that launched an attack, or the state responsible for the machine that launched an attack. Through technical attribution, or analysis of malicious functionality and malicious packets, it may be possible to determine the node that initiated or that is controlling an attack. When combined with other personal or human information, a state could positively attribute responsibility for an attack.[8]

Determining whether an attack can be traced back to an individual or machine depends upon the level of information connected to an Internet Protocol (IP) address. For example, if an Internet Service Provider captures and links billing information for an IP address to a specific person, an attack from that machine could be attributed to the specific owner or individual user of the machine. However, if no link to a specific individual exists, then the Internet address would only lead to a network endpoint, or small grouping of machines.[9] Compounding this difficulty, an individual could use an anti-attribution mechanism or identity mask to prevent an Internet address from being linked to a specific activity. Different groups of people such as military personnel and intelligence analysts, journalists, and others use anonymizers to conduct research or to hide the start and end points for communications.[10] Others use anonymizers to hide criminal activity. Additionally, proxies or "intermediate nodes that perform technical services during transmission" complicate attribution because they "change the source

IP address of a packet from that of the actual sender to their own address in the course of performing their service."[11]

Furthering the complexity of attribution, sophisticated attacks may be multi-stage in character. A multi-stage attack is one in which "an attacker infiltrates one computer to use as a platform to attack a second, and so on."[12] Determining the identity of the intermediary computer may not assist in assigning responsibility for the attack and the intermediary machine may not even be acting upon the intent of its owner.[13] Additionally, a level of uncertainty remains with attribution even when packets can be traced to a machine or when an Internet address is associated with an individual. The machine could be portable and used in many locations, or the person may be identifiable but have unknown affiliation or motivations. It would also cast doubt if a machine owner claimed that the computer was stolen or malicious packets were introduced to the machine without knowledge.[14]

Leaving behind a long chain of compromised machines is just one obfuscation technique that an attacker may use. Among others, code obfuscation hides or transforms cryptographic keys and data algorithms to conceal the purpose of the code,[15] and operating system obfuscation alters the "signature of a computer" to mask information so an adversary cannot identify the target system's operating system.[16] These obfuscation methods add further complexity to the multifaceted attribution problem.

If attribution is not specific to an individual, it may be identifiable to a geographic location since "many networks have a hierarchical design to their physical connectivity, and map the addresses to the levels of the hierarchy."[17] While this technique may not

pinpoint a specific location, it may allow a "very accurate guess about where the end-point is located" with some commercial firms claiming location accuracy between 90-96% to the specific state or city.[18] However, combined with intelligence and other analysis, a state may not need to identify a specific computer or individual in order to attribute a cyber attack. In order to determine attribution, a state would analyze similar attacks, forensic information, technical signatures, and knowledge of intent and capability of potential actors.[19]

Most cyber experts agree that attribution is a serious and complex issue with definite impacts on cyber attack, deterrence, countermeasures, and retribution. "Attribution is central to *deterrence*, the idea that one can dissuade attackers from acting" based upon their fear of a retaliatory attack.[20] However, retaliation *"requires knowing with full certainty who the attackers are*."[21] General Keith Alexander, Commander of U.S. Cyber Command, recommends that the United States approach the attribution issue through increasing the security of our own networks to deter attackers and partnering closely with both our own intelligence community and with international allies who share U.S. desires for a lawful cyberspace to determine attribution. Strengthening our own networks makes us a harder target, and working with likeminded allies and interagency partners would lead to agreements on accepted norms of behavior and ultimately to quicker notifications of attacks. General Alexander also notes that ultimately, the "only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do."[22]

Cyber practitioners, policymakers, and those seeking to adapt international law to encompass cyber activities should consider the complexities related to the attribution problem as they work through issues.

International Law in Cyberspace

The Just War Framework provides an organized way to determine whether the reasons for going to war and the conduct of the war itself are morally justified. Based upon the Charter of the United Nations and the Geneva Conventions respectively, these two paradigms provide criteria intended to restrain war.[23] Judgments about *jus ad bellum* and *jus in bello* are not inextricably linked. It is possible to fight a war justly yet have no just basis for going to war and vice versa.[24]

*Jus ad Bellum (*Just Recourse to War*)*

Jus ad bellum encompasses conclusions about whether one state has committed an act of aggression and whether another can invoke the right to self-defense.[25] Elements of *jus ad bellum* include: just cause, legitimate authority, public declaration, just intent, proportionality, last resort, and reasonable hope of success.

Just cause requires a legitimate reason to go to war, which is typically in response to aggression. The legitimate authority criterion defines who may authorize the use of force, seeking to limit the number of people who could do so for a state.[26] A public declaration serves as a formal notice from one state to another that an issue is deemed so egregious as to warrant the use of force if the offender does not peacefully - and immediately - resolve the issue.

The just intent criterion requires that the focus of hostilities remain the just cause that initially brought two parties into conflict. As a normative practice, just intent typically involves restoring the *status quo* that existed prior to hostilities. The requirement for

proportionality is that the price exacted through the use of force in war must be proportional to the attack suffered, or simply that "the damage done in war should be worth it".[27] The last resort criterion requires that a state has exhausted all reasonable non-violent options before resorting to use of force. However, this criterion causes much debate because typically a less amenable diplomatic solution would be preferable to any military action or use of force. Finally, having a reasonable hope of success requires that a state has a reasonable expectation that it will achieve its goals through use of force. It is not acceptable to cause death and destruction if there is no chance of restoring the *status quo* that existed prior to hostilities.[28]

Cyberspace and *Jus ad Bellum*

As the primary basis for *jus ad bellum*, the U.N. Charter defines what constitutes a war and when a nation can legally start a war. Article 51 codifies a state's inherent right of self-defense and Article 2(4) controls the use of force.[29] The Charter forbids the use of force except in two circumstances: when the U.N. Security Council authorizes it through a resolution, and when a signatory invokes its right to self-defense following an armed attack.[30] However, both the use of force and the right of self-defense are questionable when applied to cyberspace.

First, the Charter does not clearly define what constitutes "force" or "use of force" in a kinetic or traditional manner, and thus cannot delineate whether cyber operations constitute a use of force. One legal definition of force is "[p]ower, violence, or pressure directed against a person or thing".[31] Based upon this definition, force can be associated with a physical impact or change that is the result of power, violence, or pressure exerted upon a person or thing.[32] Therefore, if a kinetic operation results in the destruction of a building then it is a use of force. If a cyber operation results in the

destruction of a building (for example, through the meltdown of a nuclear reactor which then explodes) then it is a use of force as well. If the cyber operation has the same result as a kinetic operation, it is a use of force.[33]

Gray areas within guidance from the Charter do exist in "use of force" for kinetic and cyber operations. For example, while "Article 2(4) prohibits the use of force that could damage person or property" except as outlined above, it "allows other acts (specifically, economic sanctions) that could damage persons or property".[34] Similarly, a gray area exists in the definition of force for cyber operations that either do not have a clear kinetic effect or that do not have a clear kinetic effect *immediately*. For example, a theft of defense information from a system may not cause a change in the system itself. A low-level bombardment of a system may annoy users but not cause a system shutdown. However, harassment of a system over time may negatively impact trust in, or use of, a system, ultimately rendering it useless. Therefore, a question would be whether the accumulation of cyber activity over time could potentially reach the threshold for use of force and/or constitute a just intent.

Returning to the definition of force, we should note the inclusion of "violence" in the definition. Violence is defined as the "use of physical force, usually accompanied by fury, vehemence, or outrage".[35] This definition alludes to intent to cause physical change based upon passion or anger. It follows that the intent to do harm to a state's systems through cyber operations would equate to a use of force. However, causing physical change through cyber operations with no intent to do harm, such as accidentally causing a blackout in the northeastern United States while mapping an electrical grid, would not. However, it is widely acknowledged that differing definitions of

"use of force" will likely lead to different responses. During his confirmation proceedings, General Alexander wrote that "There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."[36]

Cyber expert Michael N. Schmitt provides a consequences-based approach to determining whether a cyber operation reaches the threshold for a use of force. His approach involves assessment of seven criteria: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[37] For severity, as his most important element, Schmitt explains that "[c]onsequences involving physical harm to individuals or property will alone amount to a use of force" and elaborates that severity depends on the "scale, scope and duration of the consequences".[38] For immediacy, he asserts that states have greater concern over effects that "manifest" immediately than those that build over time due to the lack of opportunity to mitigate effects.[39]

The directness criterion relates to the "chain of causation" or how closely related the act and its effects are; the "greater the attenuation between the initial act and the resulting consequences, the less likely States will be to deem the actor responsible for violating the prohibition on the use of force."[40] The invasiveness criterion relates to the security and availability of the targeted system. The "more secure a targeted system, the greater the concern to its penetration".[41] Here Schmitt excepts the use of cyber exploitation for the purposes of espionage, stating that "although highly invasive,

espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target-State's territory".[42]

Measurability is essentially the battle damage assessment of the cyber operation - the physical number of people, vehicles, or buildings destroyed. Presumptive legitimacy is the absence of an international law expressly forbidding the action. Schmitt provides the examples of "propaganda, psychological warfare, or espionage" which if "conducted through cyber operations" are "presumptively legitimate".[43] Finally, responsibility addresses when the international community will hold a state accountable for a cyber operation, in that the "closer the nexus between a State and the operations, the more likely other States will be to characterize them as uses of force".[44]

There are perhaps few cases when Schmitt's approach would without question reach the threshold for use of force. An example he uses to demonstrate application of his approach is the attack on Estonia. He concludes that the incident "arguably reached the use of force threshold" even as he notes that the "criteria are admittedly imprecise".[45] When applied to cases such as economic impacts without physical damage, temporary but reversible interruptions of systems or services, or data destruction, it would be difficult for a state to argue use of force unless there was a corresponding egregious outcome over which a state would publicly declare war. In some cases, such as with the *Stuxnet* virus that targeted Iranian nuclear centrifuges, the targeted country may not wish to admit that there was an impact. All of these factors which leave judgments open to interpretation demonstrate why application of international law to cyberspace is so difficult.

The second area where the U.N. Charter has difficulty in application to cyberspace relates to the right to self-defense. Article 51 only expresses the individual or collective right of self-defense in the case of "armed attack" against a member state; however, it does not define what constitutes an "armed attack".[46] As proposed above, if a cyber operation has the same effect as a kinetic operation, it would constitute a use of force. What then, is the difference between the use of force and an armed attack?

Some scholars argue that there is no difference between the two terms; however, the International Court of Justice defined the difference as "primarily one of 'scale and effects'" in *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. US), which indicates that not every use of force is an armed attack and therefore not every use of force can justify the right of self-defense.[47] Adopting the International Court of Justice approach, determining whether a cyber operation reaches the threshold of armed attack therefore requires determination of whether the results of the operation are substantial enough in terms of "scale and effects".

It is important to note that the United States disagrees with this distinction. Speaking for the U.S. government in his address at the U.S. Cyber Command Inter-Agency Legal Conference in September 2012, Mr. Koh remarked that:

> the United States has for a long time taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response – such responses must still be *necessary* and of course *proportionate*.[48]

Therefore it is important for U.S. security professionals to acknowledge that the requirement for an armed attack is hazy at best, and that it provides a potential area of disagreement between the United States and others in the international arena.

However, as Koh states, that does not mean that there is a "no-holds-barred" approach to self-defense. The response must be in accordance with the *jus in bello* requirements for the conduct of war itself.

Jus in Bello (Just Conduct of War)

The *jus in bello* portion of Just War Framework presumes that a state of armed conflict exists and provides guidelines for the conduct of the war itself. Based upon the Geneva Convention, the *jus in bello* law sets forth the requirements of military necessity, discrimination, and proportionality. The criterion of military necessity relates to the requirement that military operations must serve a material military purpose and must provide an advantage to assist in military defeat of an adversary.[49] Under the provision of proportionality, the use of force must be in proportion "to the threat or grievance provoking the use of force"[50] and should be "proportionate to the military value of the target".[51] While the requirement of proportionality does account for some collateral damage, an attack with an expected level of collateral damage that outweighs the expected military advantage would not meet the criteria.[52] Discrimination dictates that a state must distinguish between combatants and noncombatants and between military targets and civilian structures. In becoming a "combatant" either through personal choice or coercion, a person loses "immunity from deliberate attack".[53] When it is difficult to distinguish between combatants and non-combatants, such as in cases of counterinsurgency operations or guerilla warfare, a state must take the best care it can in determining the status of individuals.

Cyberspace and *Jus in Bello*

As with the U.N. Charter, the Geneva Convention does not expressly address scenarios relating to cyber. However, members of institutions such as the International

Committee of the Red Cross have weighed in, citing manipulation of civilian infrastructure through cyber operations as a "bloodless" method of warfare that could cause as much damage to civilians as more typical forms of warfare. In cases of power or water supply disruption, the effects could be severe. Additionally, the ability exists to interfere with airport and transportation control systems, causing collisions or other disruptions.[54]

In cyberspace, the requirement for military necessity would seem to be straightforward. If a state attacked a military network to disrupt or destroy a military command and control system, that attack would serve a specific military purpose and provide a concrete military advantage to the attacker. However, determining the specific military advantage can become complex when an attacker does not know enough about a system or the second and third order effects that would occur due to system linkages. For example, an attacker might gain a military advantage from hacking into an electric generator control, "but the system may have unforeseen layers that prevent such an advantage from occurring"; therefore, the advantage would not be definite enough to meet the requirement for military necessity.[55] Additionally, because so much of the cyberspace infrastructure is dual-use, it can be extremely difficult to determine where the specific military advantages lie. Another issue with the military necessity requirement is that it is often difficult to determine the concrete military advantage *prior* to an attack. Cyber warfare shares this difficulty with traditional warfare. In both, the attacker often cannot determine the effects of an attack unless it is successful. Put simply, the before and after analysis of an attack may differ based on the outcome of

the attack.[56] The determination of military necessity - providing a concrete military purpose and a definite military advantage - is situation dependent.

The requirement of proportionality also poses challenges for cyber attack. Because so many systems are dual-use, it is difficult to weigh the collateral damage to the civilian population with the anticipated military advantage. For example, attacking a power plant or dam could cause a level of disruption, hardship, or even death to a civilian population that would vastly outweigh the expected military advantage.[57] When a target is data on a network server, dual-use complexities increase.[58] A definitive understanding of how the theft of data, or changes made to data, will impact other systems and how the theft or changes to data tie to a tangible military result, outcome, or effect is paramount.

Cyber attacks could be more desirable than kinetic attacks because they are often not as deadly and may be reversible. Depending on the sophistication level of an attacker, a cyber attack could, in fact, be highly controlled and easily meet the requirements of proportionality.[59] One example of a very narrowly-targeted cyber attack is the *Stuxnet* virus, which "incorporated features designed to limit its effect": *Stuxnet* functioned only on a specific target, self-activated only under specific conditions, and self-destructed after a specific period of time.[60] Even with these limiting factors, parts of the attack could be questionable depending on which side of the attack you sit. For example, the *Stuxnet* virus was spread through manipulation of a line of code in civilian software, and arguably could have damaged both civilian and military nuclear power programs. Ultimately, before launching a cyber attack, it is important to understand the

value of the military target and the potential damage to civilian populations that will result from it.

Meeting the principle of discrimination can also be a significant challenge in cyberspace due to the dual-use nature of much of the cyber infrastructure. For example, satellites, routers, servers, and undersea cables routinely carry both civilian and military communications.[61] However, if it is impossible to differentiate communications as either military or civilian then the attack could meet the distinction criteria. Additionally, objects that serve a material military purpose for an opponent would be valid cyber targets.[62]

The people who create or launch cyber attacks raise issues when it comes to distinction between combatant and non-combatant status. A civilian who directly participates in combat does not garner a protected status under the Geneva Convention. The International Red Cross provides several examples of when an individual is directly participating in an attack: "interfering electronically with military computer networks (computer network attacks)" or "disturbing" military communications through "interrupting the power supply of radar stations", or "transmitting tactical targeting intelligence for a specific attack".[63] Individuals would be in a protected status except for the time when they directly participate in hostilities, meaning that an individual or "hacktivist" is not protected while carrying out a cyber attack, but that the individual would then revert to a protected status afterward. The distinction is important because an enormous amount of cyber expertise lie in the civilian domain; a civilian's use of cyber attack would at least open the door to criminal prosecution, but in the case of a declared war could also result in status as an unlawful combatant without the

protections of combatant immunity or prisoner of war privileges in the case of capture.[64] Although capture is highly unlikely, the risk should be acknowledged.

There are several specific examples of civilian actions that would likely result in civilians losing protected status. For example, civilian employees who help develop or design a cyber weapon that requires continuous modification to ensure its effectiveness, non-state actors who perform a cyber attack at the behest of the state so that the state can maintain plausible deniability of the attack, or a civilian company that counterattacks to protect its dual-use infrastructure.[65] At this point, whether or not a cyber attack rises to the level of armed attack and justifies actions in self-defense becomes important.

The Geneva Convention requires a "level of organization or state command responsibility" in its definition of lawful combatants, which includes armed forces with cyber capability and groups that are not inherently military but that receive consent or direction from the state.[66] In cyberspace, however, unorganized individuals can anonymously participate in attacks that cause damages with levels that are commensurate to a combatant. As mentioned above, civilians may fall under the definition of lawful combatant depending on their direct actions. Additionally, the Geneva Convention requires that lawful combatants wear a "fixed sign" or carry arms openly to distinguish themselves as lawful combatants. A source of ongoing legal debate for both traditional and non-traditional forms of warfare, this distinction applies less to cyber attackers who generally operate remotely from the intended target and employ layers of protection to assure anonymity.[67] One suggestion that would clearly adhere to the principle of distinction for cyber warfare would be to have any such

attacks originate from a military or government Internet Protocol (IP) address. However, to do so would virtually paint a "bulls-eye" on that computer.[68]

Current Cyberspace Efforts in International Law

Together, the *jus ad bellum* and *jus in bello* tests are largely based on armed attack scenarios that do not account for contemporary issues such as non-state actors and cyber attack.[69] The 2011 *International Strategy for Cyberspace* acknowledged that gaps exist, but also stated that the international community does not need a wholesale revision of applicable law:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.[70]

The international community is seeking to clarify norms, most notably through NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE). According to General Alexander, "The cyber assaults on Estonia in 2007 spurred the United States and our NATO allies to deliberate regarding what in cyberspace would constitute an 'armed attack' on an alliance member that would trigger the North Atlantic Treaty's provisions on collective defense."[71] The CCD COE worked for three years to determine how existing international laws or norms apply to cyber warfare. The group formally published its work, commonly known as the *Tallinn Manual*, in early 2013. The manual describes 94 "rules" that an International Group of Experts agreed upon, and provides both the legal basis for the rule and any differences of opinion.[72] It is important to note, however, that the *Tallinn Manual* is neither an official NATO document, nor the policy of any NATO member. Rather, it reflects the collective opinions of the International Group

of Experts.[73] The *Tallinn Manual* comprehensively addresses both the *jus ad bellum* and the *jus in bello* aspects of armed conflict, which they note are synonymous with the law of war, the law of armed conflict, and international humanitarian law.[74] While the 94 "rules" indicate that in many areas international agreement may be possible, there were several areas in which the CCD COE experts could not reach consensus. Among others, these areas include the delineation of a state's unlawful "use of force" and defining an "armed attack" that would justify a state's responding use of force.[75]

The *Tallinn Manual* relies on the International Court of Justice for its proviso that the use of force and self defense apply to "any use of force, regardless of the weapons employed", thereby treating a kinetic weapon and a cyber weapon the same.[76] Furthermore, the experts agreed that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[77] The use of force includes acts that "injure or kill persons or damage or destroy objects" but also must have been "carried out by, or are attributable to, a state".[78] Where the experts disagreed was on cyber operations that lack a parallel kinetic effect. They adopted the consequences-based approach to determining whether a cyber operation reaches the threshold for a use of force, outlined above, but left the issue unresolved.

Regarding the right to self-defense and the types of activities that reach the threshold of armed attack, the Tallinn experts agreed that a state can legally exercise self-defense in cases of cyber operations that reach the level of armed attack. They clarified that "cyber operations that kill or seriously injure individuals or cause serious damage to objects qualify as armed attacks."[79] However, the experts could not agree on

other situations that propelled cyber operations to the threshold of armed attack. They adopted the International Court of Justice's "scale and effects" test but could not agree on what those entailed. They did agree that "combining effects" would meet the threshold of armed attack if the attacks are "conducted by the same attacker (or attackers operating in concert), are related in terms of objective, and satisfy the requisite scale and effects threshold."[80] The experts rejected cyber operations conducted for preventive self-defense, wherein an attack is possible but that attacker either lacks the capability or intention to carry out the attack. While many experts did agree that in the case of anticipatory self-defense, a state *could* take action, they did not agree on *when*. Some believe that the impetus is the proximity in time between the defensive action and the attack that prompted it, and some believe that the impetus is whether the state would "lose its opportunity to effectively defend itself unless it acts."[81] Koh outlined the views of the United States in his speech - that self-defense potentially applies against *any* illegal use of force.[82]

Many other topics in the *Tallinn Manual* are notable. For example, Rule 5 (Control of Cyber Infrastructure) prescribes that "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive government control to be used for acts that adversely and unlawfully affect other States."[83] Under this rule, a state is accountable if it "fails to take reasonably feasible measures to terminate the conduct" once it is becomes aware of an ongoing attack either through its own efforts or when another state provides credible information of an attack. However, the experts could not agree whether this rule applies if the state "has only constructive ('should have known') knowledge" or "fails to use due care in policing cyber activities".[84] The

term "policing" highlights the differences in acceptable - or legal - activities from state to state. They could also not agree on whether a state is responsible when an attack is routed through its sovereign territory but originates somewhere else.[85]

The *Tallinn Manual* specifically addresses the responsibility of states as it relates to non-state actors under Rule 6 (Legal Responsibility of States). Adhering again to the International Court of Justice rule that "a State is responsible for the acts of non-State actors where it has 'effective control' over such actors", the *Tallinn Manual* clearly distinguishes between organized groups acting on behalf of the state and individuals acting on their own initiative[86]. The experts also noted that the International Court may hold a state responsible for the actions of non-state actors if the state provides "cyber expertise during the planning of specific cyber attacks" or later if the state "expresses support for them and uses its cyber capabilities to protect the non-State actors against counter-cyber operations".[87]

In contrast to some of the disagreements above, the International Group of Experts "did not find dual-use cyber infrastructure to be uniquely problematic as a matter of law."[88] Citing comparisons between other military-civilian infrastructure such as airfields, electrical networks, and railheads, the experts agreed that such infrastructure would become a military object once it was "used" to shield military activity or communication regardless of whether the civilian activity continued.[89] The *Tallinn Manual* does differentiate between things like a router and an entire computer network; if a router qualifies as a military object, that does not mean that the entire network qualifies. Additionally, once the object is no longer used for military purposes, it would revert to a civilian object and no longer qualify as a legal military target.[90]

Conclusion

Malicious actions in cyberspace raise multiple legal and ethical questions for states wishing to respond to, or prevent, such actions. Issues such as attribution, dual-use technology, and the right of self-defense require experts to exercise extreme care in determining when cyber operations are warranted and whether their resultant impacts to both military and civilian personnel and objects are acceptable.

Together, the U.N. Charter and the Geneva Convention provide the jus *ad bellum* and *jus in bello* requirements for determining whether the reasons for going to war and the conduct of a war itself are justifiable. While international laws and norms are still largely based on armed attack scenarios, it is not necessary to conduct a wholesale revision of applicable law. The international community must adapt international law to new scenarios related to cyberspace and continue to formulate international norms of acceptable behavior. International efforts such as those conducted through NATO's Cooperative Cyber Defence Centre of Excellence are taking place, and they are making progress. The United States must continue to participate in these and other forums and continue to partner with like-minded actors who share our goals of an open and secure cyberspace.

Endnotes

[1] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), Introduction.

[2] Jason D. Jolley, "Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?," *International Law Research* 2, no. 1 (2013): 1.

[3] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring*

CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (Washington, DC: The National Academies Press, 2010), 151, http://www.nap.edu/catalog/12997.html (accessed January 17, 2013).

[4] Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 10.

[5] Ibid., 12.

[6] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record to the Senate Committee on Armed Services (April 18, 2013): 1.

[7] Koh, "International Law in Cyberspace," Remarks to the Inter-Agency Legal Conference, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (accessed December 28, 2013).

[8] W. Earl Boebert, "A Survey of Challenges in Attribution," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 43, http://www.nap.edu/catalog/12997.html (accessed January 17, 2014).

[9] David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, 32.

[10] Ibid., 33.

[11] Boebert, "A Survey of Challenges in Attribution," 45.

[12] Ibid., 26.

[13] Ibid., 31.

[14] Boebert, "A Survey of Challenges in Attribution," 43, 49.

[15] Christian S. Collberg, "Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection," *IEEE Transactions on Software Engineering* 28, no. 8 (August 2002): 738.

[16] Sherry Murphy, Todd McDonald, and Robert Mills, "An Application of Deception in Cyberspace: Operating System Obfuscation," in *International Conference on Information Warfare and Security* (Reading, UK: International Conference on Information Warfare and Security, April 2010), 241.

[17] Clark and Landau, "Untangling Attribution," 33.

[18] Ibid., 33-34.

[19] Lin, "Cyber Conflict and International Humanitarian Law," 522.

[20] Clark and Landau, "Untangling Attribution," 25.

[21] Ibid.

[22] Keith B. Alexander, “Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command,” http://epic.org/Alexander_04-15-10.pdf (accessed January 18, 2014).

[23] Martin L. Cook, "Ethical Issues in War: An Overview,” in J. Boone Bartholomees, Jr., ed. *U.S. Army War College Guide to National Security Issues,* 5th ed., Vol. II: *National Security Policy and Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, July 2012), 221, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1110.pdf (accessed June 3, 2013).

[24] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustration,* 4th ed. (New York: Basic Books, 2006), 21.

[25] Ibid.

[26] Cook, "Ethical Issues in War: An Overview,” 221.

[27] Ibid., 222.

[28] Ibid.

[29] Charter of the United Nations, https://www.un.org/en/documents/charter/index.shtml (accessed December 28, 2013).

[30] Herbert Lin, "Cyber Conflict and International Humanitarian Law," *International Review of the Red Cross* 94, no. 886 (Summer 2012): 524.

[31] Bryan A. Garner, *Black's Law Dictionary,* 8th ed. (St. Paul, MN: Thomson/West), 673.

[32] Jolley, "Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?" 3.

[33] Ibid.

[34] Lin, "Cyber Conflict and International Humanitarian Law," 524.

[35] Garner, *Black's Law Dictionary,* 1601.

[36] Alexander, “Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command.”

[37] Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 25.

[38] Ibid.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Charter of the United Nations, Chapter VII: Action With Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, https://www.un.org/en/documents/charter/index.shtml (accessed December 28, 2013).

[47] Michael Gervais, "Cyber Attacks and the Laws of War," *Berkeley Journal of International Law* 30, no. 2 (2012): 9.

[48] Harold Hongju Koh, "International Law in Cyberspace," Remarks to the Inter-Agency Legal Conference, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (accessed 28 December 2013).

[49] Lin, "Cyber Conflict and International Humanitarian Law," 525.

[50] Garner, *Black's Law Dictionary,* 1255.

[51] Cook, "Ethical Issues in War: An Overview," 225.

[52] Lin, "Cyber Conflict and International Humanitarian Law," 526.

[53] Cook, "Ethical Issues in War: An Overview," 224.

[54] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," *International Review of the Red Cross* 94, no. 886 (Summer 2012): 539.

[55] Gervais, "Cyber Attacks and the Laws of War," 20.

[56] Ibid.

[57] Lin, "Cyber Conflict and International Humanitarian Law," 526.

[58] Kyle Genaro Phillips, "Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain," *Joint Force Quarterly* 70 (Third Quarter 2013): 74.

[59] Gervais, "Cyber Attacks and the Laws of War," 23.

[60] Ibid., 24.

[61] Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," 541.

[62] Paul A. Walker, "Law of the Horse or Law of the Submarine: The Future of State Behavior in Cyberspace," lecture, U.S. Army War College, Carlisle Barracks, PA, November 26, 2013, cited with permission of CDR Walker.

[63] International Committee of the Red Cross, "Direct Participation in Hostilities: Questions and Answers," February 6, 2009, http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm (accessed January 25, 2014).

[64] Knut Dörmann, "The Legal Situation of 'Unlawful/Unprivileged Combatants,'" *International Review of the Red Cross* 85, no. 849 (March 2003): 45. The terms “unlawful combatant” and “unprivileged combatant/belligerent” are used in legal literature and case law to generally describe persons who are not integrated into the regular armed forces but who take a direct part in hostilities without being entitled to do so. These individuals therefore cannot be classified as prisoners of war on falling into the power of the enemy. The terms "unlawful combatant" and "unprivileged combatant/belligerent" do not appear in international humanitarian law.

[65] Vijay M. Padmanabhan, "Cyber Warriors and the *Jus in Bello*," *International Law Studies*, 89, no. 288 (2013): 293-294.

[66] Gervais, "Cyber Attacks and the Laws of War," 20.

[67] Padmanabhan, "Cyber Warriors and the Jus in Bello," 295.

[68] Ibid.

[69] Cook, "Ethical Issues in War: An Overview,” 225.

[70] Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 12.

[71] Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 5.

[72] *NATO Cooperative Cyber Defence Centre of Excellence Home Page,* https://www.ccdcoe.org/249.html (accessed December 28, 2013).

[73] Ibid.

[74] Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual/5?e=0 (accessed December 28, 2013).

[75] Liis Vihul and Michael N. Schmitt, "The Tallinn Manual on Cyber Warfare – A First Tool for Legal Practitioners," http://www.cambridgeblog.org/2013/11/the-tallinn-manual-on-cyber-warfare-a-first-tool-for-legal-practitioners-michael-schmitt-liis-vihul-nato/ (accessed January 17, 2014).

[76] Michael N. Schmitt, "Tallinn Manual on the International Law applicable to Cyber Warfare" (Cambridge: Cambridge University Press, 2013), 42, http://issuu.com/nato_ccd_coe/docs/tallinnmanual/45?e=5903855/1802381 (accessed January 18, 2014).

[77] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal Online* 54 (December 2012): 19.

[78] Ibid.

[79] Ibid., 21.

[80] Ibid., 23.

[81] Ibid.

[82] Koh, "International Law in Cyberspace."

[83] Schmitt, "Tallinn Manual on the International Law applicable to Cyber Warfare," 26.

[84] Ibid., 28.

[85] Ibid.

[86] Ibid., 32-33.

[87] Ibid., 33-34.

[88] Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," 29.

[89] Ibid.

[90] Schmitt, "Tallinn Manual on the International Law applicable to Cyber Warfare," 128-129.