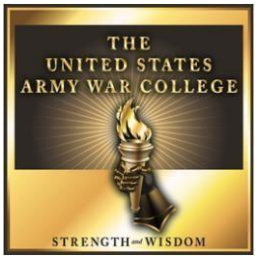
Strategy Research Project

A Framework for Legal Risk in Military Cyber Operations

by

Colonel Nicholas F. Lancaster
United States Army

Under the Direction of:
Dr. Jeffrey L. Groh



United States Army War College
Class of 2016

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-04-2016	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
A Framework for Legal Risk in Military Cyber Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Nicholas F. Lancaster
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Jeffrey L. Groh

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.
Please consider submitting to DTIC for worldwide availability? **YES:** ☒ **or NO:** ☐ **(student check one)**
Project Adviser recommends DTIC submission? **YES:** ☒ **or NO:** ☐ **(PA check one)**

13. SUPPLEMENTARY NOTES
Word Count: 5,709

14. ABSTRACT
Combatant and Joint Force Commanders are comfortable weighing operational risk, however they must also weigh legal risk when operating in cyberspace. Four areas of legal risk for cyber operations include avoiding inadvertent armed attacks, complying with the law of armed conflict, following the intelligence oversight rules, and ensuring operations do not qualify as covert action. An armed attack under international law is the trigger for a response in self-defense, so commanders must conduct their cyber activities below this threshold and conduct their operations in accordance with the law of armed conflict. On the domestic side, commanders must carefully plan and supervise their operations to ensure they comply with intelligence oversight rules designed to protect U.S. persons. Finally, because cyber operations are innately devoid of attribution, commanders must be vigilant to ensure their operations do not qualify as covert action that the President must independently authorize and report to Congress.

15. SUBJECT TERMS
Armed Attack, Jus Ad Bellum, IHL, Covert Action, Intelligence Oversight

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	30	

A Framework for Legal Risk in Military Cyber Operations

(5,709 words)

Abstract

Combatant and Joint Force Commanders are comfortable weighing operational risk, however they must also weigh legal risk when operating in cyberspace. Four areas of legal risk for cyber operations include avoiding inadvertent armed attacks, complying with the law of armed conflict, following the intelligence oversight rules, and ensuring operations do not qualify as covert action. An armed attack under international law is the trigger for a response in self-defense, so commanders must conduct their cyber activities below this threshold and conduct their operations in accordance with the law of armed conflict. On the domestic side, commanders must carefully plan and supervise their operations to ensure they comply with intelligence oversight rules designed to protect U.S. persons. Finally, because cyber operations are innately devoid of attribution, commanders must be vigilant to ensure their operations do not qualify as covert action that the President must independently authorize and report to Congress.

A Framework for Legal Risk in Military Cyber Operations

Operations in cyberspace pose as much or more legal risk than operational risk when compared with operations in other domains. This is because the operators are usually not actually on the battlefield, meaning there is little physical risk, yet there may nonetheless be very high legal risk. The 2010 Quadrennial Defense Review (QDR) divides the types of risk into four categories: Operational, Force management, Institutional, and Future challenges.[1] Operational risk is described as "the ability of the current force to execute strategy successfully within acceptable human, materiel, financial, and strategic costs."[2] Legal risk as described overlaps with operational risk and is consistent with the term "political risk," also identified in the 2010 QDR.[3] Political risk is listed as one of three broader risk considerations required by Title 10, alongside strategic and military risk. Political risk as described in the 2010 QDR is the perceived legitimacy of our actions in the international context along with maintaining public support in the United States.[4] Legal risk considered here is the potential for operations to run afoul of international or domestic rules governing the conduct of operations. The international community, and more importantly, the American people, may consider military operations that violate the rules unlawful and illegitimate uses of force. Much has been written about particular legal aspects of operating in cyberspace,[5] however there is little overall guidance for commanders beyond simply consulting with their lawyers.[6]

This paper proposes a framework of four questions Combatant and Joint Force Commanders should consider when planning operations in cyberspace. First is whether a particular act in cyberspace might qualify as a use of force or armed attack, such that another State might legally respond in self-defense. Second is whether the operation

itself complies with International Humanitarian Law (IHL), the Law of Armed Conflict (LOAC). Third is whether a particular operation complies with, or at least is consistent with, the intelligence oversight rules. Fourth, does the operation raise questions as to whether it should be considered covert action rather than a traditional military activity? Commanders must consider legal risk when planning military operations in cyberspace to avoid inadvertently violating international law or running afoul of the intelligence oversight rules.

This paper describes the four legal questions Commanders should consider when planning cyberspace operations. After providing the background for each question, it explores the application of each to operations in cyberspace. Finally, the paper summarizes the four questions as a recommendation for Commanders and Staffs to use when considering cyberspace operations.

Jus Ad Bellum (Armed Attack)

The first question Commanders must consider when planning operations in cyberspace is whether a particular act in cyberspace could be considered a use of force or armed attack by other States. This is important because a use of force or armed attack might trigger a response in self-defense under international law. The terms “use of force” and “armed attack” both come from the United Nations Charter, which provides the international legal rules for using force.

Fundamental to International law is the principle of non-intervention, also known as sovereignty. This is the idea that States are responsible for security within their borders and other states have no right to interfere.[7] In line with this principle, the United Nations Charter prohibits the use of force unless authorized by the Security Council under Chapter VII, or self-defense under Article 51 or customary international law.[8]

Article 2(4) of the Charter reads: “All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”[9] When the United Nations Security Council determines under Chapter VII there has been a threat to the peace, a breach of the peace, or an act of aggression under Article 39, then it may recommend actions under Art. 39,[10] or mandate actions under Art. 41 or 42 of the Charter. Article 41 says the Security Council can mandate non-military enforcement measures including “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.”[11] Article 42 authorizes the Security Council to mandate military action by forces made available through special agreements with U.N. member States.[12] An example of U.N. action under Chapter VII is United Nations Security Council Resolution 2011, authorizing ISAF to take “all necessary measures” to fulfill its mandate to assist the government of Afghanistan in improving the security situation and building its own security capabilities.[13]

Even if the United Nations Security Council has not authorized action under Chapter VII, States still maintain their right to self-defense under both the Charter and customary international law. Article 51 of the Charter reads: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations until the Security Council has taken measures necessary to maintain international peace and security.”[14] This reads as if the right to self-defense is only applicable until the Security Council has time to act, however most States agree there is a customary international law right to self-defense

independent of the U.N. Charter.[15] Self-Defense under the United Nations Charter is only authorized in cases of “armed attack,” not against just any use of force.

Armed attack is generally understood to mean an attack that has physical effects.[16] When the Charter was originally conceived, there were some States who desired to outlaw the use of economic or political force alongside military force. However, this minority position was not adopted in the final version of the Charter. Due to this history, it is clear that only an “armed attack” allows a response in self-defense under Article 51.[17] This idea of armed attack is particularly relevant in cyberspace, since presumably a State could not respond in self-defense with kinetic force to cyber activity not amounting to an armed attack.

Self-Defense under the U.N. Charter includes the concepts of both individual and collective self-defense. Individual self-defense means protection of a State’s territorial integrity, political independence, and protection of nationals and their property abroad.[18] Collective self-defense means the protection of others, and allows victim States to receive assistance from others in responding to and repelling an armed attack.[19] However, collective self-defense requires an invitation or request for assistance from the victim state because the state is effectively waiving sovereignty. One example of self-defense under Art. 51 of the U.N. Charter is UNSCR 1368 authorizing use of force in self-defense in Afghanistan the day after the 9-11 attacks.[20]

Another important self-defense concept is anticipatory self-defense, or the use of force in anticipation of an imminent armed attack. This is the idea that a State doesn’t have to wait until actually attacked, i.e. absorb the first blow, but rather can respond before it is attacked by another.[21] Anticipatory self-defense is appropriate only if the

circumstances leading to the use of force are “instantaneous, overwhelming, and leaving no choice of means and no moment for deliberation.”[22] An extension of anticipatory self-defense argued by the United States during the Bush administration is the idea of pre-emptive self-defense, which stretches the concept of imminence by arguing the greater the threat, the greater the risk of waiting for attack at a time and place of the enemy’s choosing.[23] This means under some circumstances anticipatory self-defense could be used even when an attack is not strictly imminent, and has been used as the rationale for anticipatory self-defense in response to WMD and terrorism.[24]

Operations in cyberspace are by nature not physically violent themselves, however they may have physical consequences. Sending malicious code through cyberspace to the control center of a dam is not a physically violent act, however if the code causes the floodgates to open and water destroys infrastructure downstream, then the consequence is clearly physical. Most well-known cyber operations, such as the distributed denial of service (DDoS) attacks in Estonia in 2007,[25] have not had physical consequences, however there is at least one that inarguably did, the Stuxnet virus that caused physical damage to Iranian centrifuges in 2010.[26]

Experts in international law have been grappling with the issue of when a cyber operation qualifies as an armed attack since at least 1999.[27] Although many authors have written on the subject, the only real consensus is the idea that if an operation results in physical damage analogous to a use of kinetic force, then it is considered an armed attack. The Tallin Manual, drafted by international law experts in 2013, defines a cyberattack as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”[28]

This means Commanders must carefully consider whether a particular operation in cyberspace may have physical consequences before going forward.

Jus In Bello (Law of Armed Conflict)

The discussion thus far has been about the Jus Ad Bellum, the international legal rules for when force may be used. The legality of a decision to use force hinges on whether a particular operation qualifies as an armed attack, allowing a response in self-defense. The next section will consider the Jus In Bello, the rules governing the use of force during operations.

United States policy is to apply the law of armed conflict in all military operations, regardless of how categorized.[29] More specifically, the United States has made it clear that existing international norms apply to operations in cyberspace.[30] This means Commanders and planners must be cognizant of the law of armed conflict in all planned cyber operations.

The law of armed conflict is referred to in the international community as International Humanitarian Law (IHL), and is based primarily on The Hague and Geneva Conventions and their Additional Protocols.[31] The provisions contained in these treaties mainly come from customary international law, which embodies the rules followed by states over time out of a sense of legal obligation, but not necessarily written down anywhere. The overall purpose of these treaties is the prevention of civilian suffering during war. Four general principles of IHL are military necessity, distinction or discrimination, proportionality, and the prevention of unnecessary suffering. The application of each principle in cyberspace will be addressed in turn.

Military Necessity “justifies those measures not forbidden by international law which are indispensable for securing the complete submission of the enemy as soon as

possible."[32] Basically, this is the justification for resort to the use of force required to accomplish a military mission. Importantly, this principle does not justify all uses of force, but only lawful uses of force under international law. This is the fundamental principle that although the use of force is permitted, it is not an unlimited mandate, there are rules that must be followed even in war.[33]

The principle of military necessity applied to cyber operations is not significantly different than when applied to kinetic operations. Operations in cyberspace are justified so long as they adhere to the rules of IHL. This means the three principles below must be considered specifically for their application in cyberspace.

The principle of distinction or discrimination requires distinguishing combatants and military objects from civilians and civilian objects. Combatants can be attacked at any time, whereas civilians must be protected from attack. Combatants are members of regular armed forces of a State, and those who generally meet four requirements: "(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war."[34] Combatants are immune from prosecution for their warlike acts, and are treated as prisoners of war if captured. If they surrender, become *hors de combat*, or otherwise are out of the fight, then they may not be attacked.[35] Those who participate in armed conflict but do not meet the four criteria are considered unprivileged belligerents, such as spies, who are subject to host nation criminal law for their actions.[36]

Military objects are 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."[37] Examples of military objects include weapon systems and military installations or positions.

IHL defines civilians in the negative, that is, anyone who is not a combatant is considered a civilian.[38] There is an important exception, however, for civilians who directly participate in hostilities. Direct Participation in Hostilities (DPH), is the idea that civilians enjoy protection from direct attack "unless and for such time as they take a direct part in hostilities."[39] Civilians can lose their protected status if they engage in military acts. This sounds a bit more straightforward that it is, however, since civilians are only targetable while engaging in those acts. If a civilian plants an Improvised Explosive Device (IED), and then walks away, he or she is targetable while digging the hole and implanting the device, and even while walking away. However, the next day, while merely walking down the street, he is once again considered a civilian and not subject to attack.[40] In practice, the situation is often resolved by gathering information on the IED implanter to properly categorize him as a combatant who may be lawfully targeted, rather than a civilian.

In the same way IHL defines civilians in the negative as anyone not meeting the requirements of combatants, IHL defines civilian objects as objects that do not qualify as military.[41] Civilian objects are those that are not military by their nature, location, purpose, or use.[42] Using these definitions, it is easy to see that while most persons and objects are considered civilian, a case can often be made for military attributes. Consider a school occupied by military forces. The school may now be considered a military object because of its current use, even though normally categorized as a civilian

object. Once military forces have left the premises, however, the school can no longer be targeted, because it has returned to its civilian use.

This scenario raises the issue of so called “dual use” objects, similar to the revolving door issue of DPH. How should objects be categorized when they serve both military and civilian purposes? The answer again lies in the nature, location, purpose, and use of the object. A classic example of a dual use object is an electrical grid powering both civilian and military infrastructure. So long as an attacker observes the other principles of IHL, the grid is considered both a civilian and military object, and may be lawfully attacked.[43]

The principle of distinction is difficult in kinetic operations, where military and civilian personnel are often mixed across the battlefield, but even more difficult in cyberspace, where many actors and potential targets are dual use, or possess both civilian and military characteristics. Most of cyberspace is inherently dual use, consisting of the Internet and systems connected with the Internet. It may be particularly difficult to tell whether a civilian is participating in hostilities in cyberspace, where the activity is much less apparent than in the physical world. Even if the fact of direct participation is established, what are the parameters for the activity? In other words, what are the left and right limits for when he or she may lawfully be attacked? While a dual use object may be lawfully targeted as military considering the principle of distinction, meeting the requirements of proportionality may be more difficult.

Proportionality is the idea that “the anticipated loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained.”[44] This principle requires the commander to weigh

the impact of his or her operations against the anticipated gain. This is also where the term collateral damage is used. Collateral damage is unavoidable and unintentional damage to civilian personnel and property incurred while attacking a military objective. It is important to note that collateral damage is not illegal, however the potential for collateral damage must be factored in when determining the proportionality of a particular action on the battlefield.[45]

Commanders are familiar with conducting a proportionality balancing for kinetic operations, and there are a variety of technical and analytical tools used by targeteers to try and predict the impact of particular military actions. Staffs identify potential targets and prepare the most effective ordnance to achieve the desired effects while minimizing collateral damage. Even so, this is a difficult and complex task on the battlefield, and one commanders rightly take seriously. Targeting cells typically first exclude all civilian objects from consideration, and only after identifying military targets consider the possibility of collateral damage. The commander then ultimately weighs the military advantage against the anticipated loss of life and damage and decides whether to attack.

Like distinction, proportionality is a challenging principle in kinetic operations that is even more challenging in cyberspace, where there is great potential for unintended consequences. In kinetic operations there is often a fair amount of available data, both on structures targeted, and on the effects of various types of ordnance, to predict with relative accuracy the results of a particular attack. In cyberspace there is much less information, and the results of a particular cyberattack may be much less predictable. Launching a missile, or dropping a bomb has a generally predictable effect. Munitions

generally explode with a predictable and pre-determined amount of force. Even if circumstances at the target location are different from anticipated, a 500 pound bomb is limited to the maximum explosive effect of a 500 pound bomb. In cyberspace, a bit of malware, designed to effect a particular target, may have more unpredictable effects. The malware may have to pass through an uncertain number of networks, rather than launching on a predictable trajectory. Even if it reaches the intended target, it could infect other targets along the way, or travel through cyberspace in an unpredictable pattern. This is not to assume there are no precise cyberattack methods in existence, just that commanders and staffs must take more care in cyberspace than in the kinetic realm. An attack in cyberspace has the potential to unleash a viral infection spreading uncontrollably through civilian systems. This is not a realistic possibility in kinetic operations.

The final IHL principle to understand is the prevention of unnecessary suffering, or humanity, which means avoiding inflicting gratuitous violence on the enemy. It may seem counterintuitive to have a principle of IHL which tells combatants to minimize suffering, however this is one of the primary purposes of IHL. The Hague Regulations of 1907 state "it is especially forbidden…to employ arms, projectiles or material calculated to cause unnecessary suffering."[46] This provision is understood to prohibit the use of chemical and biological weapons, hollow point bullets in most circumstances, poison, and glass filled projectiles, to name a few. Chemical and biological weapons may offer the best comparison for cyberspace weapons. They are prohibited both because they cause unnecessary suffering and because they are by nature indiscriminate. Once a chemical, or particularly a biological weapon is deployed, the weapon's effects are

impossible to control. It is also impossible to restrict the effects of such weapons to combatants and military objects.

In cyberspace, this principle would impact activities that could lead to mass civilian casualties, like opening the floodgates of a dam, or disabling air traffic control while hundreds of planes are in the air. Disabling traffic control for a particular aircraft, or for military aircraft generally would be unobjectionable, but using a cyberattack to disable traffic control that affects civilian aircraft would be considered indiscriminate. Another example might be a cyberattack on the system of satellites that provide global positioning system (GPS) coverage. Knocking out GPS might have a military purpose in degrading an enemy's command and control systems, but today there are so many civilian applications for the same system that it might be considered indiscriminate. If the same cyberattack that disables enemy command and control also causes a loss of navigation data for commercial civilian shipping, the attack would likely be considered indiscriminate, causing unnecessary suffering for the civilian population.

Intelligence Oversight

The previous two sections of this paper discussed the first two questions in the framework, both directly related to the international law covering the use of force. The next two sections are both focused primarily on the domestic intelligence oversight rules designed to prevent the U.S. government from collecting information on U.S. persons without a warrant. Commanders must consider the intelligence oversight rules to avoid violating the rights of U.S. persons when planning and conducting operations in cyberspace.

Executive Order (EO) 12333 lays out rules designed to protect the privacy of U.S. persons from collection by United States Intelligence Organizations. The EO

contains a list of various procedures for collection with the rules for each. The EO basically divides the world of persons into two categories, U.S. persons and non-U.S. persons, and makes collection against U.S. persons without their consent illegal without a warrant or some other law enforcement type process.[47]

EO 12333 and its implementing regulations at the DoD[48] and service[49] levels don't technically apply to most military operations since they are designed for, and by their terms only apply to, the intelligence community. When the EO was originally signed in 1981 this may have made sense, however in the intervening years there has been a convergence between operations and intelligence such that the distinction makes less sense today. Although there is a surface and mechanical attractiveness to the argument there should be different rules for intelligence operations, it doesn't bear reasoned scrutiny in today's environment. In 1981, few if any regular military operations contained elements of intelligence. Today, many operational units are conducting missions that previously would have been categorized as intelligence operations.[50]

Professional intelligence personnel receive detailed and comprehensive training on the intelligence oversight rules designed to protect the privacy of U.S. persons. Non-intelligence personnel receive little if any training in this area. If the rules are only for intelligence professionals, then the system is designed for trained intelligence personnel to comply with the rules, while less trained personnel can collect U.S. person information at will. This does not make sense. Even if a particular commander believes the rules do not apply to his or her unit's activities, the current sensitivity of the U.S. public to allegations of spying or misuse of private information argue for caution when engaging in any operation likely to involve U.S. person information.

EO 12333 and its implementing regulations allow the intelligence community to collect information on U.S. persons only in accordance with procedures described in the order. The head of the intelligence element doing the collecting must authorize, and the Attorney General of the United States must approve, the particular procedure used.[51] The EO specifies the types of information that may be collected in some detail, primarily information related to foreign intelligence or counterintelligence activities, necessary for protecting our own elements and activities, and information collected with the consent of the target. The EO gives primacy to collection within the United States to the FBI, and specifies that collection may not be undertaken regarding the domestic activities of U.S. persons.[52] From the perspective of protecting the rights of U.S. persons this makes eminent sense, since the FBI is a domestic law enforcement agency and can be expected to understand best the rules for protecting individual rights by obtaining warrants for example.

The EO describes the types of collection that may be authorized, and also lists the various techniques that may be used for collection. The guiding principle for choosing a technique is least intrusive means. This means collection within the United States or against U.S. persons must use the least intrusive means available. The EO specifies that collection techniques including electronic and physical surveillance, unconsented physical searches, and use of monitoring devices may not be used except in compliance with procedures approved by the Attorney General. “Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.”[53] It goes on to prohibit the CIA from engaging in electronic surveillance within the U.S., and prohibit any agency but the FBI from

conducting physical searches and surveillance within the United States. Finally, the EO prohibits "[p]hysical surveillance of a United States person abroad…except to obtain significant information that cannot reasonably be acquired by other means."[54]

One area where intelligence personnel often struggle that will almost certainly implicate operations in cyberspace is undisclosed participation. The procedure for undisclosed participation requires a U.S. intelligence official to disclose their intelligence identity when participating in a group including U.S. persons when the interaction is for an intelligence purpose.[55] The idea is that organizations consisting of U.S. persons do not want their government to spy on them. This procedure, along with the other intelligence oversight rules, was put into place in response to revelations of domestic spying in the 1960s and 1970s.[56]

The intelligence oversight rules are designed to protect the rights of U.S. persons during the conduct of intelligence collection activities. If intelligence collection was a discrete function only undertaken by intelligence community personnel, then it would not be an issue for most military commanders. They could trust the conduct of intelligence operations to their assigned intelligence officers and units and feel comfortable that the rights of U.S. persons were being protected during operations. Unfortunately, with the growth of cyber capabilities, there are many more operations that now impact the rights of U.S. persons, and more opportunities for non-intelligence personnel to inadvertently violate the rules.

Service members at the lowest level now have the ability to collect information using simple widely available tools. It is easy to imagine, for example, an exercise within the United States where there is electronic chatter, on Facebook or Twitter for example.

A natural inclination may be to go to those sites for the purpose of seeing what the chatter is about, perhaps to make sure there is not a threat to interrupt the exercise. A credentialed counterintelligence agent, trained in the rules, may be authorized to collect communications for counterintelligence purposes. However, a typical service member, without counterintelligence responsibilities or training, would not be permitted to do the same thing. This seems like a minor issue until it is reported in the media with a headline that says “military monitoring citizens’ communications on Facebook.” Another example is the use of military training for personal purposes in cyberspace. Service members are trained in some circumstances to track the electronic presence of an enemy for targeting in an overseas military operation. Unfortunately, any service member can use the very same techniques to track an ex-girlfriend or boyfriend in the United States.

Service members could easily violate the undisclosed participation rules in cyberspace. This situation may develop in a cyber operation conducted by non-intelligence personnel, for example an operation to simply monitor Facebook, Twitter, or other social media for force protection purposes. Simply following somebody on Twitter might not rise to the level of a procedure 10 violation. However, actively seeking and friending a person or group for the purpose of monitoring their activity in cyberspace would probably qualify.

Covert Action

Along with describing the rules for collecting intelligence while protecting the rights of U.S. persons, EO 11233 and its implementing regulations specify that “No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.”[57] The EO then goes on to define the term

and its exceptions by reference to the covert action statute, 50 U.S.C. 413(b). The Covert Action Statute defines Covert Action as: “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include-…(2) traditional diplomatic or military activities, or routine support to such activities;…”[58] A quick reading of that definition would seem to exclude any activity the military could classify as “traditional,” including virtually all actions currently classified as Operational Preparation of the Environment (OPE).[59] Unfortunately for military operations, the House and Senate reports accompanying the Statute contain a much more detailed discussion of the intent behind the definition. That discussion makes it clear that in addition to the “traditional” nature of the actions covered by the exception, the issue of attribution is paramount. If the role of the United States Government is not to be acknowledged publicly, then the activity is likely to be considered covert action. On the other hand, if a particular action is executed in concert with a military operation where the role of the United States Government is apparent or acknowledged, then it is not considered covert action.[60]

This means attribution is not an issue with cyber activities that accompany an overt military operation. The discussion makes it clear that if the operation is to be acknowledged publicly, then any supporting activity is also considered to be acknowledged. This would cover, for example, a cyber operation immediately preceding or contemporaneous with a kinetic attack. A cyber operation designed to shut down enemy air defenses, or to hinder enemy communications, or even to corrupt their battlefield management systems as the opening act of a kinetic attack would all be no

problem. However, cyber activity that takes place far in advance of a kinetic attack, along the lines of OPE, such as implanting a worm that will activate at some later contingent date to facilitate an attack, if not intended to be acknowledged, might not fall within the definition of traditional military activity.[61]

One way to address this issue is to simply say that the cyber operation is in fact to be acknowledged publicly, just not until the supported operation commences. This explanation may carry the day when the time between the cyber operation and the supported military operation is relatively short, but not when the cyber operation is months or years in advance of a more speculative or contingent military operation.

The foregoing discussion of defining an operation as covert action versus a traditional military activity raises the significant issue of attribution in cyberspace. Cloudy attribution is one of the signature factors of cyber operations generally. It is often difficult to determine the author of a particular cyber operation, even when the operation itself has been detected. Cyber activity can appear to emanate from a location other than its true locus, and the routes to the target can wind through multiple servers in various countries.[62] Most of the well-known recent "cyber-attacks" were not quickly or even definitively attributed.[63] Even after expert organizations like the FBI have stated definitively that a cyber-attack came from a particular source, many other experts have disagreed or refused to accept the answer, instead positing their own theories of who was responsible for the attacks.[64]

Because it is relatively easy to cloud the identity of the actor in cyberspace, the temptation is to disregard the requirement of acknowledging the role of the United States Government in any particular cyber activity. Commanders should be careful to

address the issue of public acknowledgement up front when planning operations in cyberspace to avoid their operations being labelled as covert action in violation of the statute.

Recommendations

When planning operations in cyberspace, Combatant and Joint Force Commanders should consider the four broad legal questions proposed in this framework. Two questions concerning international law, and two questions involving domestic legal rules. First, does the planned operation stay under the “armed attack” threshold for operations that might qualify as a use of force under international law? Second, does the operation comply with the traditional principles of international humanitarian law? Third, does the operation comply with the intelligence oversight rules designed to protect the Constitutional rights of U.S. persons? Fourth, and finally, is there a plan to acknowledge the operation at some future time, so that the operation will not be categorized as a covert action that requires a presidential finding?

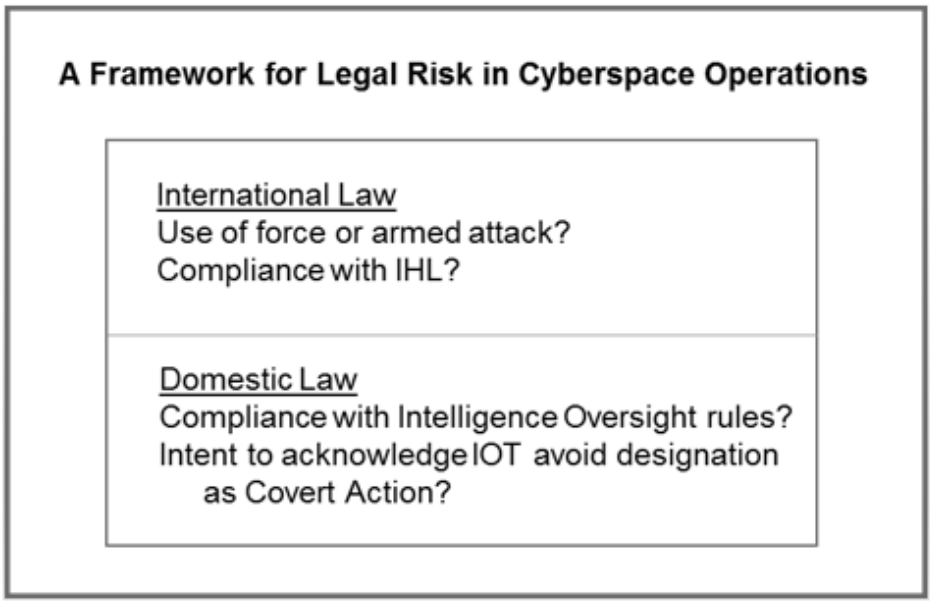


Figure 1. Legal Risk in Cyberspace Operations[65]

When commanders fail to consider legal risk in operations, they may undermine the legitimacy of military actions. The support of the American people depends in part on their trust that the U.S. military is conducting operations in accordance with the law. Accounting for legal risk ensures operations comply with U.S. policy and the international rules for the use of force enshrined in the U.N. Charter. Compliance with policy and law in cyberspace poses more of a challenge than similar operations in other domains. Although the physical risk of operations in cyberspace is low, the legal risk of cyber operations is potentially high. The opportunity to inadvertently cross a legal line that qualifies as a use of force under the U.N. Charter, or even worse, an “armed attack” that would justify a response in self-defense is higher in cyberspace than in traditional kinetic operations. Even if an operation avoids the international law pitfalls, there are domestic legal constraints that apply with greater force in cyberspace than in the other domains. Operations in cyberspace may inadvertently violate the Intelligence oversight rules, including the prohibition on covert action. To mitigate this legal risk, commanders

must comprehensively consider the international and domestic rules that might come into play when planning operations in cyberspace.

Conclusion

The potential for significant legal consequences in cyberspace operations argues for Combatant and Joint Force Commanders to use a framework for legal risk when assessing their operations in this domain. Joint Publication 3-12 tells commanders they must understand the law in this area:

> Before conducting CO [cyberspace operations], commanders, planners, and operators must understand the relevant legal framework in order to comply with laws and policies, the application of which may be challenging given the ubiquitous nature of cyberspace and the often geographic orientation of domestic and international law.[66]

The four questions contained in the framework proposed here provide a foundation for understanding the legal environment. Combatant and Joint Force Commanders should use the framework as a tool for prompting discussions with their staffs and legal advisors when considering how to mitigate the legal risks associated with cyberspace operations.

Endnotes

[1] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), 90.

[2] Ibid.

[3] Ibid., 95.

[4] "In the international context, political risk derives from the perceived legitimacy of our actions and the resulting impact on the ability of allies and partners to support shared goals. In the domestic context, political risk relates to public support of national strategic priorities and the associated resource requirements in the near term, midterm, and long term." Ibid.

[5] See Matthew Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36 (Summer 2011): 421. Describing when operations in cyberspace might qualify as a use of force or armed attack contemplated by the U.N. Charter;

Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks," *Texas Law Review* 88 (June 2010): 1533-1569. Discussing the International Humanitarian Law (IHL) rules that apply to operations in cyberspace; Michael N. Schmitt, "Wired Warfare: Computer Network Attack and International Law," *International Law Studies* 76, Computer Network Attack and International Law, eds Michael N. Schmitt and Brian T. O'Donnell (Naval War College, Newport, RI, 2002); 187-218. Discussing the application of IHL to Computer Network Attack (CNA); Aaron P. Brecher, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations," *Michigan Law Review* 111 (2012). Discussing when operations in cyberspace might be considered covert action.

[6] For instance, AR 381-10 states "Commanders will seek legal advice from their supporting U.S. legal advisor," and goes on to require legal review of collection activities. U.S. Department of the Army, *U.S. Army Intelligence Activities*, Army Regulation 381-10 (Washington, DC: U.S. Department of the Army, May 3, 2007), Para. 1-6. DoD guidance says "All questions of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned." Under Secretary of Defense for Policy, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, DoD 5240.1-R, C1.3 (Washington, DC: U.S. Department of Defense, December 1982); Joint Pub 3-12 says "It is essential that commanders, planners, and operators consult with legal counsel during planning and execution of CO [cyberspace operations]." U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R), III-10 (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013).

[7] The Law Dictionary, "Sovereignty," http://thelawdictionary.org/sovereignty/ (accessed February 3, 2016). There is, however, the emerging concept of humanitarian intervention, for situations when States are unable or unwilling to maintain security or are themselves responsible for violence against their own citizens. This concept is known as the Responsibility to Protect (R2P).

[8] *Charter of the United Nations*, June 26, 1945, 59 Stat. 1031.

[9] Ibid., art. 2(4).

[10] Ibid., art. 39. Although Article 42 suggests the Security Council could mandate military action, since there are currently no agreements for standing UN forces, this is technically how force is authorized, it is recommended rather than mandated.

[11] Ibid., art. 41. It is interesting in this context to note that Article 41, though clearly pre-dating the existence of cyberspace, does contemplate the interruption of communications as a use of force short of armed attack.

[12] Ibid., art. 42. See Endnote 7 above for explanation of why military action is recommended under Article 39 instead of mandated under Article 42.

[13] United Nations, *United Nations Security Council Resolution 2011* (UNSCR 2011) (New York: United Nations, October 12, 2011), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2011%282011%29 (accessed February 3, 2016).

[14] *Charter of the United Nations*, art. 51.

[15] Todd C. Huntley, "Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review* 60 (2010): 19; U.S. Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: U.S. Department of Defense, 1999), http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf (accessed May 10, 2016).

[16] Ibid., 16.

[17] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999): 905.

[18] Major William Johnson, ed., *Operational Law Handbook*, JA 422 (Charlottesville, VA: The Judge Advocate General's Legal Center and School, 2013), 4. See generally, Yoram Dinstein, *War, Aggression and Self-Defense* (Cambridge, UK: Cambridge University Press, 2001), 192-221.

[19] Ibid., 4; Dinstein, *War, Aggression and Self-Defense*, 222-245.

[20] United Nations, *United Nations Security Council Resolution 1368* (UNSCR 1368) (New York: United Nations, September 12, 2001) http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1368%282001%29 (accessed February 3, 2016).

[21] The traditional standard for imminence comes from the "Caroline Case." The Caroline case is not actually a legal case, but rather a situation that arose when a U.S. riverboat was attacked by British forces while carrying supplies to Canadian rebels in 1837. After the incident there was an exchange of letters between the U.S. Secretary of State, Daniel Webster, and the British foreign office, which laid out the accepted customary international law rules for anticipatory self-defense. The full text of the letters can be found online at: The Avalon Project: Documents in Law, History, and Diplomacy, "British-American Diplomacy: The Caroline Case," http://avalon.law.yale.edu/19th_century/br-1842d.asp (accessed February 3, 2016).

[22] Letter from Daniel Webster, Secretary of State, to Lord Ashburton, July 27, 1842, The Avalon Project: Documents in Law, History, and Diplomacy, "British-American Diplomacy: The Caroline Case."

[23] George W. Bush, *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 17, 2002), 15.

[24], "Feith: Iraq Attack was Pre-emptive," *CBS News,* April 3, 2008, http://www.cbsnews.com/news/feith-iraq-attack-was-preemptive/2/ (accessed March 22, 2016).

[25] Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 7.

[26] Ibid., 42.

[27] Schmitt, "Computer Network Attack and the Use of Force in International Law," 914-15. This article lays out a series of six factors to be considered when examining and categorizing uses of force, including severity, immediacy, directness, invasiveness, measurability, and

presumed legitimacy. Considering the consequences of uses of force using these six factors is referred to as using the "Schmitt factors."

[28] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013). The Tallinn manual uses the six Schmitt factors in footnote 21 plus military character and state involvement as evaluation criteria when assessing use of force in cyberspace.

[29] U.S. Department of Defense, *DoD Law of War Program*, Department of Defense Directive (DoDD) 2311.01E (Washington, DC: U.S. Department of Defense, November 15, 2010, certified current as of February 22, 2011).

[30] Harold Hongju Koh, "International Law in Cyberspace," speech, U.S. Cyber Command Inter-Agency Legal Conference, Fort Meade, MD, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (accessed February 3, 2016).

[31] U.S. Department of State, "Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulation Concerning the Laws and Customs of War on Land," October 18, 1907, 36 Stat. 2277; U.S. Department of State, "Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Geneva Convention I)," August 12, 1949, T.I.A.S. 3362; U.S. Department of State, "Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Geneva Convention II)," August 12, 1949, T.I.A.S. 3363; Department of State, "Geneva Convention Relative to the Treatment of Prisoners of War (Geneva Convention III)," August 12, 1949, T.I.A.S. 3364; Department of State, "Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Geneva Convention IV)," August 12, 1949, T.I.A.S. 3365; International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I)," June 8, 1977, 1125 UNTS 3; International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Additional Protocol II)," June 8, 1977, 1125 UNTS 609.

[32] U.S. Department of the Army, *The Law of Land Warfare*, Field Manual (FM) 27-10 (Washington, DC: U.S. Department of the Army, July, 1956), para. 3(a).

[33] Ibid.

[34] U.S. Department of State, "Geneva Convention Relative to the Treatment of Prisoners of War (Geneva Convention III)," art.4.

[35] Article 3 common to all four Geneva Conventions. Department of State, "Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Geneva Convention I)," art. 3; Department of State, "Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Geneva Convention II)," art. 3; Department of State, "Geneva Convention Relative to the Treatment of Prisoners of War (Geneva Convention III)," art. 3; Department of State, "Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Geneva Convention IV)," art. 3.

[36] International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I)," art. 46.

[37] International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I)," art. 52(2).

[38] Ibid., art. 5.

[39] Ibid., art. 51(3).

[40] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities* (Geneva, Switzerland: International Committee of the Red Cross, May 2009).

[41] International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I)," art. 52.

[42] Military objects are defined 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." International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I)," art. 52(2).

[43] Rule 39 states "An object used for both civilian and military purposes-including computers, computer networks, and cyber infrastructure-is a military objective." Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 39.

[44] U.S. Department of the Army, *The Law of Land Warfare*, para. 41.

[45] International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I)," art. 51(5)(b). The term collateral damage is not defined in international law, however Article 51(5)(b) describes an indiscriminate attack as one "which may be expected to cause incidental loss of human life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

[46] U.S. Department of State, "Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulation Concerning the Laws and Customs of War on Land," art. 23(e).

[47] EO 12333 defines a United States person as "a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States persons or permanent resident aliens, or a corporation incorporated in the Unites States, except for a corporation directed and controlled by a foreign government or governments." The White House, *United States Intelligence Activities*, Executive Order 12333, 40 Fed. Reg. 59,941 (Dec. 4, 1981), as amended by Executive Order 13284, 68 Fed. Reg. 4,077 (Jan. 23, 2003), and by Executive Order 13355, and further amended by Executive Order 13470, 73 Fed. Reg. 45,328 (July 30, 2008).

[48] Under Secretary of Defense for Policy, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, DoD 5240.1-R (December 1982).

[49] U.S. Department of the Army, *U.S. Army Intelligence Activities*, Army Regulation 381-10, (Washington, DC: U.S. Department of the Army, May 3, 2007).

[50] See generally Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy* 5 (2012): 539.

[51] The White House, *United States Intelligence Activities*, Executive Order 12333.

[52] Ibid.

[53] Ibid.

[54] Ibid., part 2.4(d).

[55] Ibid., part 2.9.

[56] U.S. Congress, Senate, Select Committee to Study Governmental Operations With Respect To Intelligence Activities, Intelligence Activities and the Rights of Americans, *Final Report of the Select Committee to Study Governmental Operations With Respect To Intelligence Activities, Intelligence Activities and the Rights of Americans*, Senate Report 94-755, 94th Congress, 2d Sess. (April 26, 1976). The full report is better known as the Church Committee report, named for Idaho Senator Frank Church, the committee chairman.

[57] The White House, *United States Intelligence Activities*, Executive Order 12333, part 2.13.

[58] *Intelligence Authorization Act, Fiscal Year 1991*, Public Law 102-88, 105th Cong. (1991). Codified at 50 U.S.C. 413(b)(e).

[59] "The conduct of activities in likely or potential areas of operations to prepare and shape the operational environment. Also called OPE," U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05 (Washington, DC: U.S. Joint Chiefs of Staff, July 16, 2014), GL-9.

[60] *Intelligence Authorization Act for Fiscal Year 1991*; U.S. Congress, Senate, Select Committee on Intelligence, *Authorizing Appropriations for Fiscal Year 1991 for the Intelligence Activities of the U.S. Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System, and for Other Purposes*, Senate Report 102-85, 102d Congress, 1st Sess. (June 19, 1991; U.S. Congress, House of Representatives, Conference Report, *Intelligence Authorization Act for Fiscal Year 1991*, House Conference Report 101-928, 101st Congress, 2d Sess. (October 23, 1989).

[61] See generally Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate." Discussing whether a given computer network operation (CNO) might be categorized as covert action or traditional military activity (TMA).

[62] Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," 443-448.

[63] Rid, *Cyber War Will Not Take Place*, 6-9. See generally Neil C. Rowe, "The Attribution of Cyber Warfare," in *Cyber Warfare, A Multidisciplinary Analysis*, ed. James A. Green (New York: Routledge, 2015).

[64] "FBI Still Believes North Korea is Responsible for Sony Hack," *CBS News,* December 30, 2014, http://www.cbsnews.com/news/fbi-still-believes-north-korea-is-responsible-for-sony-hack/ (accessed January 27, 2015).

[65] This is simply a graphical representation of the four questions comprising the framework for considering legal risk in cyberspace operations proposed in this paper.

[66] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R) (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013), III-10.