Abstract

In light of the alleged North Korean breach against Sony Pictures Entertainment and other cyber-enabled attacks against private companies in the past year, it has become increasingly important for both the government and private companies to establish protocols to address such incidents. Currently, there are no laws that specifically address cyber attacks against a state for a political or national security purpose, and many such attacks do not reach the “armed attack” threshold set by the law of war.

A growing consensus among legal scholars has suggested instead that the law of countermeasures, which addresses international law violations, could be used to justify retributive actions against cyber attacks. However, we argue that the unique nature of networks make active countermeasures a troublesome precedent to set both legally and technically. The problem of identifying and directing a countermeasure against an attacker is uniquely difficult in network attacks, and allowing forceful countermeasures in
a cyber context could lead to escalating retaliations and standards that could be applied in a non-cyber context. Furthermore, countermeasures in a cyber context weaken the restrictions of necessity and proportionality, threatening the purpose of said checks and possibly causing repercussions for the law.

Instead, we suggest that, in a perfect system, passive defenses should be sufficient to ward off cyber attacks. These controls include prevention measures such as link encryption and firewalls, detection measures such as intrusion detection systems and recovery measures such as segmentation and redundancy. In cases where a cyber attack evades these passive defenses, non-cyber responses such as economic, diplomatic and political restrictions should be applied instead.

**Introduction**

Earlier this month, President Barack Obama signed an Executive Order granting the Treasury Department the right to financially cut off hackers responsible for cyber-enabled activities that pose a “significant threat to the national security, foreign policy, or economic health or financial stability of the United States” [1]. After the alleged North Korean hack against Sony Pictures Entertainment and other high profile attacks in the past year against Target, JP Morgan and Home Depot that left the personal information of over 200 million customers vulnerable, this move by President Obama reflects the government’s increasing concern with protecting the country against digital attacks [6].

While these specific incidents involved the private sector, it has become increasingly important for both the government and private companies to establish protocols to address such breaches as the variety, frequency and potential of cyber-
enabled attacks grow. Presently, there are no laws that specifically address cyber attacks and retributive actions that a state may take against them. Instead, other laws that govern conduct in the course of war or that respond to international law violations have been interpreted to address cyber attacks. However, the application of these sets of laws are limited since they were not written with a cyber context in mind. The law of war (*jus ad bellum*) sets a threshold of an “armed attack” to justify engagement in war, which cyber attacks do not meet if they do not cause physical destruction, as is often the case [7]. There is a growing consensus among legal scholars that the law of countermeasures, which addresses international law violations that do not meet the “armed attack” threshold, could be applied to these instances of cyber attacks. However, there are a number of issues with countermeasures that make it a troublesome precedent to set in a cyber context. As some legal scholars have pointed out, the law of countermeasures was not intended to serve for attacks of force, and using this set of laws for such instances could have snowballing consequences for both cyber and physical attacks below the *jus ad bellum* threshold. Furthermore, due to the nature of computer networks, the restrictions on countermeasures such as necessity and proportionality face technical challenges that could allow justified retributive actions to quickly escalate. Thus, in this paper we point out many of the issues with applying the law of countermeasures in a cyber context, and instead argue that in an ideal technical setting, passive defenses should be sufficient to ward off cyber attacks. In cases where they are not, since cyber security is not perfect, non-cyber responses such as economic, diplomatic and political restrictions should be used instead.
Defining a cyber attack

In legally dealing with cyber attacks, the first step is defining what constitutes such an attack. Article 2(4) of the Charter of the United Nations prohibits the use or threat of force, stating that member states “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” [7]. When a state violates said use of force through an attack upon another state, the law of war, an aspect of public international law also defined in the UN Charter, explains the acceptable justifications to engage in war (jus ad bellum) and the limits to acceptable wartime conduct (jus in bello).

Jus ad bellum defines the legitimate reasons to engage in war as an exception to the prohibition of force in Article 51: “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” [7]. Thus, this wording sets the threshold of engaging in war at responding to an “armed attack.” While a cyber attack has never instigated an armed conflict and therefore this is all theoretical, the phrase “armed attack” has conventionally been interpreted to mean those that have tangible physical consequences. As legal scholar Oona Hathaway notes, the best test of whether a cyber attack meets this threshold is if it results in physical destruction comparable to a conventional attack, called a “kinetic effect” [1]. In other words, the use of cyber technology to facilitate a kinetic attack that causes physical destruction would constitute an “armed attack,” while attacking a state’s financial network and causing economic damage, for example, would not. Those attacks that fall into the former category have been termed cyber warfare.
Furthermore, the legal limits to acceptable wartime conduct laid out by *jus in bello* also do not neatly apply to cyber attacks. The law lays out principles of proportionality, distinction and necessity, and the first two pose unique challenges in a cyber context. With regards to proportionality, the law prohibits “an attack which may be expected to cause incidental loss of civilian 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” [7]. However, with the explicit mention of loss of and injury to civilians as well as damage to civilian objects, this makes the principle almost impossible to apply to non-lethal, temporary cyber attacks. Except in the context of cyber-enabled kinetic attacks, cyber attacks frequently damage virtual network systems, which do not directly compare to physical death and destruction. Additionally, the *jus in bello* principle of distinction requires that attacks are restricted to military objectives, thereby distinguishing between civilian and military targets. This works in a physical war setting, as legitimate military targets are defined as positions and infrastructures that are occupied by or contribute to military action. However, given that 95% of military communications use civilian networks, this distinction is much more difficult to uphold in a cyber context, especially when attacks would take place over said networks [1].

Thus, the majority of cyber attacks do not meet the *jus ad bellum* threshold of an “armed attack” as they are not physical attacks nor do they cause physical destruction. Additionally, cyber attacks could pose serious consequences for the principles intended to regulate *jus in bello* conduct due to the unique nature of cyber networks. Therefore retributive actions cannot, and arguably should not, be justified under these sets of laws.
For these reasons, in this paper we would like to examine a broader category of cyber attacks – those that do not fall under cyber warfare – for which the legal interpretation is much murkier. We will instead look at cyber attacks that, while they encompass cyber warfare, also include attacks that are not physical in nature.

We will use the definition for this category of cyber attacks proposed by Hathaway: “Any action taken to undermine the functions of a computer network for a political or national security purpose” [1]. The first part of this definition, “any action taken to undermine the functions of a computer network,” connotes an objective-based rather than means-based approach that does not specify the weapon. This is especially important in a cyber context given that technologies are rapidly evolving, and broadens the *jus ad bellum* “armed” definition to include any type of attack with the objective of undermining a computer network. This definition encompasses a number of actions against a network, including hacking, bombing, cutting and infecting. However, this definition is also limited to attacks against a cyber entity. For example, operating a drone via a computer network would not fall under this definition since the drone is using but not attacking a network – it instead falls under traditional kinetic attacks. But bombing a group of undersea network cables, which would be considered cyber warfare due to the resulting physical destruction, would fall under this definition for cyber attacks since the destroyed items are for the purpose of attacking a computer network. The word “function” was justified by Hathaway to distinguish dismantling or attacking the network from passively observing or copying data. This reflects the distinction between espionage and offensive attacks in traditional warfare. Lastly, the phrase “for a political or national security purpose” serves to distinguish cyber attacks from cyber crimes. Cyber crimes are
defined as any illegal act committed using a computer-based means, such as internet fraud or identity theft. However, because of the interest in protecting national security, the distinction between domestic and international law and the scope of the law of war, Hathaway included this to separate cyber attacks against a state for a political purpose versus those cyber crimes that are not. For the scope of this paper, we also wish to solely examine the former category.

Examples of cyber attacks under the definition presented above include Distributed Denial of Service (DDOS) attacks, semantic attacks and secure computer network infiltration [5]. A DDOS attack is an attempt to make a machine or network resource unavailable to its users by overwhelming it with traffic from unsuspecting computers that have been hijacked by viruses. A semantic attack modifies electronic information that causes the computer system to fail while it appears to operate normally, and secure computer network infiltration can, in addition to passively harvesting information, target the secure network to disrupt its function.

**Law of countermeasures as applied to cyber attacks**

As explained above, the laws governing *jus ad bellum* only sometimes apply to cyber attacks, specifically those that have direct physical consequences. Given our broader definition of cyber attacks in the previous section, these categories of wartime laws do not apply. Instead, there has been a growing consensus among legal scholars that the international law of countermeasures could instead be applied to these cases of below threshold attacks.
The law of countermeasures regulates how states may respond to international law violations that do not rise to the level of an “armed attack” justifying self-defense under *jus ad bellum*. It provides that when a state commits an international law violation, the injured state may respond with a reciprocal act known as a countermeasure. Specifically, the Draft Articles on State Responsibility define countermeasures as “measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation” [4]. This doctrine places restrictions on said reparative countermeasures: first that the countermeasure is proportional to the initial unlawful behavior, second that the countermeasure must be targeted only at the state responsible for the wrongful act, and third that the countermeasure must be temporary and directed to induce the responsible state to cease its violation and cannot be launched if the wrongful act has ceased.

It has been proposed that in a cyber context, countermeasures would employ active defenses, which attempt to disable the source of an attack using reciprocal methods. These stand in contrast to passive defenses, which are cyber security methods that attempt to simply prevent, detect or recover from cyber attacks. Examples of such include firewalls and intrusion detection systems.

**Issues with “active defenses” as countermeasures**

However, the law of countermeasures also was not written with a cyber context in mind, and applying it to such a context brings up a number of legal and technical concerns. From a legal perspective, the law of countermeasures was never intended to be
applied to actions that constitute uses of force. In fact, Article 50 of the UN Charter explicitly states that “Countermeasures shall not affect the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations” [4]. However, in many occasions a cyber attack constitutes a “use of force” in violation of Article 2(4). In these cases, an active countermeasure that responds proportionally according to the restrictions placed by the law of countermeasures, especially if using the same method of network infiltration, would presumably also be a “use of force.” Therefore it would be a violation of Article 50 while simultaneously abiding by the law of countermeasures.

Furthermore, Article 50 is an important limit on countermeasures that should not simply be ignored in the context of cyber attacks. It prohibits states from responding with force to every illegal use of force; injured states cannot forcefully retaliate against attacks that do not reach the threshold of an “armed attack.” This limit is important in the physical sphere since without this check, small offenses would result in a sequence of retaliations that would likely increase and escalate over time. In other words, any illegal use of force could provoke a forceful response, thereby effectively eliminating the “armed attack” threshold. Not abiding by this prohibition in a cyber context would also be able to be applied to a non-cyber context, because of how laws are interpreted, and thus ignoring this limit could have grave consequences.

From a technical perspective, the law of countermeasures raises a number of challenges and concerns, specifically with regards to the regulations set on said retributive countermeasures, due to the nature of computer networks. A network is a collection of computing systems that are connected across some medium by hardware
and software that enable communication. Networks stand at much higher vulnerability for attacks than stand-alone computing systems for many reasons including [5]:

*Anonymity* – an attacker can mount an attack without coming into direct contact with the system and, because the attack can be passed through many other nodes, its origin can be disguised.

*Many points of attack* – while one computer system may enforce rigorous security policies, because of the connections between many different computing systems, it may not have control over the security of other systems in the network, thus leaving many points of vulnerability within the network.

*Sharing* – because networks enable resource and workload sharing, more users have the potential to access networked systems.

*Complexity of the system* – since the average computer can run background processes unknown to the user, an attacker can take advantage of this complexity to perform part of the attack’s computation. Augmented by the fact that there are multiple computing systems in a network further diminishes confidence in the network’s security.

*Unknown perimeter* – one computer system may be a node on two different networks, connecting the resources on one network to the users of the other network, thereby introducing uncertainty about the network boundary.

*Unknown path* – there are often many paths from one host to another and network users seldom have control over this routing, introducing another element of uncertainty with regards to security between networks.
These attributes of networks introduce many challenges for active countermeasures. First, a countermeasure must effectively cause the attackers to cease the unlawful behavior. However, because attacks can be mounted from afar and passed through many other nodes in the network, the attacker is more likely to be able to relocate their operations than in a physical attack. Second, in order for the countermeasure to be targeted only at the state responsible for the wrongful act, the identity of the attacker and origin of the attack must be accurately identified. This is a difficult problem to solve when dealing with networks due to their connectivity and unknown perimeter and path that allow an attack to pass through multiple nodes and disguise its origin. Lastly, the countermeasure must injure only the attackers. Again, due to the connectivity of networks, this is much more difficult than in a non-cyber context. Since an attack through a network passed through many nodes, launching a countermeasure to disable said attack could require disabling those nodes, many of which might have been unknowingly used to launch the attack. These last two points are especially true in DDOS attacks that enlist unsuspecting computers to launch the attack, making accurate attribution and a directed countermeasure uniquely difficult.

Finally, the requirements of necessity and proportionality for countermeasures face reduced constraints in a cyber context, threatening the purpose of said checks and possibly causing repercussions for the law. The requirement of necessity exists to establish countermeasures for corrective rather than punitive function. Article 52 of the UN Charter requires that before a countermeasure is launched, the injured state must “call on the responsible state” to cease its wrongful conduct, “notify the responsible state of any decision to take countermeasures and offer to negotiate with that state” [4].
Furthermore, an injured state cannot employ a countermeasure if the wrongful act has ceased or been submitted to an international court or tribunal. However, the article also includes an exception to this notification and offer to negotiate: “the injured state may take such urgent countermeasures as are necessary to preserve its rights” [4]. The purpose of such an exception is to prevent the responsible state from immunizing itself from countermeasures. However, in a cyber context, this exception allowing for a rapid response is much more likely to take place due to the nature of cyber attacks. Since attacks through a network can inflict damage quickly and spread rapidly and unexpectedly among nodes, they justify the injured state to take urgent countermeasures, effectively weakening the necessity requirement.

Similarly, the proportionality restriction on countermeasures also faces reduced importance within a cyber context. Article 51 of the UN Charter states that “countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question” [4]. The UN commentary on this article notes that countermeasures are more likely to satisfy the requirements of necessity and proportionality “if they are taken in relation to the same or a closely related obligation” [8]. Given that tracing the origin of a network attack would require using the same avenue as the original attack, reciprocal countermeasures especially make sense in a cyber context. Such a reciprocal countermeasure could be an automatic or manual response system that would mirror the attack back at the responsible networks. But reciprocal tactics do not necessarily produce reciprocal effects. If the countermeasure is launched at a larger network, although the tactic is the same, the effects would be amplified. It would attack a greater network infrastructure and larger
population, escalating the conflict. Thus, while the proportionality restriction makes sense in a physical context to allow for retribution but prevent the rise of conflict, the scalability and potential widespread and unanticipated repercussions of attacking a network challenges a restriction that was meant to ensure equal actions.

**Proposed alternative solutions**

Addressing cyber attacks with active countermeasures opens the door for a number of legal and technical concerns. Here, we instead propose that in an ideal network, cyber attacks would have little to no permanent damage. Therefore, we advocate for a focus on developing and emphasizing passive defenses.

Security in a computing system relies on the balance of three goals: confidentiality, integrity and availability. Confidentiality or privacy ensures that assets are accessed only by authorized parties, integrity ensures that assets can be modified only by authorized parties, and availability ensures that assets are accessible to authorized parties at appropriate times. A security breach occurs when one of these goals is compromised, and passive defenses aim to preserve these three goals. Harm – when a threat is realized against a vulnerability in a system – can be dealt with in a number of ways: preventing it by blocking the attack, deterring it by making the attack harder, deflecting it by making another target more attractive, detecting it and recovering from its effects.

As explained previously, networks can be vulnerable to attacks for a variety of reasons, but these vulnerabilities can also be mitigated though a number of security controls. For example, link encryption and firewalls protect information as it is
transmitted between computers to prevent a breach – the former by securing the message itself, the latter by filtering traffic between the inside and outside networks. In the case that an attack passes through the system, intrusion detection systems can detect it and activate an alarm to take defensive action, such as notifying users of an attacked entity or blocking the attackers’ IP addresses. Finally, network design principles such as segmentation and redundancy to eliminate single points of failure aid in recovery if the system is in fact attacked. Segmentation limits the amount of damage a single vulnerability can cause, and redundancy eliminates single points of failure in the system. In a network, it allows for a function to be performed on more than one node in case one is damaged, and in a database, it allows for rollbacks to recover lost data.

Thus, in an ideal network, any attacks would be prevented and if not, they could be recovered from. Of course, however, network security is far from perfect and practically speaking they will still stand vulnerable to attacks. However, this point is to illustrate that emphasis should be drawn towards improving passive defenses rather than employing or designing active countermeasures. Since the law of countermeasures raises a number of legal and technical concerns, other non-cyber responses should be taken in the event that a cyber attack evades passive defenses. Economic, diplomatic and political restrictions placed against the injuring state can serve as retribution without triggering the possibly escalating consequences of active countermeasures.

**Conclusion**

As the variety, frequency and potential of cyber attacks rise, it has become increasingly important for states to establish protocols to address such assaults. The law
of countermeasures has been proposed to guide retributive actions against cyber attacks that do not meet the threshold of an “armed attack” defined in *jus ad bellum*. However, allowing for active countermeasures against such cyber attacks could have a number of unintended repercussions – allowing forceful countermeasures could lead to escalating retaliations, identifying and directing a countermeasure against an attacker is uniquely difficult in network attacks, the nature of cyber attacks can justify urgent countermeasures and weaken the restriction of necessity, and reciprocal countermeasures may not have reciprocal effects and might violate the proportionality restriction. Thus, rather than using the law of countermeasures to justify retributive active defenses, we instead propose that the most effective means of warding off cyber attacks should be through strengthening passive defenses. While cyber security may not be perfect – in which cases non-cyber punitive actions can be taken – an emphasis on protection will result in stronger networks and fewer possible legal repercussions.
References

   http://digitalcommons.law.yale.edu/fss_papers/3852

   https://ccdcoe.org/cycon/2014/proceedings/d2r1s5_hathaway.pdf


   http://www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf


