Indiana University - Purdue University, Indianapolis

From the SelectedWorks of Anthony Rodin

April 26, 2012

The Ambiguity of Cyber Attacks in International Law

Anthony Rodin, Purdue University

Available at: https://works.bepress.com/anthony_rodin/2/
The Ambiguity of Cyber Attacks in International Law

In the 2007 summer blockbuster movie “Live Free or Die Hard,” a former Pentagon official unites a group of hackers with the goal of committing a “fire sale” on the primary computer systems that control American infrastructure. With just a few keystrokes, stock markets stop trading, communications go down, utilities are taken offline, and the American state is completely blind, deaf and dumb. In order to prevent the government from getting a lead on them, the villains use their cyberspace superiority to control the flow of natural gas and direct it to the pumping station where the heroes are, causing it to blow up.

As fantastic as the plot of this movie was, it is an all-too-real threat for developed societies that have come to increasingly rely on the internet to maintain and control key components of their states. Cyber attacks, part of a broader spectrum of new tools in an area called Information Operations (IO), take on many which are currently not regulated by international law. Instead, scholars have had to try to create a guideline for their usage by relying on an approach of law by analogy. Ultimately, there are simply too many questions and vague areas, which make any clear, definitive law or guidelines to the usage of IO impossible to decipher. This conclusion splits the legal community in terms of solutions to this problem. One group argues that a broad information regime needs to be established to monitor and police cyberspace. Another group argues that, rather than a broad international regime (which will likely not be ratified), the only laws that need to be created are those which govern the most

3 Id.
disruptive use of these weapons, while allowing state behavior to become customary law, and thus fill in the many gaps in the existent legal regime.

Thus there are two main questions which still lack clarity in terms of international law: Do cyber attacks constitute a declaration of war according to existing *jus ad bellum* regulations? Are cyber attacks valid forms of aggression in the current *jus in bello* regime? This paper argues that in order to best answer these questions, cyber attacks need to be parsed out in terms of both the vector of attack (virus, logic bomb, DoS, etc.) and the targets they are used against. Some forms of attacks do constitute a use of force and thus could spark a war. Also, depending on the target and the means used, cyber attacks are valid uses of force, which in some instances, should be encouraged because they are likely to result in *fewer* fatalities than conventional, kinetic attacks.

This paper further argues that the second approach, relying on customary law, is more likely to lead to produce results, as the current legal structure and norms on the use of IO prevent states from launching fully debilitating attacks on each other. Plus, there are simply too many questions and ambiguous terms that apply to IO that cannot be definitively codified. While there needs to be a basic outline on the types of attacks that are allowed in international law, a broader regime is not necessary, and is unlikely to be successfully implemented. The focus of this paper is on state-backed cyber attacks against another state. While there is significant literature on (and significant threat from) cyberattacks from non-state actors or criminal organizations, the purview of this paper will stay solely focused on attacks condoned by one sovereign state against another.

This paper proceeds in six sections. Section I goes over the basic definitions in this vein of literature, what is meant by “cyberspace” and the different types of weapons that can be used
in this realm. Section II gives case studies of IO in recent years, focusing primarily on the attacks on American defense networks dubbed “Titan Rain” in 2003, the massive disruption in Estonia in 2007, the attack on Georgian web sites in conjunction with a conventional attack in 2008 and the Stuxnet worm that hit Iranian nuclear sites in 2010. Section III examines existing *jus ad bellum* and *jus in bello* laws which scholars argue apply, at least partially, to the use of IO between states. Section IV is the main section of synthesis. It focuses on the ambiguities of international laws as they apply to IO, including whether or not IO are *sui generis*, attribution, proportionality, anticipatory self-defense and whether or not IO constitute a “use of force”\(^4\) or is a manifestation of “armed conflict”\(^5\) as outlined by the United Nations Charter. Section V delves into the argument between establishing an invasive international regime or allow state-driven customary law to overcome these ambiguities, and argues that the second school of thought is both more realistic and more likely to succeed. Section VI concludes.

Section I – Definitions

The progenitor of the creation that became the modern day internet was as a network of computers that facilitated communication between the Department of Defense and its various academic and contractor affiliates. It was hoped that this network could withstand the EMP effects of a nuclear attack\(^6\). The first manifestation of this network, ARPANET, came on line in 1969\(^7\). Since its inception, the global network has exploded, with almost a billion users\(^8\) using the internet on a regular basis.

---


\(^7\) Id.

\(^8\) Id.
This massive increase in international connectivity has coined the term “cyberspace,” which lacks a singular definition. For example, the Department of Defense defines “cyberspace” as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers”\(^9\), while the Air Force Cyber Command defines it as “a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures”\(^10\). For the sake of this paper, cyberspace is defined as the global information network, the data that flows across its space, and the physical control centers and infrastructure institutions that are tied to it.

Cyber attacks are violations and manipulation of this space with various weapons for various reasons. Cyber attacks are a form of Information Operations (IO), a broader umbrella term that will be used to mean cyber attacks and other forms of aggressive behavior in cyberspace. IO is formally defined as “seeking to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting one’s own”\(^11\). These disruptions and manipulations can come as a result of different sources and tools.

The most basic form of attack is a virus, a piece of code or program that takes root in a computer via some kind of exploitation or loophole in a system’s defense\(^12\). These viruses, or worms, then propagate either through e-mail attachments, unguarded network computers, or latching on to flash memory drives. Worms and viruses usually only target a specific program,

---

\(^8\) Id.
\(^12\) Schaap, supra at note 9
and only operate when that program is operating, remaining invisible at other times. These tools can also destroy data, clog networks and input false data in its place. A Trojan Horse is a type of worm that, rather than focusing on stealing or devouring data, instead takes control of the infected computer. So called because they are often initially innocuous when downloaded, these types of viruses turn infected computers into “zombies” which run processes dictated by the virus. A logic bomb is a specific type of Trojan Horse which remains dormant and undetectable until a certain condition is met (e.g. a certain number of computers are infected or a certain program is run a number of times). The CIA used this type of approach to destroy a gas pipeline in the USSR during the Cold War.

The tools described so far require the stealthy infiltration of a single piece of code onto a network, which, if done successfully, can cause a significant amount of damage. Another type of attack altogether is a Denial of Service (DoS) attack. In these attacks, a targetted website is inundated with a large number of requests for information, and is forced to shut down. A more powerful variant of this is a Distributed Denial of Service (DDoS) attack, where a large number of hijacked computers (usually zombies compromised by a Trojan Horse or Logic Bomb) form a single network, or “botnet”, and inundate a targeted website with bogus requests for information. This tactic can be particularly disruptive, and was the primary modus operandi in the attacks on Estonia and Georgia. Because their effects are so widespread, DDoS attacks have become known as “carpet bombing in cyberspace.”

---

13 Hollis, supra at note 11
14 Id.
15 Id.
18 Id.
These are the primary tools of the trade of IO. A cyber attack can be a single virus a wholesale DDoS against an entire country’s informational infrastructure. In recent history both methods have been applied, with devastating results.

Section II – Examples of Cyber Attacks

As the civilian internet has expanded in both size and use, the number of cyber attacks has also increased. Within the last ten years there has been numerous examples of international cyber attacks of differing types. The examples in this section look at unique examples in terms of the damage done, the method of attack, the target of the attack, and the presence or absence of an accompanying conventional attack. These examples will be used when examining the international law framework in Section III.

A. “Titan Rain” – Chinese IO Against American Targets

“Titan Rain” is the codename given to a series of attacks against American infrastructure and defense networks between 2000 and 2003. These incidents took the form of a multi-armed attack, incorporating both viruses and small-scale DoS attacks. These attacks were successful in stealing files and information from a number of American military sites and networks, including an Air Force Research and Development team at Redstone Air Force Base, and also compromised the power grid of the west coast of the US almost to the point of collapse. The US traced the intrusion back to hackers in China, which seemed to have capabilities and

---

20 Schaap, supra at note 9
21 Id.
equipment only available to its military\textsuperscript{23}. This led US intelligence officials to believe that the intrusion was at least condoned by Chinese state officials, if not encouraged or enabled by them. The result of Titan Rain was a loss of sensitive state secrets, but no physical damage was caused by the intrusion.

B. Estonia’s Blackout

From the end of April through May of 2007, Estonia was subject to a massive DDoS attack which had devastating effects on the nation’s electronic, telecommunications and financial infrastructure. It is the quintessential example of the power and reach that cyber attacks can have on a country that is fully integrated into the internet, as well as some of problems with applying the laws of war to cyber attacks.

Prior to the attacks, Estonia was a model country for developing states in incorporating the internet age into their society. The country had free wireless internet country-wide and most of the governmental and bureaucratic workings could be done entirely online\textsuperscript{24}. This heavy saturation and adaptation of the internet led to the small Baltic country being known as “eStonia”\textsuperscript{25}. It was because the country was so tightly integrated with the internet that the following attacks had such a profound effect, and why Estonia is a worrying example for other developed countries which have embraced the internet.

The attacks started on April 27\textsuperscript{th} in response to Estonia’s moving of a World War II monument to Soviet soldiers from a central park in the capital to a less public space. Diplomatic relations between Russia and Estonia cooled quickly, and on the 27\textsuperscript{th} the first hints of a cyber

\textsuperscript{23} Schap, supra at note 9
\textsuperscript{25} Id.
attack emerged, as numerous Estonian government websites were hacked and defaced with Soviet iconography\textsuperscript{26}. Over the next few weeks numerous Estonian media outlets were forced to shut down their websites, effectively cutting them off from the world and preventing them from communicating with the outside world about the attack.\textsuperscript{27} The most dire threat came on May 10, as attacks focused on telephone exchanges, communication, financial, and emergency coordination networks. Only the efforts of Estonia’s Cyber Emergency Response Team prevented a total collapse that would have caused massive social disruption, riots and fatalities\textsuperscript{28}. Even with this defense, however, more than 150 people were injured in riots and demonstrations as a result of the attacks\textsuperscript{29}.

From the beginning, Russia was the primary suspect, especially considering the fact that the attacks came during a period of tension between Estonia and Russia, and the presence of Soviet iconography on the vandalized websites. However, Russia flatly denied having anything to do with the attack, instead blaming hackers from various countries. Because the attack relied primarily on using “zombie” computers corrupted by Trojan Horses, the attacks against Estonia came from computers based around the world, including the United States, which made it difficult to track down the real culprits\textsuperscript{30}. Even now, three years later, it is still unclear who exactly was responsible and how complicit the Russian government was in instigating the attack.

C. Conventional and Cyber Attacks – Russia’s Two-Pronged Thrust on Georgia

Tensions between Russia and Georgia were high in the summer of 2008, as Georgia was increasingly violent in its attempts to rein in the breakaway regions of South Ossetia and

\textsuperscript{26} Schaap, \textit{supra} at note 9
\textsuperscript{27} Id.
\textsuperscript{28} Id.
\textsuperscript{29} Schaap, \textit{supra} at note 9
\textsuperscript{30} Id
Abkhazia, whose independence Russia supported. As tensions mounted, the website of Georgian President Mikheil Saakashvili came under a limited DDoS attack on July 19 and had to be taken offline. When the tensions in the region exploded into open war on August 7, the Russian army’s advance into Georgia was coupled with a cyber attack on Georgian governmental websites. This attack was much more widespread and severe than the earlier attack, as the governmental e-mail system went down and most of the Georgian government’s and media’s websites were forced to go offline. Even before the first shots were fired on Georgian troops in the region, Russia had already managed to cripple the Georgian government’s ability to communicate and work online. For the first time, conventional and cyber warfare worked in tandem to cripple an enemy.

The July 19 cyber attack was, in retrospect, most likely a rehearsal for the larger August attack. Much like the Estonian attack, Georgian websites were brought down by a global network of hijacked computers. However, the coordination between the August attack and actual troop movements make it likely that the Russian government was at least partially responsible for these attacks, though no formal responsibility has been claimed.

D. Precision-Guided Cyber Attacks – Stuxnet Strikes Bushehr

In 2010 technicians at energy and industrial facilities around the world found that their network had been infected with an especially malicious logic bomb. This logic bomb, dubbed

---

32 Ophardt, supra at 22
33 Korns, supra at 31
34 Ophardt, supra at 22
35 Clayton, Mark. 2010. “Stuxnet malware is ’weapon’ out to destroy ... Iran's Bushehr nuclear plant?” Christian Science Monitor, September 21.
Stuxnet from one of its file names\textsuperscript{36}, behaved differently from other viruses, in that it did not try to steal or destroy data. Instead, Stuxnet was programmed to only go after the most critical systems of industrial and energy operations, primarily systems which control centrifuges at nuclear processing plants\textsuperscript{37}. Also unlike other viruses, Stuxnet relied on not one, but four different exploits of the Windows operating system\textsuperscript{38}. Usually when an exploit is found it is quickly capitalized upon in order to profit from the exploit as much as possible before the exploit is patched by developers. Stuxnet’s array of exploits made it difficult to detect and even more difficult to eliminate\textsuperscript{39}. The most startling characteristic of Stuxnet was that it was able to infect computers that were in no way connected to the internet, and were thus not thought to be vulnerable to cyber attacks. Stuxnet was able to get to these systems through a memory stick or another form of portable memory from computer to computer\textsuperscript{40}.

Once Stuxnet was found, a sweep of global computers found that the epicenter of the viral outbreak was Iran. This clue has lead scientists to believe that the Iranian nuclear program, specifically the nuclear plant at Bushehr, was the main target. It appears to have worked too, because the plant has suffered numerous, mysterious delays in getting under way\textsuperscript{41}. The coding of the virus shows that it has a unique ability to target not only specific systems, but only certain versions of those systems. In other words, unless a system matched the very specific requirements built into the worm, the virus left the computer alone and was completely dormant. This has led one technician to dub Stuxnet “a 100-percent-directed cyber attack aimed at destroying an industrial process in the physical world…a guided cyber-missile”\textsuperscript{42}. No country

\textsuperscript{36} Id.
\textsuperscript{37} Id.
\textsuperscript{38} Id.
\textsuperscript{39} Id.
\textsuperscript{40} Id.
\textsuperscript{41} Id.
\textsuperscript{42} Id.
has come forward to claim responsibility, but the sophistication and target choice has led many
to believe that either the United States or Israel is behind the virus.

Each of these attacks are unique, and together they highlight the broad spectrum that IO
encompass. Titan Rain was primarily an intelligence mission, which almost created destructive
physical manifestations. Estonia suffered probably the largest DDoS attack ever seen which
effectively put in the dark, and was very close to full blown electronic collapse. Georgia was
assaulted through both conventional on electronic means. Iran was the target of the first virus to
be so specifically targeted to cause physical harm to a certain target. Which of these attacks, if
accurate and timely attribution of the guilty parties could be made, were aggressive acts that
could have sparked a war? Which of these attacks violate international humanitarian law, which
set the guidelines for acceptable behavior in conflict?

Section III – The Existing International Law Regime

Current international law on armed conflict (LOAC) is divided into two sections: *jus ad
bellum*, or laws regarding the initiation and causes of war, and *jus in bello*, or international
humanitarian law (IHL) regulating the types of weapons and behavior which is acceptable in the
conduct of a war. In both of these areas, IO falls into a gray area, leaving much up to
interpretation.

A. The Development of the Contemporary *Jus Ad Bellum* Regime

War between two sovereign states is partly the result of the Westphalian system which
defines the international community today. States are the primary units in this anarchic system,
and violent conflict between them releases the most destructive forces mankind can wield. Since
the inception of the Westphalian system in 1688 there have been numerous attempts at crafting
constraints and laws which limit the conditions when interstate war would be acceptable.
However, prior to the United Nations Charter of 1945, these attempts, such as the League of
Nations Covenant\textsuperscript{43} and the Kellogg-Briand Pact\textsuperscript{44}, had little success in curbing the outbreak of
war.

Contemporary \textit{jus ad bellum} law is built on the United Nations Charter, which both limits
Members shall refrain \ldots 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”}\textsuperscript{45}. Thus, state are not allowed to use for or threaten to use force against another
state. The problem with applying Article 2(4) to IO is that the term “force” is not fully defined.
This is a problem that will be elaborated on in Section IV.

While Article 2(4) limits states from using or threatening to use force (whatever that term
may mean), the Charter does not forbid any violent interstate actions. There are some instances
where states may be allowed to go to war against another state. These exceptions are found in
articles 39, 42 and 51. Article 39 empowers the Security Council \textquote[Id.]{“to determine the existence of
any threat to the peace, breach of the peace, or act of aggression and shall make
recommendations \ldots to maintain or restore international peace and security”}\textsuperscript{46}, and, should these
threats be found to endanger international peace, Article 42 states that the Security Council \textquote[Id.]{“may


\textsuperscript{46} Id.}
take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security”\textsuperscript{47}. Together, articles 39 and 42 give the Security Council the power to ensure international peace and security through violent means if a state is found to be in violation of Article 2(4). If IO become a more accepted form of use of force, Article 42 may have to be amended or adjusted to include cyberspace in the areas that the UN may take action in.

The only time when a state can commit an act of interstate violence independent from the Security Council can be found in Article 51, which states “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”\textsuperscript{48}. If a state comes under attack, they are allowed to respond without the blessing of the Security Council. However, applying Article 51 to an IO-based attack requires a clear definition of what an “armed attack” is. Can the use of cyber weapons be seen as an “armed attack,” or are they outside of this vein of thought? This will also be examined in Section IV.

While Article 51 gives states the right to act in self-defense, an earlier event that has become customary international law gives states the right to act in self-defense before an actual attack takes place. The \textit{Caroline} case resolved that states can act in anticipatory self-defense in cases where the “necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation”\textsuperscript{49}. The notion of anticipatory self-defense is another gray area for IO, which will be examined later.

\textsuperscript{47} Id.
\textsuperscript{48} Id.
In 1974 the UN attempted to resolve some gray areas by defining “aggression,” to help parse out which types of behavior were legal and which were illegal in relations and actions between states. The 1974 General Assembly Resolution XXIX “(1) limits aggression to the use of traditional armed force, (2) is highly State centric, (3) uses examples of traditional aggregated warfare, and (4) relies on traditional concepts of territorial integrity”\(^{50}\). Much like Article 2(4), however, it is difficult to discern if IO fall under “traditional armed force” or not, since modern cyber weaponry was far from the realm of possibility when the definition was crafted.

In sum, the current *jus ad bellum* regime regulates conflict based on ambiguous terms like “force,” “armed attack” and “traditional armed force.” Just how well IO fits with these terms will be examined in a later section. For now, it is clear that there are gray areas which exist in the current *jus ad bellum* legal regime, which cannot fully account for the presence and many uses of IO.

B. International Humanitarian Law: *Jus In Bello*

When wars do break out, “the right of belligerents to adopt means of injuring the enemy is not unlimited”\(^{51}\). Over time, certain weapons and forms of behavior have been prohibited from use in war for a number of reasons. Applicable to the conversation on IO, the main laws which are pertinent here regard military necessity; distinction between combatants and non-combatants (or military vs. civilian targets); proportionality of the attack to the threat; limiting unnecessary suffering; perfidious behavior; and the right of states to be neutral in conflict, and that neutrality should be expected\(^{52}\).

\(^{50}\) Ophardt, *supra* at 22, at 4

\(^{51}\) Convention With Respect To the laws and Customs of War on Land (Hague II), July 29, 1899 at Article 22

\(^{52}\) Basic organization of IHL from Schaap, *supra* at note 9
Military necessity refers to the military capabilities of a selected target. Attackers are expected to choose targets that have high military value and avoid those which have low military, yet high civilian, value. This imperative comes from Article 52(2) of Additional Protocol I to the Geneva Convention, which has been accepted as customary international law.\(^{53}\) The Article defines a military attack as being legal only when they are “limited to 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”\(^{54}\).

Additional Protocol I also provides the foundation for the requirement of distinction between combatants and non-combatants. These two classes of person receive drastically different levels of attention and care during conflict. The basic premise of the Protocol, as stated in Article 48, is “in order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives”\(^{55}\). Coupled with the concept of necessity, warring states thus need to ensure that the targets chosen for attack have both military necessity and do due diligence in protecting enemy non-combatants.

Just choosing an appropriate target is not enough, however. The targets need to be attacked with the appropriate, proportionate level of force. This concept “prohibits the use of any kind or degree of force that exceeds that needed to accomplish the military objective”\(^{56}\). The

---

\(^{53}\) Schiap, \textit{supra} at note 9

\(^{54}\) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, accessed from http://www.icrc.org/ihl.nsf/7e4d08d9b287a42141256739003e636b/f6e8b9fee14a77fde1dc125641e0052b079 on Nov. 13, 2010

\(^{55}\) \textit{Id.}

\(^{56}\) Schiap, \textit{supra} at note 9, at 151
concept of proportionality can be found in Article 51 of Additional Protocol I. Article 51(b) states “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” would be deemed indiscriminate, and thus illegal under the Protocol. Military targets therefore need to be attacked with an appropriate weapon, one which will limit the amount of collateral damage suffered by civilians. Failing to do so breaks the Protocol, and thus breaks international law.

The Hague Convention IV of 1907 also places limits on the tools which can be used to wage war. Specifically, Article 23(e) states attacks which “employ arms, projectiles, or material calculated to cause unnecessary suffering” are illegal in the conduct of war.

The types of weapons used and their targets are not the only things that are limited in jus in bello law. The behavior of individual combatants is regulated as well. Specifically, perfidious or treacherous behavior is forbidden by international law, as “it destroys the basis for a restoration of peace short of the complete annihilation of one belligerent by another.” The Hague convention speaks to this in Article 23(b), where it forbids acts which “kill or wound treacherously individuals belonging to the hostile nation or army.” Protocol I to the Geneva Accords also prohibits perfidy, specifically in Article 37(1) which says “it is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of

---

57 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), supra at note 54
58 Schaap, supra at note 9
60 Schaap, supra at note 9, at 152
61 Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, supra at note 59
international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy. It then goes on to give examples of perfidious behavior, which includes the falsification of surrender, of suffering wounds or incapacitation, of being a non-combatant, and wrongly adopting international symbols which ensure safe passage.

Finally, states engaged in conflict need to respect those states which are not a party to the conflict, which have declared themselves to be neutral. These states are immune from attack, so long as they too abide by the rules of neutrality, such as not allowing combatant states to stage forces in their territory and equally allowing transport through their borders. Neutrality poses a large problem in terms of IO, as the interconnectedness of the internet and other information networks makes it hard to discern what areas of cyberspace a country has sovereignty over.

This and other issues of neutrality will be examined in the next section.

There are numerous other laws and regulations which dictate the type of weapons, attacks and behavior which are acceptable in the conduct of interstate war. However, the six areas listed above highlight some of the larger problems in fitting IO into the *jus in bello* legal regime.

Section IV – Challenges Applying Existing Laws to IO

The previous sections have identified what is meant by IO and cyber attacks, their many forms, recent examples of their use, and the current legal foundation underlying interstate conflict. This section will synthesize the findings up to this point and show that IO are far from a perfect fit in the existing legal structure. Recommendations for overcoming these flaws and ambiguities will come in Section V.

---

62 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), *supra* at note 54
63 *Id.*
64 Schaap, *supra* at note 9
A. IO are *sui generis*

Cyber weapons are wholly unique for two reasons: their stealth and deniability, and their potentially catastrophic effects.

First, IO are the ultimate stealth weapon. For armies and weapons in the physical world, there is the ever-present risk of detection by the defending states. With modern satellite technology, other states know when armies are staging for an assault, when strategic bombers are fuelling and arming up for a strike, and where naval assets are. Even missile strikes give a modicum of warning time for the target nation after they are launched. IO on the other hand can come completely from out of the blue with absolutely no warning. Stuxnet, for example, was present on computers for months before being picked up\(^65\). The attack on Estonia came with no warning or detection, giving the Estonians no time to mount some kind of defense for their network or boost capacity\(^66\).

The stealth capability of cyberweapons means not only that the victim has no idea the attack is coming, but that they have little chance of quickly identifying who is responsible. Even though the attacks against Estonia\(^67\) and Georgia\(^68\) were presumed to be of Russian origin, no definitive evidence has emerged, years after the attacks took place. The initial “dress rehearsal” against Georgia, for example, came primarily from computers based in the United States\(^69\). The Stuxnet worm’s creators are still unknown\(^70\). In the physical world, any attack from an air raid to a commando raid usually leaves traces of evidence which make the identity of the attacker a total

---

\(^65\) Clayton, *supra* at note 35
\(^67\) *Id.*
\(^68\) Korns, *supra* at 31
\(^69\) *Id.*
\(^70\) Clayton, *supra* at note 35.
certainty. This certainty does not exist with IO, as the internet allows attackers to mask their origins or use zombie computers located around the world to hide their true identity.

Second, when an IO is underway, there is no way for either the victim or the attacker to know exactly how much damage the attack will cause. During Titan Rain the power grid of the west coast was almost completely shut down. It is unknown, though thought to be unlikely, that the Chinese had any desire to actually disable the entire power grid, as it could have caused a larger provocation. Attacks like the one suffered by Estonia could have numerous “higher order” costs, as society itself breaks down from lack of communication, utilities and emergency management and suffering total financial collapse. These effects cannot be controlled by the attacker once a virus is let loose. However, this may be changing, as the Stuxnet worm shows that viruses are beginning to be created to function only in the most specific of circumstances and target only very specific systems. If this trend continues, this sort of micro-precision may establish more control for the attacker, as they can design their attack to eliminate systems which are strictly military in nature.

Because they can strike with literally no warning, their progenitors can take years to uncover (if at all), and their damage potential is beyond the control of both the attacker and the victim, cyber weapons are sui generis. It is precisely because of their unique nature that IO cannot find a place in the existing jus ad bellum and jus in bello legal structures without bringing up questions of applicability and definitions.

---

71 Ophardt, supra at 22
72 Schaap, supra at 10
73 Clayton, supra at note 35
B. IO and *jus ad bellum* – When is a cyber attack an actual attack?

The most debilitating cyber attack was doubtlessly the one suffered by Estonia. The attack posed a significant problem to Estonia’s defense minister, Jaak Aaviksoo, who had to decide whether or not to implement Article 5 of the NATO treaty (of which Estonia was a party to), which considers an “armed attack” against one member state to be an attack against all. But did Estonia suffer an “armed attack”? No missiles were fired, no physical property was destroyed, no army infiltrated Estonia’s borders. Had Aaviksoo declared the cyber attack to be an armed attack, the full weight of NATO could have been wielded against the (unknown) perpetrators of the attack. In the end, Estonia asked for technical help from NATO with dealing with the cyber attack, but did not invoke Article 5.

This scenario highlights the central issue with IO in the *jus ad bellum* legal regime. The laws and principles mentioned earlier, primarily the United Nations Charter, give seemingly-clear rules regarding when the use of force is appropriate in international relations. However, terms like “use of force” do not cleanly apply to IO. Traditionally, force has meant physical, not economic or political, coercion. However, as the attack against Estonia proved an IO attack can have debilitating consequences without ever having a physical manifestation.

Where do IO fall then? How can political, intelligence and economic coercions (which are legal uses of coercion) be weeded out from those attacks which might have physical manifestations? One of the primary arguments is to look not at the attack itself, but rather at the consequences of the attack. Those attacks which *cause* physical damage, intentional or not, should be construed to be uses of force under Article 2(4) of the United Nations Charter and thus

---

74 North Atlantic Treaty art. 5, Apr. 4 1949
susceptible to UN condemnation and interference, as well as giving the aggrieved nation the green light to respond with force\textsuperscript{77}.

IO which are uses of force can be discerned from legal forms of IO by applying a six-fold test to the actual consequences of the attack. First, severity: did the attack threaten physical damage and property more than other types of attacks\textsuperscript{78}? Second, immediacy: negative consequences are usually quicker to manifest themselves as a result of a physical attack than an economic or political one\textsuperscript{79}. Third, directness: guilty acts in and of themselves usually produce physical coercion more than alternative forms of coercion\textsuperscript{80}. Fourth, invasiveness: acts of physical coercion usually extend solely into the borders of the aggrieved, while other forms of coercion exist outside of the victim’s borders\textsuperscript{81}. Fifth, measurability: physical uses of force leave their mark in easily measurable ways, usually in terms of amount of physical damage caused, while other forms cannot be measured as easily\textsuperscript{82}. Finally, legitimacy: the use of the force is seen as being prima facie illegal in the international realm unless a claim of self-defense is invoked\textsuperscript{83}. In sum, the goal of this test is to weed out which attacks using IO are actual attacks from those which fall under protected forms of coercion and espionage.

The problem with the consequences-based approach is that, even though it tries to account for immediacy, the full damage done by IO can take a significant amount of time to fully ascertain. Titan Rain ran over the course of a number of years\textsuperscript{84}, and Stuxnet had been operational for months before the severity and scope of the infiltration was discovered\textsuperscript{85}.

\textsuperscript{77} Id.
\textsuperscript{78} Id.
\textsuperscript{79} Id.
\textsuperscript{80} Id.
\textsuperscript{81} Id.
\textsuperscript{82} Id.
\textsuperscript{83} Id.
\textsuperscript{84} Ophardt, supra at note 22
\textsuperscript{85} Clayton, supra at note 35
Second, the use of legitimacy as a determinant of the validity of the attack is legally backwards, as “it requires determining the legitimacy of an attack under international law by asking whether the attack is legitimate”\textsuperscript{86}.

A more clear-cut approach towards an effects-driven determination looks at the effect of the attack to see if there was any actual physical damage. If so, and if the damage is similar in nature to the amount of damage caused if the attack came from kinetic-based weapons, then the attack violates Article 2(4) and was a use of force. Every act short of that falls under the umbrella of acceptable uses of IO in international relations\textsuperscript{87}. The problem with this vein of thought is that attacks which are massively disruptive to a society, such as the DDoS attacks suffered by Estonia and Georgia, yet results in no physical damage, are allowed. These attacks are massively detrimental to a state and should be considered a use of force simply because of the scope of disruption.

Another problem applying existing \textit{jus ad bellum} laws to IO is the concept of self-defense. Because IO can strike with literally no warning, it is impossible for states to truly know when they are about to be attacked. While states should be allowed to respond to IO which are construed as a use of force, applying the \textit{Caroline} rules in regards to IO is difficult. Using IO as a tool of anticipatory self-defense has drawn numerous criticisms: “A cyber attack should never be allowed as a first strike. It is too easy to start wars this way, and retaliation can be just as easy, just as quick, and just as reckless as traditional warfare”\textsuperscript{88}. Thus if it does come out that Israel was responsible for the Stuxnet worm, and that it was used as a form of anticipatory self-defense

\textsuperscript{86} Barkham, \textit{supra} at note 2
against the Iranian nuclear program, it would be in violation of this vein of thought and could be open to Iranian retaliation.

Another problem incorporating IO into the laws of *jus ad bellum* is the fact that, even if cyber attacks were found to be uses of force, conclusively identifying the aggressor state is an almost impossible task. In each of the examples in Section II, no aggressor state has been conclusively proven. In the Estonian and Georgian cases, the attacks were indeed masterminded and coordinated in Russia, primarily in Russian nationalist chat rooms\(^\text{89}\), yet no clear tie between the attackers and Russian officials has been found. In the case of Estonia, the only arrest for the attacks was of a Russian national living in Estonia\(^\text{90}\).

Because IO use hijacked computers around the world, expecting victimized nations to both deflect a sudden, incapacitating strike and be able to trace the attack to a specific state is unreasonable. And again, even if the attack was traced back to a certain state, there needs to be a clear tie between the officials of that state and the attackers. Cyber attacks, due to the comparatively low amount of technical expertise and start-up capital necessary to launch them, can be launched by a dedicated group of hackers or other non-state actors. Thus, in some instances, cyber attacks could be a matter for criminal, rather than international, law.

In sum, IO do not fit well within the contemporary *jus ad bellum* legal structure. First, it is unclear whether all, some, or no forms of IO are “uses of force” as stipulated by Article 2(4) of the United Nations charter. Attempts to differentiate IO from economic and political coercion, either through a consequence-based or physical-effects based test, are incomplete or unreasonable, especially given the nature of IO. Second, because of their ability to come with no warning and the odds of their use increasing provocation, cyber attacks should not be

\(^{89}\) Schaap, *supra* at note 9  
\(^{90}\) *Id.*
considered a viable weapon for anticipatory actions of self-defense. Finally, because IO can be launched from hijacked computers around the globe, victims will have a hard time accurately and quickly identifying the attacking state, while concomitantly trying to mitigate the damage. Even if the attacker is found, differentiating the attack from an act of criminal behavior or terrorism perpetrated by non-state agents would be difficult. Thus a state would not know how to react, or against whom.

C. IO and *jus in bello* – Encouraged yet Reviled

As examined in section III, modern international humanitarian law (IHL) has six central components: military necessity, distinction, proportionality, limiting unnecessary suffering, perfidy and neutrality. In some of these areas, IO are in clear violation, while in others, the use of IO should actually be encouraged over other, kinetic forms of attack. As a result, blanket prohibition or allowance of IO are not reasonable recommendations. Instead, IO need to be regulated to prevent instances where IHL is violated, yet allowed in instances where it does not. These rules will be discussed with the assumption that a state of war exists between the attacking and the victimized state. Thus the goal of this section is to examine when IO can be used as a legitimate part of a state’s arsenal, and when they should be avoided.

Evaluating the military necessity of a certain target is a difficult task, especially in cyberspace. Attackers in the physical realm can differentiate between an air force base and an airport, or a military convoy and civilian traffic with relative ease. In cyberspace, however, the increasing amount of interconnectedness of information and communication networks means that there is significant overlap between civilian and military networks. Titan Rain is an excellent example of this. The files which were taken from Redstone Air Force Base were perfectly
legitimate targets for IO. However, the attack had wider consequences and almost plummeted the West Coast into blackout. Cyberspace is home to relatively few purely military targets.

Most of the attractive targets, including communication centers, aircraft radar systems, emergency management and transportation nodes, are dual-use targets, or used for both military and civilian purposes. Article 52(2) of Additional Protocol I stipulates that these targets can only be legitimate targets for attacks when the target “makes an effective contribution to the enemy’s military action” and “its destruction must provide a definite military advantage to the attacker”\(^91\). Applying this rubric to the attack against Georgia, the attacks against government e-mail servers could be seen as an appropriate dual-use target, as it prevented communication between the commander in chief and his forces. However, the vandalism of President Saakashvili’s website was not a valid target, as the site served no military purpose\(^92\).

A related corollary to military necessity is the concept of distinction between combatants and non-combatants. IO need to develop further to fully satisfy this rule. The attack against Estonia targeted civilian infrastructure and posed significant threat to the basic services necessary for Estonia to function not just as a military entity, but as a state overall. The attack had no distinction between civilian and military targets, wreaking havoc on the entire country\(^93\). However, new forms of IO show this problem is starting to be overcome by increasingly sophisticated weapons, like the Stuxnet worm, which can effectively discern between targets and pose little threat to systems that it inadvertently spreads to\(^94\).

Some forms of IO violate, while others are actually the preferred tool for use according to, the third tenet of IHL: proportionality. The attack on Estonia, for example, clearly violates

---

\(^91\) Schaap, *supra* at note 9, at 157  
\(^92\) Korns, *supra* at note 31  
\(^93\) Ashmore, *supra* at note 66  
\(^94\) Clayton, *supra* at note 35
proportionality, as its effects were similar to an electromagnetic pulse attack or sustained air raid targeting infrastructural targets. It is because of attacks like the ones against Estonia and Georgia that both the United States and Russia have publicly declared that they will respond to such attacks with nuclear weapons. DDoS attacks can be devastating and indiscriminate and are disproportionate in their means. However, here again the Stuxnet worm shows that IO may be developing to comply with IHL. Stuxnet’s ability to so specifically target a particular system shows that future IO may be able to pinpoint their attacks against targets which are appropriate and proportionate for the level of conflict.

Much of the above about proportionality can also apply to the requirement of attackers to limiting unnecessary suffering. The massive disruptions caused by DDoS attacks do nothing to ensure that the suffering of civilians is limited. Instead, massive communications and power outages spread suffering across the entire country, and threaten anyone from hospital patients to commuters to utility technicians. Once the IO genie is out of the bottle, its effects are almost impossible to contain by either the attacker or the victim.

However, attacks that use new versions of IO should actually be encouraged over attacks that rely on kinetic weapons because they are better able ensuring that collateral damage will be minimal. The Stuxnet worm was allegedly able to knock out an Iranian nuclear power plant without causing any actual physical damage or injuries. Assuming that this was an Israeli weapon, Stuxnet managed to accomplish a mission that would have required almost 50 Israeli Air Force planes and hundreds of bombs through kinetic means. An Israeli air raid doubtlessly

---

96 Id.
97 Raas, Whitney, and Austin Long. 2007. "Osirak Redux?: Assessing Israeli Capabilities to Destroy Iranian Nuclear Facilities." International Security 31 (4):7-33. The strike package necessary to ensure the destruction of Iranian nuclear processing facilities after suffering the attrition that long flights over Iranian territory would create was estimated at a total of 60 attack aircraft, not counting supporting tanker aircraft. Almost all of Israel’s inventory of
would have cost lives, both Israeli and Iranian, and collateral damage from errant bombs or
downed planes was well within the realm of possibility. In this case, using IO was actually more
in compliance with IHL than a kinetic attack. These types of attacks should be encouraged, as
they can be incredibly precise, even more so than precision-guided bombs, and can thus end up
saving lives and limiting unnecessary suffering.

While IO may be more precise and can limit the suffering of the victims more so than
kinetic attacks, they are also more prone to perfidious behavior. Of special interest here are
DDoS attacks which hijack computers in other countries. In effect, these attacks, if sponsored by
a state and are uses of force, mask themselves by adopting non-combatant identification.
Personal computers of civilians, neutrals and other non-combatants are hijacked for nefarious
means by an attacking state. Other forms of IO are less perfidious, depending on their vector of
attack.

The final tenet of IHL, neutrality, is hard to discern in cyberspace. There are no borders,
no clear demarcation between sovereign entities online. How much sovereignty can states claim
in cyberspace? The answer, so far, is: not much. While states can control economic
transactions and police content for violations of laws, they cannot claim an intrusion into their
online sphere as an attack akin to violation of territorial borders. The main problem regarding
neutrality is DDoS attacks, which use assets in neutral nations and effectively weaponizes them.

The attack against Georgia highlights two areas where IO do not cleanly fit with the
modern definitions of neutrality. First, during the “dress rehearsal” to the attack on July 19,
American computers were used to test Georgia’s defenses. During the actual attack on August 8,
computers around the world were used to oversaturate Georgia’s computer network\textsuperscript{99}. This is analogous to using neutral territory (and even weapons of neutral states) in the commission of interstate war. This strongly violates the rules regarding neutrality.

The second area of concern emerged when an American company, without informing or asking permission of the American government, contacted Georgian officials and helped them move their governmental websites and e-mail accounts to American domains\textsuperscript{100}. This violated America’s stated neutrality in the conflict, as it was openly and unequally aiding a combatant to the detriment of another. Once the websites were moved to American domains, the attacks continued\textsuperscript{101}. Thus, while the websites had Georgian content and were arguably viable targets for Russian agents, they were based in American cyberspace. In instances like this it is unclear who exactly is in the wrong, by how much, and who gets to demand justice, and what form that justice should take\textsuperscript{102}.

In sum, certain types of IO violate certain basic rules of IHL. The biggest offender are DDoS attacks, which are indiscriminate, can cause unnecessary humanitarian suffering, are inherently perfidious and violate neutrality. On the other hand, advanced new forms of viruses, like Stuxnet, which are supremely precise in terms of target selection, should actually be encouraged in lieu of physical, kinetic attacks, as they are much more able to limit collateral damage and suffering of non-combatants. The current approach to incorporating IO to international law does not differentiate between different forms of cyber attacks. However, as this section showed, only some forms should be prohibited, while others encouraged.

\textsuperscript{99} Korns, \textit{supra} at note 31.
\textsuperscript{100} \textit{Id.}
\textsuperscript{101} \textit{Id.}
\textsuperscript{102} Kanuck, \textit{supra} at note 98
Section V – Crafting an IO Treaty

The previous two sections show that there is a significant amount of gray area regarding IO in international law. There is thus plenty of room for a comprehensive international law for IO (ILIO) in international relations. Just how stringent this treaty should be, and how much power the UN should have, has been an issue of debate between legal scholars. However, in examining the issues that need to be resolved, and the capabilities and characteristics of IO, the best solution would be to craft just a very basic framework, prohibiting the most destructive forms of IO (mainly DDoS attacks) yet allowing for other forms (Trojan horses, viruses, etc.). While this approach does not resolve every issue, it allows for customary international law to fill in the gaps. This approach is much more restrictive than other proposals, but it is also more likely to actually be adopted and mitigate future uses of IO.

First and foremost, it is crucial to understand that the genie is already out of the bottle, that IO cannot be contained or prevented from proliferating. Cyber attacks have increased in frequency in the last ten years, as the internet and the interconnectedness of information networks and infrastructure has permeated the globe. As the globe becomes more interconnected, states are devoting more attention to IO, both in terms of aggression and defense. Because of the comparatively low amount of start-up funds and technical expertise required to facilitate IO, it is now thought that more than 140 countries have or will soon have IO capabilities.\(^\text{103}\)

Since IO are now available to the majority of states (as well as a significant number of non-state actors), proliferation prevention is pointless. The focus of ILIO should be to clarify when IO can be used, through what methods, and how this can be enforced, if at all. Once these

---

\(^{103}\) Schaap, *supra* at note 9
questions have been answered, the proposed ILIO needs to be feasible and acceptable to states, to ensure that it enters into force.

The first question ILIO needs to answer is: do IO constitute “uses of force” under Article 2(4) of the United Nations Charter? Unfortunately, this is a question that ultimately lacks a blanket answer. Some forms of IO, especially those which result in physical destruction (such as overheating a generator\textsuperscript{104}), should be easy to identify as uses of force, as their consequences are the same as kinetic attacks. The problem comes with discerning purely cyber attacks which disable systems and websites, yet do not have a physical manifestation. In these cases, it is better to let the individual country decide how to best respond, and thus allow customary law to fill in the gaps.

This is not the first time that a wholly unique weapon has emerged on the battlefield and posed difficult questions. The advent of the atomic bomb changed the strategy and components of modern war practically overnight. While a nuclear weapons legal regime eventually came into being, starting with the Nuclear Non-Proliferation Treaty (NPT) in 1968 and numerous successive legal structures, it took more than twenty years to do so. During that time, the United States and Soviet Union each encountered numerous situations where the nuclear option was at least on the table\textsuperscript{105}. These states were forced to come to decisions about the limits and guidelines for using these terrible new weapons without any formal international treaties. The

\textsuperscript{104} Schaap, \textit{supra} at note 9. The Department of Homeland Security showed just how feasible this is when it ran the Aurora Generator Test. The goal of the test was to cause a power generator to overheat using basic, off-the-shelf software. Within an hour, the generator was running well above recommended speeds, and within two hours the generator dramatically failed.

\textsuperscript{105} Yengst, William C. et al. 1996. “Nuclear Weapons That Went To War.” United States Department of Defense: Defense Special Weapons Agency, San Diego, CA. This report highlights numerous crises where nuclear weapons usage was at least discussed and the weapons themselves were deployed. Prior to the NPT in 1968, the United States discussed using nuclear weapons against North Korean forces in the Korean War; creating a nuclear ring of fire around Dien Bien Phu to relieve French forces under siege from the Viet Cong; against Egyptian and Jordanian forces should the Lebanon Crisis of 1958 erupt into war; and during the height of the Cuban Missile Crisis. In all of these instances, decisions on nuclear use was guided by \textit{realpolitik} and geopolitical concerns, since no comprehensive international law on nuclear weapons existed.
same approach should be applied to ILIO, especially with those cases where the attack causes significant damage in cyberspace yet has no physical effects.

Most proposals for ILIO incorporate the United Nations to a significant degree, including the creation of an agency like the International Atomic Energy Agency to monitor global networks for pernicious activity and helping those afflicted by IO attacks, primarily DDoS attacks, identify the attacker\textsuperscript{106}. However, this is too obtrusive into the networks of sovereign states, and is unlikely to be accepted\textsuperscript{107}. Instead, the main role of the UN, especially the Security Council, should be to quickly assess a cyber attack and make context-driven decisions about whether or not they constitute a use of force. In times when this should fail, and a state feels they are under attack regardless of the Security Council’s decision, the afflicted nation should still be allowed to proportionately respond. Russia and America’s promises to use nuclear weapons in response to a widespread DDoS attack are more likely to deter would-be cyber attackers than a Security Council resolution. If other states adopt a similar attitude, there would be little need for a central arbiter, since the law of power (which defines the Westphalian system today) will dictate just how far IO can go before starting a war.

In terms of IHL, however, the role of ILIO should be to parse out the different forms IO into acceptable and unacceptable weapons. Primarily, ILIO needs to make DDoS attacks and other weapons of mass disruption illegal. They violate numerous tenets of existing IHL and can create massive amounts of casualties if left unchecked. There is no reason for them to be used, especially as newer cyber weapons come on line. On the other end of the spectrum, weapons like Stuxnet should be permitted under ILIO, so long as their use complies with existing IHL. This new generation of cyber weapons should not only be allowed, but actually encouraged to be

\textsuperscript{106} Barkham, \textit{supra} at note 86.  
\textsuperscript{107} \textit{Id.}
used. Primarily, in instances where an attacker is considering using physical force, they should instead turn to IO if they have the capability to do so. These attacks are more in line with existing IHL than kinetic attacks, as they pose less danger to non-combatants through collateral damage and because they can accurately (if so programmed) discern between civilian, military and legitimate dual-use targets.

In sum, a new ILIO, in order to be both effective and practical, needs to lean heavily on states and customary law to discern when IO are appropriate uses of force and when they evolve into armed conflict. The ILIO proposed here is less of an NPT treaty, and more of a START, in that it does not prevent proliferation and says very little about when the use of IO constitute acts of war. What it does focus on is discerning legal IO from illegal forms, primarily allowing (and even encouraging) worms like Stuxnet while banning the massively disruptive, indiscriminate DDoS attacks which violate established IHL of neutrality, perfidy and discrimination. While this solution isn’t perfect, it does limit the most destructive forms of IO and hopefully results in fewer DDoS attacks, as well as the level of non-combatant suffering from physical attacks.

Section VI – Conclusion

The goal of this paper was to examine the current state of international law as it relates to the use of IO and attempt to remedy some of the shortcomings. Through a combination of allowing customary law to answer the harder questions and limiting the more destructive forms of IO, the international community can incorporate IO into the existing legal regime of *jus ad bellum* and *jus in bello* laws. While IO are *sui generis*, they also need to be regulated. The proposed ILIO will limit the most damaging forms of IO, while allowing other, more advanced forms to be used. This combination makes the proposal both effective and practical, as it is not
as intrusive as other ILIO proposals, which suggest an invasive UN monitoring agency akin to the IAEA.

IO have been used in the past ten years for many uses, some legal, others illegal. This paper has shown where the lines should be drawn and what forms should be permissible and others reviled. With this basic outline of an ILIO, hopefully future conflicts in cyberspace won’t be as destructive.