The Degrees of Force Exercised in the Cyber Battlespace

Joseph Bussing [*]

Introduction

Each instance of communication via the Internet depends on the transfer of confidential, readily available, and authenticated information. If this information is read, altered, or forged in any way, it jeopardizes the secure and safe operation of any service depending on the transfer of data. Thus, the exploitation of data can be leveraged in ways that can have devastating effects on modern societies. The problem with a networked society is that the international conventions on the use of force fail to sufficiently safeguard the world from the instability caused by computer attacks. This article seeks to remedy the situation by defining what kinds of actions carried out via computerized networks constitute a use of armed force or armed conflict.

This article applies the existing Laws of Armed Conflict (LOAC) to three cases of computer-based attacks carried out by nation-states. In doing so, the aim is to highlight the legal limitations on actions that can be taken to respond to computer attacks. The first examination involves the wave of cyber attacks that precluded the 2008 South Ossetia War between Russia and Georgia. The second case addresses the United States' covert operation, codenamed "Olympic Games." For this case, the analysis will be focused on the Stuxnet computer program. The third case utilizes LOAC to assess the acts of digital espionage carried out by the Chinese People's Liberation Army Unit 61398.

Using LOAC as a legal rubric, the cases suggest that there are three distinct interpretations of computer-based operations. The case of the 2008 South Ossetia War constitutes a situation in which using computers to attack another country can be interpreted as a use of force and as an act of armed conflict. The "Olympic Games" operation reveals that a computer-based attack can be considered a use of force but not an act of armed conflict. The analysis of the actions of Unit 61398 shows a perspective on computer attacks that are neither a use of force nor an act of armed conflict. Each case expresses unique characteristics of operations in cyberspace. Therefore, in order to develop a legal understanding of these cases, the analysis favors an effects-based assessment of cyber attacks, pioneered by Michael Schmitt and expressed in the Tallinn Manual on the International Law Applicable to Cyber Warfare.[1]

---

[*] Joseph Bussing was born and raised in the Silicon Valley of California. He is a recent graduate of The New School's Graduate Program of International Affairs and a self-taught computer programmer.

[1] Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

Developing a Legal Framework of Cyber Attacks Through an Effects-Based Approach

Computer-based attacks represent a subset of actions that can be described as information operations. Information operations (IO) are defined as actions taken by the military in times of peace or war to affect adversary information and information systems while defending one's own information and information systems.[2] Broadly speaking, IO refers to radar jamming, psychological, and electronic means of carrying out operations. A subset of electronic IO is called computer network operations (CNO). CNO are defined as operations to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.[3] Two sub-elements of CNO are attack and defense. Computer network attacks (CNA) are defined as actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers themselves.[4] If the information within a computer that controls the water level in a nuclear power plant suffers any disruption to the information flow, it can have devastating physical effects.[5] Each case presented in this article represents a form of CNA with its own unique effect. The effects highlighted by each case range from denial of service and theft of information to physical destruction.

Due to the relatively new nature of state-sponsored international cyber attacks, this article addresses the existing body of international treaty law that includes the prohibitions on the use of force and self-defense as found in the United Nations Charter. These will be used to measure the extent to which computer-based attacks can be considered a use of force. Additionally, the effects-based guidelines will be used as a normative framework for determining the level of force for each case in this article.

Article 2(4) of the UN Charter acts to maintain international peace and order by prohibitive means. It prescribes that "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."[6]

Despite the intentions of this statement, the vague terminology "use of force" presents challenges for maintaining the prohibitive elements of Article 2(4). This idea was

---

2 Joint Chiefs of Staff, Joint Pub. 3-13, "Information Operations" (13 February 2006), Gl-3; available at http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf.

3 Ulhas Kirpekar, "Information Operations in Pursuit of Terrorists," Master's Thesis completed at the Naval Postgraduate School, Monterey, CA (September 2007), 63; available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.185.907&rep=rep1&type=pdf. See also Joint Chiefs of Staff, Joint Pub. 3-13, "Information Operations," II-9 for Cyberspace Operations.

4 Kirpekar, "Information Operations in Pursuit of Terrorists," 63.

5 World Nuclear Association, "Fukushima Accident 2011" (2013), available at http://www.world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Fukushima-Accident-2011/#.UXgxAIJAvIU.

6 United Nations, Article 2, paragraph 4.

introduced at the 1945 San Francisco Conference, when the Brazilian delegation argued that Article 2(4) ought to include economic coercion.[7]

This amendment to Article 2(4) never occurred, and the unclarified concept of force is further expressed in the 1986 International Court of Justice ruling on *Nicaragua v. United States*. The Court considered that the supply of funds to the Nicaraguan *contras*, while an act of intervention in the internal affairs of Nicaragua, did not amount to a use of force.[8] This ruling suggests that the instruments of force ought to be evaluated on the basis of their outcomes. For example, physical coercion has a higher probability of causing destruction, injury, and escalation than diplomatic or economic coercion. Therefore, the effects of armed force are perceived as more concerning, and thus armed action prohibited by the international community. From this concern, force is divided into a spectrum of severity that ranges from armed to economic. Thus, the challenge is to place the diversity of computer attacks on this spectrum of force.

Chapter VII, Article 41 of the UN Charter further defines the spectrum of force by establishing specific acts that are considered to be non-armed uses of force. Non-armed uses of force include "complete or partial interruptions of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications."[9] Because Article 41 uses the wording "other means of communications," it includes network technology in this level of non-armed force. The conflict of this legitimization of computer-based weapons arises when network technology is manipulated to cause physically destructive events.

Chapter VII, Articles 39 and 51 of the UN Charter authorize the use of force based on specific criteria established for the preservation of peace and self-defense. Article 39 grants the UN Security Council the "authority to determine the existence of any threat to peace, breach of peace, or act of aggression."[10] Article 51 authorizes the use of force with the expression that "nothing in the present Charter shall impair the inherent right of individual and collective self-defense if an armed attack occurs against a Member of the United Nations."[11] Under this structure, there is no use of the term "use of force." Instead, "armed attack" gives a state the right to respond in self-defense.[12] As a result, the Security Council is the only entity that may mount forceful responses to events that

---

7 Doc. 215, I/1/10, 6 U.N.I.C.O Docs. 559 (1945). See Doc. 784, I/1/27, 6 UNICO Docs. 334-35 (1945). The amendment proposed by Brazil, that would have added to the prohibition on the threat or use of force the words "and from the threat or use of economic measures," was rejected by a 26–2 vote.

8 Military and Paramilitary Activities (Nicaragua v. U.S.), 1986 I.C.J. 4,119 (27 June 1986). The court did not actually apply Article 2(4); instead, the Court applied the customary international law prohibition on the resort to force to adjudicate the issue.

9 United Nations Charter, Article 41.

10 United Nations Charter, Article 39.

11 United Nations Charter, Article 51.

12 Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework," *Columbia Journal of International Law* 37:3 (1999): 893.

threaten the peace. States using the Article 51 authorization must define "armed attacks" before using any kind of force. For states responding to computer attacks, the difficulty is in determining whether a computer attack is a threat to peace, a breach of peace, an act of aggression, or something that constitutes an imminent armed attack.

The legal frameworks regarding the prohibition on the use of force and the self-defensive authorization of force are challenged by computer-based attacks because they have a wide range of effects. They vary from annoyance to physical destruction. One category of computer attack that is interpreted as a definite use of force is an attack that directly causes physical damage.[13] The difficulty is in situating computer attacks that do not cause physical damage or injury within the spectrum of force. Given that the international community already recognizes actions at various levels of force (e.g., economic coercion or materially supporting rebels in another state), computer attacks must also be considered in a similar way. Therefore the Schmitt criteria are used to describe the various thresholds of force for a given attack based on the characteristics of their effects.

The following characteristics are used to asses the extent to which non-physically destructive computer attacks amount to a use of force: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[14]

- Severity measures whether or not an attack is physically destructive or merely diplomatic coercion. This quality considers the Article 2(4) definition that takes into account the territorial integrity or political independence of a state.
- Immediacy measures how fast an attack occurs. For armed attacks, the effects are immediate, as in the example of an exploding bomb. Even though computer attacks travel at the speed of light, they may take time for their effects to be known.
- Directness is a measure of how connected the attack is to the effect of the attack. In the case of traditional armed attacks, the missile causes the destruction. In cases of economic coercion, like currency manipulation, the effects of this attack are less certain.[15]
- Invasiveness measures the degree to which attacks occur inside or outside a country. In traditional armed attacks or uses of force, attacks occur within a country's territory.
- Measurability is similar to directness, except it is a measure of how easy it is to measure the effect of an action.
- Finally, presumed legitimacy takes into account the legal norms and considerations that authorized the attack.

---

[13] Ibid., 898.

[14] Ibid., 898–99.

[15] Daniel Ikenson, *Appreciate This: Chinese Currency Rise Will Have a Negligible Effect on the Trade Deficit* (Washington, D.C.: CATO Institute, 2010), available at www.cato.org/publications/free-trade-bulletin/appreciate-chinese-currency-rise-will-have-negligible-effect-trade-deficit.

This framework is useful because it provides a thorough set of guidelines for analyzing all types of force and attacks, including computer-based forms. The six criteria are especially helpful in describing the degree with which a computer attack may be considered a non-armed use of force or an armed use of force.

As an additional concept of this framework, in cases of computer attacks that are considered to be below the threshold of force as well as armed attack, the right to respond in self-defense is based on the following three factors:

- The attack is part of an overall operation culminating in an armed attack
- The attack is an irrevocable step in an imminent and unavoidable attack
- The defender is reacting in advance of the attack during the last possible window of opportunity.[16]

This second scheme will be applied to the cases of the 2008 South Ossetia War and the actions of Unit 61398 because these cases did not cause physical destruction. Because of the destruction caused by the "Olympic Games" operation, it will be assessed using the effects-based criteria and under the restrictions of U.S. and international law for its authorization to act. Furthermore, the Iranian response to this CNA suggests that when computers cause physical destruction they may be considered as a use of force below the threshold of armed conflict.

The 2008 South Ossetia War Between Russia and Georgia

The biggest problem with computer network attacks, especially those that are part of covert operations waged by nation-states, is attribution. Even if communications can be traced back to a specific computer, it may be impossible to demonstrate a link between that computer and a state to which responsibility can be attributed.[17] For this reason, the case analysis for the 2008 South Ossetia War assumes that branches within the Russian government sponsored the computer attacks that targeted Georgian infrastructure. The difficulty in attribution creates a problem where the legality of cyber attacks can only be discussed *post facto*. This results in a condition where there can be no real-time assessment of the cyber battlespace.

For this case, the assumption that the cyber attacks originated in Russia is made for a number reasons. The first reason is that the focus of this article is on state-sponsored computer attack. While Russia has not claimed responsibility for the computer attacks, if attribution could be made, this case would be a clear example of classifying CNA as an armed conflict and a use of force. The second reason is because when a computer network attack is used to cause unrest in a target country, it is unlikely that the perpetrator will publicly acknowledge or leave traces that can credibly determine their guilt.[18] The

[16] Schmitt, "Computer Network Attack and the Use of Force in International Law," 908.

[17] Daniel Silver, "Computer Network Attack as a Use of Force under Article 2(4)," *International Law Studies* 76, special issue on "Computer Network Attack and International Law" (2002): 79.

[18] Ibid.

third reason is that when computers are used in the context of traditional military operations, states would have little motive to raise a legal dispute solely on the basis of computer-based attacks.[19] This is because a military attack is far more egregious that a computer attack. Finally, it is likely that when states conduct computer attacks they would attempt to conceal their involvement, or to make their efforts look like those of a non-state sponsored hacker.[20]

Despite the lack of attribution in this case, evidence that Russia has been developing its offensive cyber capabilities has been growing. In March 1998, U.S. officials found a connection between intrusions into computers systems belonging to the Pentagon, NASA, the U.S. Department of Energy, private universities, and research labs. All of the attacks had come from a computer network in Russia.[21] Once more, attribution in this battlespace remains uncertain, and the identity of the culprit is still unknown to the public. Another event, this one in 2007, involved a three-week-long, politically charged cyber attack against Estonian computers. The computers reported to have originated the attacks had Russian Internet addresses and were housed at state institutions.[22] The Russian government denied its involvement with these attacks as well. In light of all these events, in 1995 Russian General Vladimir Slipchenko stated that the Russian General Staff Academy had shifted its focus from force-on-force simulation to system-on-system simulations, which included cyber and other information-related systems.[23]

In August 2008, hostilities between Russia and Georgia over the breakaway territory of South Ossetia reached a point of military engagement. On 8 August, Russian tanks crossed the border into Georgia. However, on 7 August computer operations had already been conducted against the computer systems of Georgia.[24] The targets of the cyber attack were Georgian government websites and even included websites of the U.S. and British Embassies. The attacks initially came from Russian IP addresses.[25] Even though this incident was not directly attributable to Russian government agents or military forces, it resulted in a cyber blockade that perfectly correlated with the Russian military to make its offensive more successful.[26] For these reasons, this cyber attack is consid-

---

19 Ibid.

20 Ibid.

21 "Cyber War; The Warnings?" *PBS Frontline* (2003); available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/.

22 Timothy Thomas, "Nation-State Cyber Strategies: Examples From China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington, D.C.: National Defense University Press, 2009), 475–76.

23 Ibid., 476.

24 Eneken Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," report published by the Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia (November 2008), 4; available at http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

25 Jeffrey Carr, "The Rise of the Non-State Hacker," in *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2009), 15–17.

26 Richard A. Clarke and Robert K. Knake, "Why Cyber Warfare is Important," in *Cyber Warfare: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 18–21.

ered an act of armed conflict, because it was an operational element that prepared the battlespace for a Russian military invasion of Georgia.

The effects of the cyber operation had little to offer in the terms of severity. No one was killed as a direct result of the operation, and no property damage occurred. The CNA against Georgia during the South Ossetia conflict is best characterized as a digital blockade of information. To understand this in the context of international law, the UNGA 3314 on the Definition of Aggression states that a blockade of ports or coastlines is considered an act of aggression.[27] In this case, no physical goods were prevented from entering the country. The digital blockade severed the information pipeline and repopulated it with Russian propaganda, during a time when information confidentiality, integrity, and availability were major priorities.

During this computer attack, websites containing important information were defaced, and Internet communications were jammed by using a flooding technique. The result rendered inoperable the websites of the Georgian president, parliament, government, and foreign ministry.[28] The lack of access to legitimate information coming from the government of Georgia limited the vital dissemination of information flowing between government ministries and the public. An additional element of this attack was that it motivated the National Bank of Georgia to stop offering electronic services for a period of ten days.[29]

The immediacy of the cyber attacks in context of Russia's military incursion into Georgian territory further bolsters the interpretation that this attack represents a use of armed force. Even though the only severe effect of the CNA was communications disruption, it happened at a time when communication was vital to the Georgian government.[30] It also happens that the attacks only lasted for several days, beginning on 7 August 2008.[31] This short duration, which coincided exactly with the Russian incursion into South Ossetia, indicates a directness that connects the harm caused by the cyber attack with the harm inflicted by Russian military forces. On any other day the digital blockade would have been a nuisance, but the temporal proximity to actual military fighting conveys that this was a digital act of armed conflict. Another way of viewing this is to consider the attack as a part of a military operation in the same way that radar jamming or communications disruption serve to contribute to the overall effectiveness of an operation.

The measurability and invasiveness of this operation are limited to cyberspace. Because the method of the attack was to disrupt service and deface websites, the only digital "invasion" that occurred existed within the computers that hosted the following URLs: www.president.gov.ge (the Georgian president's website); www.nbg.gov.ge (the National Bank of the Republic of Georgia); and www.mfa.gov.ge (the Ministry of For-

---

[27] Definition of Aggression, United Nations General Assembly Res. 29/3314, Annex, U.N. Doc. A/RES/29/3314/Annex (14 December 1974).
[28] Thomas, "Nation-State Cyber Strategies."
[29] "Cyber War; The Warnings?"
[30] Ibid.
[31] Ibid.

eign Affairs of the Republic of Georgia).[32] The denial of service attacks are measured in the flow of information to specific websites. As a standard measurement, the average Mb/s for attacks that were defended by Kaspersky Labs prevention software in 2011 was 70 Mb/s.[33] In a report from a computer security firm that monitors Internet traffic, the attacks against these Georgian websites reached an average of 211.66 Mb/s, and peaked at 814.33 Mb/s, which averaged a length of two hours and fifteen minutes, but reached a peak attack duration of six hours.[34] The measured intensity of the attack on Georgia relative to the average intensity of a similar style attack conveys an extremely organized and calculated effort. Concluding, the measurability and invasiveness of the cyber attack against Georgia further supports the idea that the attack was made in concert with the Russian military, and thus constitutes a use of force and qualifies as an armed conflict.

The presumptive legitimacy of this attack is directly related to the threshold of force established in the United Nations Charter. The current reading of Article 41 suggests that the disruption of digital communications is internationally accepted as being a non-armed use of force. This presumptive legitimate framework suggests that, because this computer attack did not cause physical damage, it is not an act of armed force, but rather an act of non-armed force.

For the reasons stated above, the Schmitt criteria offer a better way of understanding non-armed uses of force in the context of computer attacks. The actions whereby the Russian government distanced itself from the nationalistic hacker community granted the Kremlin the benefit of having plausible deniability while gaining the additional benefit of passively supporting and enjoying the strategic rewards of the hackers' actions.[35] Even though this act is a non-armed use of force under Article 41, the immediacy, directness, invasiveness, and measurability suggest that this attack is an act of armed conflict.

To conclude, if the 2008 South Ossetia cyber attacks did in fact originate from the Russian government, they would be considered an act of armed conflict. The attacks were calculated to have an invasive aspect that directly served as an information blockade immediately before a military invasion. Because of those characteristics, the attack certainly violates the Article 2(4) prohibition on the use of force and qualifies as an act of armed conflict subject to an Article 51 response of self-defense.

Stuxnet – The Cyber Equivalent to Precision-Guided Missiles

The best kind of covert operation is the one that no one ever knows about. The U.S. National Security Act of 1947 defines covert action as an activity or activities of the United

---

[32] Ibid.

[33] Yury Namestnikov, "DDos Attack in Q2 of 2011," *Securelist* (29 August 2011); available at www.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011.

[34] Jose Nizario, "Georgia DDoS Attacks—A Quick Summary of Observations," Arbor Networks (12 August 2008); available at http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

[35] Thomas, "Nation-State Cyber Strategies."

States government designed 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.[36] This definition is in direct conflict with the prohibition on the use of force described in Article 2(4) of the UN Charter. To influence political, economic, or military conditions in another country is to violate that country's political sovereignty, and thereby constitutes an act of force. Whether or not the force is armed or non-armed is subject to debate. Thus, the highest goal of physically destructive covert operations is to remain undiscovered, or plausibly deny involvement.

As was made evident in the ICJ ruling on the *Nicaragua v. United States* case, even if covert operations are discovered, they can function at a level below the threshold of armed conflict. This suggests that, despite the lack of clarity around the terms "armed" or "attack," states agree that not all military actions equate to an armed conflict.[37] Military attacks that clearly violate a state's political sovereignty yet do not constitute armed conflict is a category that can also be said to include the Stuxnet computer attack. For that reason, it is an excellent case to use for analyzing covert computer attacks waged against nation-states, because it is the only example where attribution is absolutely certain and where the cyber attack constitutes a clear use of force.

The "Olympic Games" operation began in 2006 during the second term of the George W. Bush Administration, and lasted until November 2010, during President Obama's first term in office (even though the computer code had a self-deletion date of 24 June 2012).[38] The earliest phases of Stuxnet's development involved lawyers auditing the program code to make sure that the cyber weapon did not violate the laws of armed conflict.[39] Furthermore, the intent of the computer program was not only to hinder the nuclear ambitions of Iran; it was also designed to interfere with Iran's best scientific and military minds.[40] The Stuxnet designers made it seem like sloppy engineering or faulty mechanical hardware were at fault for causing problems. This unresolved issue caused a great deal of stress and instability among the staff working at Natanz.[41] The Stuxnet program had different forms that had affected different systems within the enrichment facility and had caused varying effects. The developers of Stuxnet were constantly changing the modalities of the attack to create new versions of the bug.[42] The end result was a physically destructive and psychologically destabilizing computer attack directed at the country of Iran.

The effects-based analytical guidelines suggest that there are two ways of categorizing this attack. The views can either support or deny the interpretation of this event as an armed attack. The severity of the physical damage caused by the attack is limited to the

---

36 SEC. 503 [50 U.S.C. §413b] (para e).
37 United Nations Charter, Article 39.
38 David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012), 202.
39 Ibid., 193.
40 Ibid., 199.
41 Ibid.
42 Ibid.

tangible destruction of uranium centrifuges located within the Natanz uranium enrichment facility. Thus, according to one interpretation, this computer attack was an act of armed force prohibited by Article 2(4).

The Stuxnet worm was found on computers throughout the Middle East, and in countries as far afield as Indonesia and the United States. Even though the systems of these countries were disrupted, no physical damage resulted. This means that the designers of the attack had made every effort to keep the destructive elements of the worm inside Iran. The designers gave the program an autonomous logic that only triggered the destructive payload upon successful identification of the right computer inside the right network.

Given that this program was active for a duration of four years suggests a level of commitment on par with armed conflicts. In deciding whether or not this use of force constitutes an armed conflict, the criterion of immediacy suggests that this event is indeed an armed attack, because it lasted from the end of the second Bush Administration and went into the beginning of the Obama Administration. Even though the immediacy factor suggests that Stuxnet was an armed conflict, the other elements of the Stuxnet program suggest otherwise.

The kinetic effects of Stuxnet attack are in no ways similar to those caused by missiles or bombs. The attack had a direct effect, which caused the uranium centrifuges in Iran's nuclear facility to malfunction. Despite the physical destruction caused by the worm, it took place in a manner that did not cause harm to humans. The centrifuges were revved up and down during certain times of the month, which damaged them in a way that made it seem as though the Iranians had purchased faulty equipment or had assembled the devices incorrectly.[43] In this way, the cyber weapon's payload employed humane means below the threshold of traditional kinetic armed attacks.

The Stuxnet operation can be measured in two ways: the spread of its accidental outbreak and the physical destruction it caused. A Symantec security report that analyzed Stuxnet listed that 67,000 of the 100,000 worldwide computers infected with the virus were geographically located within Iran.[44] This fact further supports the notion that this was a calculated and targeted use of force. Additionally, this program destroyed one thousand centrifuges at Natanz (11 percent of the total number at the time) and caused a chaotic environment, which strained the engineering staff and likely significantly slowed Iran's ability to enrich uranium from 2006 to 2010.[45]

The biggest question is whether or not this attack had been legitimately authorized, and what was the legal basis of that authorization. Because Stuxnet was such a clear use of force, the following element of the analysis focuses on the presumed legitimacy of the U.S. legal structures that authorized the action. Due to the fact that this was a covert op-

[43] Ibid., 199.

[44] Nicolas Falliere, Liam O'Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response (February 2011); available at www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[45] Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly* 63 (2011): 69.

eration, it was subject to the rules and regulations governing such actions. Title V of the National Security Act of 1947 describes the various procedures for ensuring accountability of intelligence activities. The President of the United States is the only entity able to authorize covert actions, and is only permitted to do so if the action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States.[46] Additionally, every determination of the president shall be established in a published finding that meets the following criteria: a written document must be produced within forty-eight hours of the decision to use covert action; a finding may not authorize a covert action that has already occurred; each finding specifies the department, agency, or entity of the United States authorized to participate; each finding shall specify whether any third party to the United States government is authorized to act; and, finally, a finding may not authorize any action that would violate the Constitution of the United States.[47]

In the case of Stuxnet, proposals for covert action against the uranium enrichment facility in Iran came from the U.S. Strategic Command and the National Security Agency. President Bush felt that the cyber attack was a better option for dealing with Iran's nuclear ambitions than traditional military or diplomatic engagements.[48] When Barack Obama became president, he wanted the intelligence community to take control of the operation, and in doing so reviewed and renewed the set of findings related to Stuxnet so that it would allow the United States to influence the politics, economics, or military standing of another country during peacetime.[49] Therefore, using the existing legal guidelines for covert operations, the Stuxnet attack was presumed to be legitimate and compliant with the laws of armed conflict.

The Stuxnet element of the covert operation codenamed "Olympic Games" has been considered an exemplary use of a computer network attack that falls below the threshold of armed attack. This conclusion is extraordinary, because the Stuxnet worm caused physical damage to a nuclear enrichment facility inside the territory of another sovereign country, and no response or reprisal was ever issued. In November 2010, the President of Iran made a statement that the Bushehr nuclear power plant was delayed in becoming fully operational because of technical reasons. Stuxnet and Natanz were never mentioned.[50] In order to understand the groundbreaking nature of this case, replace the computer-based attack with a precision-guided missile. The difference between the means and effects are huge. The difference between these two uses of force is that if a missile were used, it would have caused an international crisis, because missiles damage more than just uranium enrichment centrifuges. The effect of the computer attack was twofold. It hindered the uranium enrichment program at the Natanz facility in Iran, and it ushered in a new way of exercising force through cyberspace.

---

[46] SEC. 503 [50 U.S.C. §413b] (para a).
[47] SEC. 503 [50 U.S.C. §413b] (para a), 1–5
[48] SEC. 503 [50 U.S.C. §413b] (para e), 191.
[49] SEC. 503 [50 U.S.C. §413b] (para e).
[50] Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Force Quarterly* 63 (2011): 70.

Unresolved Issues – Chinese Espionage against U.S. Business

There is a method of cyber attack that is currently below the level of force prohibited by Article 2(4), and that falls well below the threshold of armed conflict. The method is known as espionage. The case used to assess the instance of digital espionage is the known existence of the Chinese People's Liberation Army's Unit 61398. The case suggests that there is no legal deterrent or prohibition in place that adequately addresses digital espionage. The laws of armed conflict do not apply to this situation, because the act of digital espionage is considered to be on the same footing as traditional espionage. In some ways, it poses the same concerns as computer crimes carried out by non-state actors.

Despite the limitations of the law of armed conflict, the effects-based criteria outlined above shed light on the scope and scale of damage caused by cyber espionage. According to a report from Mandiant, an independent computer security company, Unit 61398 has stolen information from 150 companies for a period of seven years, and has accumulated more than a hundred terabytes of data.[51] If twenty terabytes of data were printed out on paper, it would fill a line of large moving trucks fifty miles long.[52] This phenomenon has been monitored for a long stretch of time, and has been directly associated with the People's Liberation Army (PLA). This practice represents a large-scale theft of the intellectual capital of U.S. businesses and undermines their competitiveness. Thus, severity can only be judged on the type of information stolen and the effect this has on the profitability of a business.

All of the factors of the effects-based criteria suggest that this is an armed attack, except for the factor severity. By using the classification levels for national security information, Executive Order 12958 provides guidelines whereby the United States can measure the significance of stolen information:

- A Type 1 attack causes a nuisance or inconvenience to the defense or economic security of the United States.
- A Type 2 attack causes damage to the defense or economic security of the U.S.
- A Type 3 attack causes serious damage to the defense or economic security of the U.S.
- A Type 4 attack causes exceptionally grave damage to the defense or economic security of the U.S.

[51] Mandiant APT 1, "Exposing One of China's Cyber Espionage Units" (2013); available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[52] Joel Brenner, *Calm Before the Storm*, Foreign Policy (2011), *available* at www.foreignpolicy.com/articles/2011/09/06/the_calm_before_the_storm.

- A Type 5 attack causes critical damage to the defense or economic security of the U.S.[53]

Thus, the degree to which an espionage attack is determined to be an armed attack depends on the classification of the information stolen.

The dilemma goes back to the problem of *post facto* judgment. First, an attribution must be made, and then the level of force must be determined. In the case of information theft, evaluating the potential significance of terabytes of stolen data can be a long and daunting task, and in most cases the theft would not rise to the level of an armed attack. If these attacks are not prohibited by Article 2(4), and are not evaluated under the law of armed conflict, there is nothing to prevent countries from engaging in this kind of action. The precedent established in the Unit 61398 cases suggests that digital espionage is beyond legal regulation because it is neither a use of force nor an act or armed conflict.

Conclusion

In all applications of the law of armed conflict, three questions are always asked: Is this an armed conflict? What kind of conflict is this? And finally, what type of combatant is involved? This article sought to answer the first question. However, this only addresses the *jus ad bellum* of computer network operations. Furthermore, each incident of computer attack that goes without legal or political repercussions establishes a precedent under which this form of international behavior is acceptable.

There are numerous unresolved issues in this new battlespace, including the legal structure governing the *jus in bello* of computer attacks. The principles of necessity, distinction, and proportionality with regard to autonomously spreading computer programs are collectively a large area of concern. Who are the combatants of a computer attack – the computers, the software, or the programmers, and what rights are these entities afforded? One of the main ways computer code propagates itself is by using treacherous deceit, which violates laws prohibiting perfidy. Because cyberspace is made up of computers that are owned by companies based in other countries, are these companies accountable because they are materially supporting the attack? Furthermore, are cyber conflicts most appropriately considered as international conflicts or domestic conflicts? The questions remain unresolved, and as societies around the globe become more reliant on information and the technological infrastructures that supply it, the conventional understanding of war and international legal structures will need to evolve in order to address the issues and concerns raised by state-sponsored computer-based attacks.

---

[53] Mark B. Treadwell, "When Does an Act of Information Warfare Become an Act of War? Ambiguity in Perception," U.S. Army War College Strategy Research Project (1998), 16–17; available at www.dtic.mil/cgi-bin/GetTRDoc?AD=ada345572.

Bibliography

Brenner, Joel. *Calm Before the Storm*. Foreign Policy, 2011.

Brown, Gary D.. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Force Quarterly* 63 (2011): 70.

Carr, Jeffrey. "*The Rise of the Non-State Hacker*." In *Inside Cyber Warfare: Mapping the Cyber Underworld*, 15-17. Sebastopol, CA: O'Reilly Media, 2009.

Clarke, Richard A., and Robert K. Knake. "*Why Cyber Warfare is Important*." In *Cyber Warfare: The Next Threat to National Security and What to Do About It*, 18-21. New York: HarperCollins, 2010.

Falliere, Nicolas, Liam O'Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Symantec Security Response, 2011.

Ikenson, Daniel. *Appreciate This: Chinese Currency Rise Will Have a Negligible Effect on the Trade Deficit*. Washington, D.C.: CATO Institute, 2010.

Kirpekar, Ulhas. *Information Operations in Pursuit of Terrorists* In *Naval Postgraduate School*. Monterey, CA, 2007.

Milevski, Lukas. "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly* 63 (2011): 69.

Namestnikov, Yury. *DDos Attack in Q2 of 2011* In *Securelist*., 2011.

Nizario, Jose. *Georgia DDoS Attacks—A Quick Summary of Observations* In *Arbor Networks*., 2008.

Sanger, David. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers, 2012.

Schmitt, Michael N.. "Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework." *Columbia Journal of International Law* 37, no. 3 (1999): 893.

Silver, Daniel. *Computer Network Attack as a Use of Force under Article 2(4)* In *International Law Studies* ., 2002.

Thomas, Timothy. "*Nation-State Cyber Strategies: Examples From China and Russia*." In *Cyberpower and National Security*, 475-76. Washington, D.C.: National Defense University Press, 2009.

Tikk, Eneken. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn, Estonia : Cooperative Cyber Defense Center of Excellence, 2008.

Treadwell, Mark B.. *When Does an Act of Information Warfare Become an Act of War? Ambiguity in Perception* In *U.S. Army War College Strategy Research Project*., 1998.