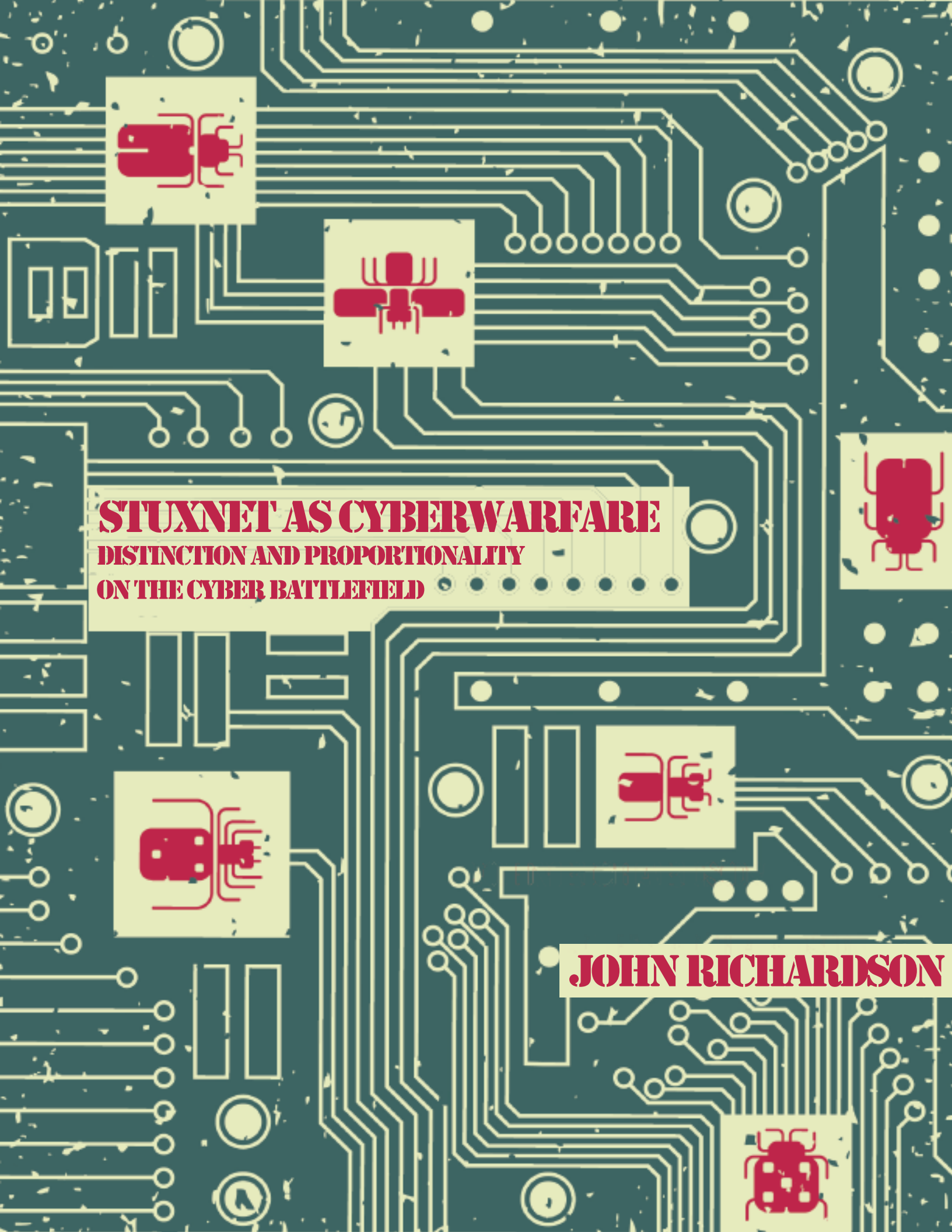

STUXNET AS CYBERWARFARE

DISTINCTION AND PROPORTIONALITY ON THE CYBER BATTLEFIELD

JOHN RICHARDSON

Stuxnet as Cyberwarfare:
Applying the Law of War to the Virtual Battlefield

by
John Richardson

About the Author

John Richardson is the President and CEO of JMR Portfolio Intelligence, Inc. a corporate governance and human rights consultant based in Washington DC. He is also the editor of Global Investment Watch, a blog dedicated to addressing human rights in the global marketplace.

Mr. Richardson received his undergraduate degree from the University of California at Santa Barbara and his Juris Doctor degree from Golden Gate University, in San Francisco and is currently working on his LLM degree in International Human Rights Law at the International Labor Studies Program at American University's Washington College of Law.

Executive Summary

In the field of international humanitarian law, there are a number of questions about the conduct of warfare in the cyber domain. In some cases, answers can be gleaned from treaties and customary international law but in other instances, solutions are seemingly intractable, begging for solutions that may only be answered by technology itself. From a legal perspective, such oversimplifications trivialize humanitarian law as well as other legal constructs already struggling to address complex issues in the cyber realm.

It is within this context that this paper focuses on a recent event known as Stuxnet, a computer virus that infected and damaged a nuclear research facility in Natanz, Iran. Reflecting on this particular cyber attack, this paper addresses two IHL issues: Does the Stuxnet attack rise to the level of an armed attack within the meaning of international humanitarian law? If so, did it adhere to the two core principles of IHL, namely *distinction* and *proportionality*? This paper finds that the Stuxnet attack does in fact rise to the level of an armed attack within the meaning of IHL and adheres to the principles of distinction and proportionality.

Table of Contents

Introduction

Conflicts in cyber space are increasing at an exponential pace. Once the playground of hackers, students and the occasional thief, the Internet is now the domain of spies, organized criminals and saboteurs. There is considerable talk in the popular media and the cyber security community about what should be done to solve these problems. Problems demand solutions and characterizing cyber problems in the war vernacular seems to suggest a simple way to solve complex problems on the Internet with a mere label. Cyber security experts prod this simplification in their books and speeches and policy makers with suspect motives sensationalize the latest online break-in or cyber espionage caper.

However, this conflation of all cyber conflicts into the language of war poses dangers for the future of the Internet and how people everywhere use it. At the very least, this sets the stage for the militarization of the Internet, a place where traditional notions of freedom become a secondary concern, displaced by inflated concerns with state security and corresponding restrictions on individual freedoms. Yet despite considerable exaggeration on the topic, there are real risks of conflict in cyberspace. If indeed there is an event that can be characterized as a cyber war, how is it distinguished from other types of conflict on the Internet, over the airwaves and through telecommunication systems?

In the field of international humanitarian law, there are a number of questions about the conduct of warfare in the cyber domain. In some cases, answers can be gleaned from treaties and customary international law but in other instances, solutions are seemingly intractable, begging for solutions that may only be answered by technology itself. From a legal perspective, such oversimplifications trivialize humanitarian law as well as other legal constructs already struggling to address complex issues in the cyber realm. "[T]he real difficulty with respect to the law and cyberwar is not any lack of

"law," per se, but rather in the complexities that arise in determining the necessary facts which must be applied to the law to render legal judgments.[1]

It is within this context that this paper focuses on a recent event known as Stuxnet, a computer virus that infected and damaged a nuclear research facility in Natanz, Iran. Reflecting on this particular cyber attack, did it rise to the level of an armed attack within the meaning of international humanitarian law? If so, did it adhere to the two core principles of IHL, namely *distinction* and *proportionality*? From this analysis, it is hoped that a better understanding of what is a cyber war will emerge.

[1] Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly (Spring 2011), at 81.

A Nuclear Problem and a Cyber Solution

In 2010, several independent technology researchers discovered a new virus that had invaded computer systems around the world. While viruses in many forms have been around since the early days of the Internet, this virus[2] caught the attention of experts because it displayed unique functions and a level of sophistication never seen before. Dubbed "Stuxnet," this worm demonstrated a number of interesting qualities, including a specific attack vector that was limited to certain computers operating in a rather unique fashion. While the worm rapidly distributed itself around the globe, infecting tens of thousands of computers, its purpose remained a mystery. While early reports suggested that this worm was intended to disrupt satellite telecommunications and other computer controlled infrastructure systems, no direct link between the virus' functions and those specific systems was established. However, after several months it became apparent that the virus had a specific geographic target: Iran. A disproportionate number of infected computer systems were located in that country. While the virus appeared around the world, no discernible damage was reported to have occurred elsewhere.

Eventually, as the computer code contained in the virus was deciphered, it became evident that it was designed as a weapon, targeting a

[2] Throughout this paper the terms virus, worm and malware are used interchangeably. *See* TechTerms.com (2011) http://www.techterms.com/definition/worm (A computer worm is a type of virus that replicates itself, but does not alter any files on your machine). Microsoft Support.com, *Computer viruses: description, prevention and recover*y (Apr. 26, 2011) http://support.microsoft.com/kb/129972 (A computer virus is a small software program that spreads from one computer to another computer and that interferes with computer operation). TechFaq.com, *Computer Worm* (2011) http://www.tech-faq.com/computer-worm.html. (Computer worms are programs that reproduce, execute independently and travel across the network connections. The key difference between a virus and worm is the manner in which it reproduces and spreads. A virus is dependent upon the host file or boot sector, and the transfer of files between computers to spread, whereas a computer worm can execute completely independently and spread on its own accord through network connections). SearchMidMarketSecurity.com, *Malware (Malicious Software),* (2011) http://searchmidmarketsecurity.techtarget.com/definition/malware (Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission).

specific nuclear "research" facility in the state of Iran. The virus – Stuxnet - was a weapon that disrupted the operation of gas centrifuges used to make highly enriched uranium, an essential component in the creation of nuclear weapons. Within months, the virus was succeeded in damaging or destroying more than 900 centrifuges, setting back Iran's uranium enrichment program by several years.

It remains unclear who launched this attack, though the list of suspects is short. What is clear is that this virus was extraordinarily precise in attacking a specific target while inflicting virtually no damage on any other computer systems. There were no reported casualties and the damage inflicted was limited to the objectives of the attack. While researchers are uncertain whether the virus has any additional functions, so far, its impact has been precise with no collateral consequence.

As more is learned about the virus, security experts and the popular media have seen it as a seminal event in the growing sophistication of cyber conflict. Stuxnet is the (not so) secret weapon of cyber warfare and America (probably) created it.

Iranian Ambitions and Western Fears

Putting the Stuxnet attack in perspective, it is worth noting the background to this cyber attack by looking at Iran and its nuclear ambitions over the last 50 years. The Islamic republic of Iran started its nuclear program in the 1960s during the reign of the Shah. Though ended after the 1979 revolution, it was suspected that Iran restarted its program in the mid-1990s.[3] This was confirmed when "in 2002, an exile group obtained documents revealing a clandestine program"[4] for the development of nuclear capabilities, which continue to this day. While American and European

[3] *Iran's Nuclear Program*, The New York Times (Jan. 18, 2011), http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html.
[4] *See Id.*

officials believe Tehran is planning to build nuclear weapons, Iran's leadership says that its goal in developing a nuclear program is to generate electricity without dipping into the oil supply it prefers to sell abroad, and to provide fuel for medical reactors.[5]

In September 2007, the government in Tehran announced that it had installed 3,000 centrifuges, the machines that enrich uranium. Uranium enrichment can produce fuel for nuclear reactors, but can also produce fissile material for use in nuclear weapons.[6] In addition to its nuclear reactor facility located near the town of Bushehr, the Iranian government has constructed both a pilot and a commercial gas centrifuge-based uranium enrichment facility near the city of Natanz.[7] As of 2011, the number of gas centrifuges at the Natanz facility has grown to more than 9000 machines.

Both the U.S. and Israeli governments have expressed continued skepticism about Iran's peaceful motives. In 2008, President George W. Bush deflected a secret request by Israel for specialized bunker-busting bombs it wanted for an attack on Iran's main nuclear complex and told the Israelis that he had authorized new covert action intended to sabotage Iran's suspected effort to develop nuclear weapons, this according to senior American and foreign officials.[8] Recalling similar incursions like the one in 1981 where Israel launched the first ever attack on a nuclear facility at the Osirak nuclear facility outside of Baghdad, Iraq,[9] and *Operation Orchard*, a 2007 Israeli airstrike on a Syrian nuclear facility then under construction,[10] the U.S. was likely unwilling to support the Israelis' overt military actions in this volatile region. This set the stage for a more subtle approach to the

---

[5] *See Id.*
[6] Paul K. Kerr, John Rollins & Catherine A. Theohary, Cong. Research Serv., R 41524, The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability, (December 9, 2010), at 4.
[7] *Iran's Nuclear Program*, *supra* note 3.
[8] *Iran's Nuclear Program*, *supra* note 3.
[9] *1981: Israel bombs Baghdad nuclear reactor*, BBC News (June 7, 1981), http://news.bbc.co.uk/onthisday/hi/dates/stories/june/7/newsid_3014000/3014623.stm.
[10] Erich Follath & Holger Stark, *How Israel Destroyed Syria's Al Kibar Nuclear Reactor*, Spiegel Online International (Nov. 9, 2009). http://www.spiegel.de/international/world/0,1518,658663,00.html.

problem in Iran in 2008 – one in which deniability of an attack combined with a less overt solution to the problem could be achieved.

A Virus Attacks

Stuxnet was originally detected in early 2010 by a computer security company in Belarus, and subsequently found to have infected (albeit without causing much actual harm) thousands of industrial control systems world-wide.[11]

What has been discovered is that the Stuxnet virus is malware that attacks widely used industrial control systems built by the German firm, Siemens AG. The company says the malware was initially distributed via an infected USB thumb drive memory device or devices, exploiting vulnerabilities in the Microsoft Windows operating system. Such systems are used to monitor automated plants - from food and chemical facilities to power generators. Analysts said attackers may have chosen to spread the malicious software via a thumb drive because many SCADA (Supervisory Control and Data Acquisition) systems are not connected to the Internet, but do have USB ports. Once the worm infects a system, it quickly sets up communications with a remote server computer that can be used to steal proprietary corporate data or take control of the SCADA system, said Randy Abrams, a researcher with ESET, a privately held security firm that has studied Stuxnet.[12]

As of September 25, 2010, Iran had identified "the IP addresses of 30,000 industrial computer systems" that had been infected by Stuxnet, according to Mahmoud Liaii, director of the Information Technology Council of Iran's Industries and Mines Ministry, who argued that the virus "is

---

[11] Duncan Holis, *Could Deploying Stuxnet be a War Crime?* Opinio Juris (Jan 25, 2011), http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/.
[12] *Factbox: What is Stuxnet?* Reuters (Sept. 24, 2010), http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUSTRE68N3PT20100924.

designed to transfer data about production lines from our industrial plants" to locations outside of Iran.[13] Some parts of Iran's operations ground to a halt, while others survived, according to the reports of international nuclear inspectors. In 2011, it still is not clear the attacks are over: Some experts who have examined the code believe it contains the seeds for yet more versions and assaults.[14]

According to Symantec Corporation, a maker of computer security software and services based in Silicon Valley, the worm hit primarily inside Iran but also in time appeared in India, Indonesia and other countries. However unlike most malware, it seemed to be doing little if any harm elsewhere. It did not slow computer networks or wreak havoc.[15] The Symantec study showed that the mainly affected countries as of August of 2010 were Iran, with 62,867 infected computers, Indonesia with 13,336, India 6,552, United States 2,913, Australia 2,436, Britain 1,038, Malaysia 1,013 and Pakistan with 993.[16]

According to Symantec, Stuxnet targets specific frequency-converter drives — power supplies used to control the speed of a device, such as a motor. The malware intercepts commands sent to the drives from the Siemens SCADA software, and replaces them with malicious commands to control the speed of a device, varying it wildly, but intermittently. The malware, however, doesn't sabotage just any frequency converter. It inventories a plant's network and only springs to life if the plant has at least 33 frequency converter drives made by Fararo Paya in Teheran, Iran, or by the Finland-based Vacon. Even more specifically, Stuxnet targets only frequency drives from these two companies that are running at high speeds — between 807 Hz and 1210 Hz. Such high speeds are used only for select applications. Symantec is careful not to say definitively that Stuxnet was

---

[13] Kerr, et al., *supra* note 6, at 3 (translated from *Iran Confirms Cyber Attack, Says Engineers 'Rooting Out' Problem,* Mehr News Agency, (September 25, 2010)).
[14] William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, The New York Times (January 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.
[15] *See Id.*
[16] *See Id.*

targeting a nuclear facility, but notes that "frequency converter drives that output over 600 Hz are regulated for export in the United States by the Nuclear Regulatory Commission as they can be used for uranium enrichment."[17]

Researchers who have spent months reverse-engineering the Stuxnet code say its level of sophistication suggests that a well-resourced nation-state is behind the attack. It was initially speculated that Stuxnet could cause a real-world explosion at a plant, but Symantec's latest report makes it appear that the code was designed for subtle sabotage. Additionally, the worm's pinpoint targeting indicates the malware writers had a specific facility or facilities in mind for their attack, and have extensive knowledge of the system they were targeting.[18]

Stuxnet is very specific about what it does once it finds its target facility. If the number of drives from the Iranian firm exceeds the number from the Finnish firm, Stuxnet unleashes one sequence of events. If the Finnish drives outnumber the Iranian ones, a different sequence is initiated. Once Stuxnet determines it has infected the targeted system or systems, it begins intercepting commands to the frequency drives, altering their operation. "Stuxnet changes the output frequency for short periods of time to 1410Hz and then to 2Hz and then to 1064Hz," writes Symantec's Eric Chien on the company's blog. "Modification of the output frequency essentially sabotages the automation system from operating properly. Other parameter changes may also cause unexpected effects."

Curiously, when international inspectors visited Natanz in late 2009, they found that the Iranians had taken out of service a total of exactly 984 machines that had been running the previous summer. "Code analysis makes it clear that Stuxnet is not about sending a message or proving a concept," wrote Ralph Langner, a well-respected expert on industrial systems security.

---

[17] Kim Zetter, *Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage*, Threat Level (Nov. 15, 2010) http://www.wired.com/threatlevel/2010/11/stuxnet-clues/.
[18] *See Id.*

"It is about destroying its targets with utmost determination in military style."[19]

Cyber Rhetoric vs. Reality

Within this context, some cyber security cyber security and public policy experts have declared that cyber warfare is imminent and the U.S. and other nations must respond – a call to action reminiscent of the cold war era.[20] However, it remains unclear what a cyber war is within the definition of international law. This is due in part to the fact that there is considerable disagreement about whether a cyber war has in fact occurred anywhere in the world. "If [a cyber attack] is truly "war," then a response under a national-security regime is possible; if not, then treating the matter as a law enforcement issue is appropriate. This is a distinction with a difference."[21]

This problem is compounded by challenges facing legal scholars and technology experts who are struggling with questions in the context of *jus ad bellum* and in particular, questions about attributing attacks to state actors.

While there is some indication that certain technologically advanced states have developed tools for determining attribution, these practical solutions are cloaked in secrecy because of national security concerns. Setting aside this challenge, many experts in the field agree that we will know a cyber war when we see it and there are some suggestions from the field of experts that indeed, such an event has occurred.

With the discovery of the Stuxnet worm, it has been suggested that the first cyber shot has in fact been fired. As noted by Gen. Michael Hayden (Ret.) former Director of both the CIA and the NSA, Stuxnet "actual[ly] created physical effects through cyber means. I think that's crossing the

---

[19] Broad, et al., *supra* note 14.
[20] David Ignatius, *Pentagon's cybersecurity plans have a Cold War chill*, Washington Post (August 26, 20010) at A13.
[21] Dunlap, *supra* note 1, at 84.

Rubicon" as a cyber warfare event.[22] On the other hand, is this simply yet another dire prophecy from one of the digerati doomsayers?[23] As the details of the code created by the Stuxnet designers are revealed, it is becoming clear that weapons of cyber warfare can be both incredibly destructive on the level of existing kinetic weapon systems and effectively precise. But is it war?

Cyber Attacks and the Law of War

The U.S. national security community views the Stuxnet attack on the Iranian nuclear facility at Natanz as a seminal event in cyber warfare. However, others view Stuxnet and its ilk as *weapons of mass annoyance*.[24] This debate embodies several basic questions about cyber conflicts, not the least of which is the threshold question of whether an attack is in fact a war. But once this question is answered, then questions concerning the legality of a cyber attack in the context of the laws of war need to be addressed. Thus, while the virus penetration into the nuclear facility's computer network might suggest that an attack rising to the level of armed conflict occurred, a more careful analysis is needed to determine if the Stuxnet attack falls within the scope of IHL. If this initial question is answered in the affirmative, a second series of questions must be addressed with regard to whether the

---

[22] Georgetown University, International *Engagement in Cyberspace part 1*, YouTube (Apr. 14, 2011) http://www.youtube.com/watch?v=R1lFNgTui00&feature=player_embedded#at=4815

[23] Noah Shachtman, *Terrorists on the Net? Who Cares?* Wired, (Dec. 20, 2002) http://www.wired.com/techbiz/it/news/2002/12/56935.

[24] Shachtman, *supra* note 23.

Stuxnet attack adheres to the IHL principles of *distinction* and *proportionality*.

Stuxnet: A Cyber Weapon or Something Else?

Does the Natanz event rise to the level of armed conflict? "Dispassionately assessing the consequences of a cyber incident to determine their similarity to an armed attack can be difficult, as initial impressions of the effects can be wildly inflated."[25] While this paper does not intend to explore this *jus ad bellum* question in depth, it is important to touch on the question as a preliminary matter.

There are several approaches to this question, each of which suggests that under certain circumstances, cyber attacks rise to the level of an armed attack. Additional Protocol I, Article 49 defines an attack as "acts of violence against the adversary, whether in offence or in defence."[26] ""Attacks" is a term of prescriptive shorthand intended to address specific consequences . . . To the extent that the term "violence" is explicative, it must be considered in the sense of violent consequences rather than violent acts."[27] Significant human suffering or mental anguish is included in the concept of injury, as does loss of assets (investments, savings and the like) constitute damage or destruction. However, mere inconvenience or discomfort is insufficient.[28] IHL principles apply when a cyber attack can be ascribed to a State and is more than "merely sporadic and isolated incidents and are either intended to cause injury, death, damage or destruction (and analogous effects), or such consequences are foreseeable. This is so even though classic armed force is

[25] Dunlap, *supra* note 1, at 86.
[26] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Art. 49(1), 8 June 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].
[27] Michael N. Schmitt, *Wired warfare: Computer network attack and jus in bello*, 84:846 IRRC 365, 377 (June 2002).
[28] *See Id.*

not being employed."[29] This issue of a one-off event not rising to the level of an attack within the meaning of IHL is an important one in the context of cyber warfare given that once a target state has identified that it is under a cyber attack, the attack itself can be halted by means akin to a flip of the switch. "In *Nicaragua v. U.S.*, the ICJ seemed to indicate that an armed attack within the meaning of Article 51 did not arise in every case of an armed clash. Rather, the ICJ considered the "scale and effects" of the use of force to determine if it met the Article 51 requirement."[30]

On the other hand, the Department of Defense takes a broader view, characterizing a cyber attack as one that can "disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[31]

Some legal scholars are of the view that the criteria put forth by Jean Pictet to determine the existence of armed conflict under Common Article 2 is a useful guide. Using this test, use of force is considered "armed conflict" when it is of sufficient scope, duration and intensity."[32] However, this approach falls short in determining whether a cyber attack falls within the scope of IHL because it inadequately addresses whether cyber attacks constitute armed attacks since such events are often undetected until after the damage is done, the attack itself may take only a fraction of a second to complete its task and its direct impacts may be unclear.

Given the sometimes-conflicting views concerning this threshold question, it is worth noting several "approaches" that have been developed that help to understand whether a cyber attack rises to the level of an armed

---

[29] *See Id.,* at 374.
[30] Dunlap *supra* note 1, at 86 citing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 181, 195.
[31] *Computer Network Attack*, HPCR Manual on International Law Applicable to Air and Missile Warfare (May 15, 2009), http://www.ihlresearch.org/amw/manual/section-a-definitions/m.
[32] David E. Graham, *Cyber Threats and the Law of War*, 4 J. of National Security L. & Policy, 87, 90 (2010).

attack.[33] Three models have been developed to apply Pictet's *Use of Force Continuum*[34] for assessing, among other events, cyber attacks.

Using an *instrument based approach*,[35] one must ask whether a cyber attack could have only previously been accomplished by kinetic means, such as dropping a bomb on a power plant or an air traffic control system. Again, this approach does not account for attacks that damage or destroy data while leaving hardware intact.

A second model is the *strict liability approach*, which asserts that an attack on critical infrastructure would be an armed attack based upon the severe consequences from such an attack on the national infrastructure of a state.[36] However, this approach does not account for less significant events causing damage on a smaller scale such as the disruption of a municipal water or sewage facility or of a commercial operation that suffers significant financial loss to itself or its customers as a result of the cyber attack.

A third model is the *effects based approach*,[37] also known as the "consequence based approach." Here the question is not whether the damage done could have been achieved through traditional means but what the overall effect the attack has on the state subject to the attack. Using this approach, one could argue that a cyber attack launched against a country's stock exchange that resulted in the disruption of the country's critical infrastructure[38] dramatically affected the well being of the state and thus viewed as an armed attack. This analysis seems to best address the

---

[33] *See Id*., at 91.
[34] *See Id*.
[35] Graham, *supra* note 32, (quoting Yoram Dinstein, "War, Aggression and Self Defence" 181).
[36] *See Id*.
[37] Graham, *supra* note 32, at 89, (quoting Thomas Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, 41-44 (2000)).
[38] Critical Infrastructures Protection Act of 2001, 42 U.S.C. §5195c(e) (2001), ([T]he term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters).

complexities of cyber based attacks by assessing the outcomes rather than the weapons used in an attack.

With respect to the events at the Natanz nuclear facility, analyzing the Stuxnet event from either an *effects based approach* or from a *strict liability approach* would suggest that an armed attack did in fact occur. Both in the Stuxnet code itself, which was tested by investigators after the Natanz attack and in the inferences drawn from statements made by Iranian officials, reveals that the effect of the malicious program was to manipulate the operation of the gas centrifuges in a manner that did eventually destroy a significant part of their uranium enrichment equipment.

An Expanded View of Cyberwarfare

While Stuxnet did not damage online banking or commerce, the question of whether a cyber attack against economic targets rises to the level of an armed attack is nonetheless a significant issue in cyber warfare. In the U.S. as well as elsewhere in the developed world, financial institutions, commerce and the capital markets are all connected via the Internet. Damage to these institutions and means of commercial exchange, while not destroying physical infrastructure can have a far greater impact on a state's economy and its social infrastructure.

As a preliminary matter, customary international law approaches this question related to cyber attacks narrowly. "Economic targets . . . are legitimate military objectives as long as they effectively support military operations, and if attacking them provides a definite military advantage."[39] The ICRC states that "[i]n literature it is sometimes claimed that the use of CNA[40] expands the range of legitimate targets because it enables attacks with reversible effects against otherwise prohibited objects. If this claim implies

[39] Jean-Marie Henckaerts & Louise Doswald-Beck, Customary Humanitarian Law Vol. 1, at 32 (2009 ed. 2005).
[40] CNA refers to *computer network attacks*. This term is used interchangeably with the term *cyber attacks* throughout this paper. *See, e.g.* Knut Dormann, *Applicability of the Additional Protocols to Computer Network Attacks*, Cambridge Review of International Affairs, (May 19, 2001), at 1.

that an attack against a civilian object may be considered lawful if the attack does not result in destruction or if its effects are reversible, this claim is unfounded under existing law." As massive cyber attacks aimed at Internet-based banking systems, financial trading systems and broad based e-commerce that render them inoperable for some period of time while not destroying them outright, their effects on states can be far more profound than kinetic attacks on specific military targets or civilian objects.

Professor Michael Schmitt has devised a useful six-part test for determining whether a cyber attack, targeting for instance economic or commercial objects, rises to the level of an armed attack within the meaning of IHL. A computer network attack, which on its face appears to be more economic or political in form than an act of armed force can be distinguished using the following six criteria:

> Severity: Armed attacks pose the threat of injury, death, damage or destruction to a much greater degree than economic or political coercion.
>
> Immediacy: The negative consequences of an armed attack are more immediate, while economic or political coercion are less so.
>
> Directness: The consequence of an armed attack is more closely linked to the attack than in is the case with economic or political coercion.
>
> Invasiveness: In an armed attack, the harmful event "usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders" with the former results in a greater intrusion on the rights of the targeted state and greater international instability.
>
> Measurability: While the consequences of an armed attack are more easily measured that are economic or political ones.
>
> Presumptive Legitimacy: The application of violence is generally

deemed illegitimate whereas economic or political force is deemed presumptively lawful.[41]

Given the unique nature of cyber attacks, as distinguished from kinetic or conventional weapons-based attacks, damage or destruction in the traditional sense is often minimal. However, the more significant harm rendered by a cyber attack takes the form of significant disruption but not permanent destruction to computer controlled systems, including online banking, electrical grids, telephone systems and the like.

> "At the very least, the LOAC does not draw entirely clear-cut distinctions. Accordingly, it is not surprising that inconsistencies might emerge if cyber attack is the means used for economic coercion, without immediate loss of life or property. Thus, one must determine the appropriate analogy that should guide national thinking about cyber attacks that result in severe economic dislocation. In particular, are such cyber attacks like economic sanctions, or like a blockade, or even like some form of kinetic attack, such as the mining of a harbor?"[42]

Several recent events shed some light on this question.

In 2007, the Estonian government faced a severe cyber attack from forces with Russia. The attack came on the heal of a decision by the Estonian government to remove a statue of Lenin from a square in Vilnius, the capital of Estonia. As noted in an article by Jeffrey Kelsey,

> [h]itting the websites of banks, ministries, newspapers, and broadcasters, the assault left Estonia without the means to tell the world it was under attack. The strike was both indiscriminate and surprisingly focused: " 'Particular "ports" of

---

[41] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Columbia J. of Transnational Law 885, 902 (June 1999).
[42] Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. Nat'l. Sec. L. & Pol'y, 63, 80.

> particular mission-critical computers in, for example, the telephone exchanges were targeted. Packet "bombs" of hundreds of megabytes in size would be sent first to one address, then another.' " This attack was more than just an inconvenience to the Estonian population: the emergency number, used to call for ambulances and the fire service, was unavailable for more than an hour. No state or terrorist group claimed responsibility after the attack, but analysts believed the complexity of the attack required the cooperation of a state and/or several large telecom firms. Given the history of the Baltic State, some naturally suspected Russian involvement.[43]

Again in 2008, a cyber attack, ascribed to the Russian state preceded the Russian invasion of Georgia:

> On August 7, 2008, following separatist provocations, Georgian forces launched a surprise attack against the separatist forces. On August 8, Russia responded to Georgia's act by military operations into Georgian territory, which the Georgian authorities viewed as Russia's military aggression against Georgia. By late August 7, before the Russian invasion into Georgia commenced, cyber attacks were already being launched against a large number of Georgian governmental websites, making it among the first cases in which an international political and military conflict was accompanied - or even preceded - by a coordinated cyber offensive.[44]

Applying Schmitt's six-part test to the facts, the challenge in determining the application of IHL to these two events is apparent. The

---

[43] Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 Michigan Law Review 1427, 1429 (2008) (quoting *Newly Nasty*, The Economist, (May 26, 2007) http://www.economist.com/node/9228757).

[44] Eneken Tikk, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm & Liis Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified, at 4 (November 2008).

attacks themselves were certainly disruptive in their effects.no obvious kinetic effects were apparent. However, in the case of the Estonia attack, there were nine deaths directly attributed to the cyber intrusion. This was not because of some external pressure, a blockade or sanctions but a disruption that occurred from actions within the borders of these two states. With respect to the Georgia invasion, the cyber attack was integral to the land based attack by the Russians. Telecommunications were disrupted, greatly diminishing the ability of the Georgian government to communicate during the heat of war. Moreover, neither cyber attack could be characterized as legitimate actions undertaken by another state and their consequences were as profound as if traditional means were used to inflict the damage experienced from the cyber attacks.

Whether a computer network attack falls within the meaning of IHL will be determined by the facts in the specific instance. Cyber attacks that result in kinetic damage or injury or death to persons certainly falls within the definition. However, this is less evident if a cyber attack that doesn't cause injury to people or damage to objects falls within the scope of IHL. Given the rapid evolution of computer networks, the Internet as well as technology as a whole and the corresponding sophistication of cyber attackers, cyber attacks on net-centric societies, commercial and government infrastructure are much more menacing and pose greater risk of significant economic harm and social disruption to states today than even three or four years ago. Traditional approaches to defining what constitutes an attack need to be expanded to account for destruction to virtual infrastructure and harm to individuals not causing outright physical injury but harmful to people's lives in just as significant ways.

Distinction on the Cyber Battlefield

What is a valid target in a cyber conflict? Like targets in the real world, in the cyber realm legitimate targets can include combatants and military objectives. In cyber conflicts, launching indiscriminate computer attacks is the norm. Whether it's a denial of service attack on the computer servers of a

commercial enterprise, distribution of a logic bomb[45] on the Internet in a particular country or by myriad other means, the common characteristic is a wide-reaching attack that makes little distinction between friend or foe. What this means when viewing the events surrounding the Stuxnet attack on the Natanz facility and the means taken for completing that attack raises a range of questions related to the IHL principles of ***distinction*** and ***proportionality***.

When a common Article 2 international armed conflict arises, there are four principles that must be applied when engaged in armed conflict. In addition to the principles of *distinction* and *proportionality, military necessity* and *prevention of unnecessary suffering* must be taken into account. Each of these principles is interrelated with the others, creating a framework for evaluating compliance with IHL. With respect to the principles of *distinction* and *proportionality*, it is important to differentiate the two principles. "Discrimination requires combatants to differentiate between enemy combatants, who represent a threat, and noncombatants, who do not. In conventional operations, this restriction means that combatants cannot intend to harm noncombatants, though proportionality permits them to act, knowing some noncombatants may be harmed."[46]

The principle of *distinction* requires that parties to a conflict must "execute [their] military operations in a manner which enables a *distinction* to be made between unlawful and lawful targets."[47] "Attacks may only be directed against combatants. . . [and] attacks must not be directed toward civilians."[48] Similarly, "[t]he parties to. . . [a] conflict must at all times distinguish between civilian objects and military objectives. Attacks may only be directed against military objectives."[49] Thus, the question is whether the

---

[45] Tech-Faq.com, *Logic Bomb* (2011), http://www.tech-faq.com/logic-bomb.html, (A logic bomb is a program, or portion of a program, which lies dormant until a specific piece of program logic is activated. In this way, a logic bomb is very analogous to a real-world land mine).
[46] U.S. Army/Marine Corps Counterinsurgency Field Manual, 7-34, (2006).
[47] Esbjorn Rosenblad, International Humanitarian Law of Armed Conflict, at 63 (1979).
[48] Henckaerts & Doswald-Beck, *supra* note 40, at 3.
[49] *See Id*.

Stuxnet attack fell within the limitations of the *distinction* principle when it was unleashed.

Article 48 of Additional Protocol I speaks directly to the principle of *distinction*: "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."[50] In a similar fashion, Additional Protocol II applicable to non-international armed conflicts, Article 13(1) touches on the subject by stating that "[t]he civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations.

Given the principles set forth in Article 48, the question arises as to what constitutes an appropriate target and/or an objective within the IHL framework. Article 51 of Additional Protocol I addresses this question, noting that "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack."[51] Paragraph 4 of Article 51 expands on this concept, asserting "[i]ndiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol."[52]

In regard to a military objective, Article 52(2) of Protocol 1 states that "[a]ttacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military

[50] Additional Protocol I, *supra* note 26, Art. 48.
[51] Additional Protocol I, *supra* note 26, Art. 51(2).
[52] *See Id.,* Art. 51(4).

action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[53]

In the cyber context, the ICRC takes a rather broad view of what constitutes a target stating, "[i]n literature it is sometimes claimed that the use of CNA expands the range of legitimate targets because it enables attacks with reversible effects against otherwise prohibited objects. If this claim implies that an attack against a civilian object may be considered lawful if the attack does not result in destruction or if its effects are reversible, this claim is unfounded under existing law."[54] The ICRC then argues that "[t]he fact that CNA does not lead to the destruction of the object attacked is irrelevant. In accordance with Art. 52 (2) of AP I only those objects, which make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked. By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way."[55]

Targeting in the Cyber Realm

With increasing frequency, cyber attacks of many varieties occur around the world. One need only think about the events in the first four months of 2011 to get a flavor of the range of cyber intrusions launched against friends and enemies alike: the denial of service attack (DDoS) against Wikileaks,[56] the network intrusions into the NASDAQ network[57] and the shutdown of the Internet in Egypt[58] are but a few of the examples of a rather

---

[53] *See Id.,* Art. 51.
[54] Dormann, *supra* note 40, at 5.
[55] *See Id*., at 6.
[56] Christina Warren, *Wikileaks Hit by Another DDoS Attack*, Mashable (Nov. 30, 2010), http://mashable.com/2010/11/30/wikileaks-ddos-2/.
[57] *Hackers Attack Nasdaq Network, Probe On: Reports* (Feb. 5, 2011), http://www.nasdaq.com/aspx/company-news-story.aspx?storyid=201102051134RTTRADERUSEQUITY_0095.
[58] Christopher Williams, *How Egypt shut down the Internet*, The Telegraph (May 1, 2011), http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.

exhaustive list. This list is exhaustive. From a targeting perspective, whether any of these objects can be considered a military objective is the question at hand.

Additional Protocol I requires that: only military objectives and not civilians or civilian objects can be attacked;[59] indiscriminate attacks are prohibited;[60] and that the previous two rules be respected and in particular, minimizing incidental civilian harm.[61] [62] In the Stuxnet context, several issues arise, including the question as to whether the virus properly distinguished between possible civilian objects and military targets located in the nuclear facility. A second set of questions focuses on whether the attack was waged in a manner that minimized collateral damage to civilian objects when it destroyed equipment that was arguably used for non-military purposes. As a preliminary matter, understanding whether the creators of Stuxnet could legally attack the Natanz facility requires an understanding of whether the facility was a legitimate military target within the meaning of IHL.

Civilian objects must not be the object of an attack.[63] Attacks are limited to military objectives. "In so far as objects are concerned, military objectives 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."[64] Similarly "[m]embers of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities."[65] In contrast, "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of

[59] Additional Protocol I, *supra* note 26, Arts. 48, 51(2) & 52.
[60] *See Id.,* Art. 51(4)(5).
[61] *See Id.,* Art. 57.
[62] Dormann, *supra* note 40, at 4.
[63] Additional Protocol I, *supra* note 26, 52(1).
[64] *See Id.,* Art. 52(2).
[65] *See Id.,* Art. 43.

violence the primary purpose of which is to spread terror among the civilian population are prohibited."

In addition to distinguishing between civilian objects and military objectives, a related question about who can be targeted arises, albeit far less frequently in the current context. In the cyber realm, the question of who is a direct participant in hostilities is, as a practical matter of little concern. Combatants, civilian or military, privileged or not, are so far removed from the consequences of their actions that targeting them in the context of active hostilities is highly improbable. However, as with many things in this area, circumstances can change quickly.

Targeting Cyber Combatants

Targeting combatants in the cyber realm raises several interesting issues that do not commonly arise in traditional conflicts. Because cyber attacks are very asymmetrical in nature – that is, only one side is usually engaged in a cyber attack while the other side is often sorting out what is happening and reacts often after the attack is completed – the likelihood that a cyber combatant will be targeted is remote. However, combatants, including civilians directly participating in hostilities are legitimate targets.

A combatant who can be legitimately targeted is defined in in Article 43(2) of Protocol 1 as "[m]embers of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) . . ."[66] In contrast, Article 51(2) of Additional Protocol I states that "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."[67] Further, Article 51(3) provides that "Civilians shall enjoy the

[66] *See Id.*, Art. 43(2).
[67] *See Id.,* Art. 51(2).

protection afforded by this section, unless and for such time as they take a direct part in hostilities."[68]

Uniformed military personnel engaging in cyber combat activities – remote drone operators, computer operators launching virus or denial of service attacks, programmers performing penetrations into an opponent's network – are legitimate targets within this definition. Also, civilians employed by the military are legitimate targets of attack and are not protected by Article 51(3). The challenge in targeting these personnel is more of a practical problem as they can be conducting their combatant role far from the site of an attack and, as a practical matter, will in most instances avoid retaliatory consequences. Civilians will more likely be illegally targeted, as noted below, when subject to widespread cyber attacks on infrastructure or suffer the knock-on effects from an attack on a military or civilian object.

Dual-Use Objects

In the context of computer network attacks, it is nearly impossible to avoid attacks on dual use objects and this was certainly the case with the Stuxnet attack. "A dual-use object is one that serves both civilian and military purposes."[69] "[A]n object that has the potential for military usage, but is currently used solely for civilian purposes, is a military objective if the likelihood of military use is reasonable and not remote in the context of the particular conflict under way."[70] One need only think of the NATO bombing of the Belgrade, Serbia television station during the Kosovo conflict, where 16 civilian employees were killed when the NATO planes attacked the military communication system to understand the dual-use problem.

"If an object is being used for military purposes, it is a military objective vulnerable to attack, including a computer network attack. This is

---

[68] *See Id.,* Art. 51(3)
[69] Schmitt, *Wired Warfare*, *supra* note 27, at 384.
[70] *See Id*., at 385.

true even if the military purposes are secondary to the civilian ones."[71] Thus, as noted by Professor Michael Schmitt, even if a civilian object is used exclusively for civilian purposes and its military use is reasonable and not a remote possibility, then it can be legitimately targeted.

In the context of Article 52 of Additional Protocol I, "[t]he criterion of purpose is concerned with the intended future use of an object, while that of use is concerned with its present function. Most civilian objects can become useful objects to the armed forces. Thus, for example, a school or a hotel is a civilian object, but if they are used to accommodate troops or headquarters staff, they become military objectives. It is clear from paragraph 3 that in case of doubt, such places must be presumed to serve civilian purposes."[72]

Thus, as applied to the operations at the Natanz facility, it was the Iranian government's position that the facility was being used for peaceful purposes. The uranium hexafluoride gas can be enriched at the Natanz at a sufficient concentration to yield fuel for atomic power stations or, if refined to a very high degree, for nuclear warheads.[73] While the operation of the plant remains a point of contention with the U.S., Israel and other western states, it remains clear that the facility can be used for military purposes if it is not already being used as such.[74]

---

[71] *See Id*., at 384.
[72] ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, at 636 (1987).
[73] *IAEA envoys visit Iran's Natanz enrichment site: report*, Reuters (Jan. 16, 2011), http://www.reuters.com/article/2011/01/16/us-iran-nuclear-natanz-idUSTRE70F12F20110116.
[74] Sharon Squassoni, Cong. Research Serv., RS21592, Iran's Nuclear Program: Recent Developments, at 5 (September 6, 2006), (Iran has pursued three different methods of enriching uranium and has experimented with separating plutonium, suggesting a steady accrual of expertise in weapons-relevant areas, according to some observers. If Iran received the same nuclear weapon design that A.Q. Khan gave Libya, the remaining technical hurdle (albeit the most difficult) would be fissile material production. On January 18, 2007, then-DNI Negroponte told Members of Congress that, "Our assessment is that Tehran is determined to develop nuclear weapons. It is continuing to pursue uranium enrichment and has shown more interest in protracting negotiations than reaching an acceptable diplomatic solution.).

Potential Risk of Dangerous Forces Released

Another aspect of the Stuxnet attack and its effects is the issue related to the unleashing of dangerous forces – nuclear radiation, destructive flooding and the like – that would render harm to the environment or to people.

"Dams and power plants, sometimes also dykes are highly dependent on computer control. Manipulation of these systems by way of CNA may cause the release of dangerous forces and cause severe damage to the civilian population."[75] Article 56 of Additional Protocol 1 provides that "[w]orks or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."[76] "This prohibition is independent of the type of weapons or methods of warfare used. It would therefore also cover attacks effected by means of CNA, for example manipulation of the computer system of a dam which leads to opening the floodgates, if this may cause severe losses among the civilian population."[77] Thus, where a nuclear facility is a military objective, it could be subject to a cyber attack if it does so without releasing dangerous forces as prohibited by Additional Protocol I.[78]

While much of the debate in national security circles centers on future scenarios, including cyber attacks on infrastructure connected to the Internet, there have been no significant attacks causing such kinetic effects that have resulted in the release of nuclear radiation or consequent harm from the release of destructive natural forces from the destruction of dams or dykes. In relation to Stuxnet and Natanz, it is important to note that such kinetic attacks from a cyber attack would be prohibited under the provisions

---

[75] Dormann, *supra* note 40, at 7.
[76] Additional Protocol I, *supra* note 26, Art. 56.
[77] Dormann, *supra* note 40, at 7.
[78] Shulman, Mark R., *Discrimination in the Laws of Information Warfare*, 37 Columbia Journal of Transnational Law 939, 962 (1999).

of Additional Protocol I if there were such profound damage to the Iranian nuclear facility that caused the release of nuclear radiation into the atmosphere. However, there is no evidence to suggest that Stuxnet unleashed such destructive radiological materials as it destroyed the targeted machines at the Iranian nuclear facility. While the Tehran regime would likely deny such a catastrophic event even if it had occurred, given that such a revelation would expose its plans and its failings, one must take it at face value that no adverse events occurred.

This brings us to the Stuxnet attack and the manner in which it targeted the Natanz nuclear facility.

Stuxnet: Distinction Perfected?

While most computer viruses today are indiscriminate by their very nature, infecting and rendering some sort of harm to any and all computers they invade, the Stuxnet virus is a major exception to that norm. Findings from security experts suggest that the Stuxnet code attacked and destroyed only specific gas centrifuges used to highly enrich uranium, operating at a specific speed that is unique to the machines operating at the Natanz facility.[79] If the virus found its way onto any other computer or computer-controlled system, it was harmless. While the virus was widely distributed and infected tens of thousands of computer control systems, it appears to have damaged only its intended military target.

In determining whether the Stuxnet attackers adhered to the IHL principle of *distinction*, the core question that must be addressed is whether the Natanz facility was and is a legitimate military objective.

Since no party to the attack, neither Iran nor the attackers – conjectured to be Israel and the U.S. – is talking about their intentions with respect to this cyber attack, one can only speculate about their motives.

[79] Shulman, *supra,* at 4.

However as noted earlier, a debate has been waged about Iran's nuclear intentions.[80] Iran's leaders have argued that its nuclear intentions are peaceful. The U.S., the U.K., Israel and the United Nations have all argued at different points that Iran is building the capability to build nuclear weapons. The fear is that Iran will use such weapons against Israel. At the center of this debate is the Natanz facility. Because it is the primary manufacturing facility for much of its nuclear programs, both civilian and if one is to believe the U.S. and its allies, military as well. As recently as April of 2011, western observers have noted with alarm that "Iran . . . is now thought to possess enough low-enriched fuel to make at least two bombs if the material were processed further. The country has consistently maintained that it does not intend to make nuclear weapons."[81]

If one were to take at face value (according to the Iranian government) that the Natanz facility is operating as a nuclear research facility enriching uranium for commercial purposes, the attack would, at first glance, violate international law. However, this dual use of a facility, even if it were used primarily for civilian purposes, could nonetheless be considered a military objective and attacked in accordance with IHL. If as is argued by the U.S., Israel, the IAEA and a host of other countries, the facility also produces highly enriched uranium for the development of nuclear weapons, then the legitimacy of the Stuxnet attack becomes clearer. Targeting the facility would be analogous to attacking a weapons plant. The limited damage inside of the facility did not unleash any destructive effects envisioned by Article 56.

Since there is no evidence that the Stuxnet virus was in any way targeting or in fact did any harm to combatants or civilian personnel, the attack does not violate the principle of distinction. Even if, as the Iranian authorities assert, that the attack was on a civilian operation, the dual-purpose of the Natanz facility makes it a legitimate target.

---

[80] *See Id*., at 7-8.

[81] Joby Warrick, *Iran touts major advances in nuclear program*, The Washington Post (April 11, 2011), http://www.washingtonpost.com/world/iran-touts-major-advances-in-nuclear-program/2011/04/11/AFZ8cxMD_story.html.

The Virus and its Collateral Effects

As the Stuxnet virus performed its tasks, it replicated itself and distributed its payload from computer to computer by way of the Internet and thumb drive memory devices, infecting tens of thousands of unintended computers.

This raises another concern that the collateral effects on civilian objects – computer-controlled infrastructure systems and networked commercial operations –were excessive relative to the malware's military objectives - this is the principle of *proportionality*. In the cyber realm, this principle has additional importance given the unique ways in which destructive forces can be unleashed on both civilians and civilian objects on a massive scale and in ways not deemed destructive in the traditional IHL sense. Nonetheless, such forces can have an equally profound effect on the civilian population during a conflict. As is typical of many viruses and other kinds of malware, when the Stuxnet attack was launched, it quickly distributed itself across tens of thousands of computer control systems without regard for whether the systems were the intended target of the attack. This characteristic speaks to both the effectiveness of this and many other viruses as well as their indiscriminate nature and the disproportionate collateral damage they can inflict on any node on a computer network or the Internet.

Article 57(2)(b) of Additional Protocol I provides that "an attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack 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."[82] Article 51(5)(b) further notes that "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or

[82] Additional Protocol I, *supra* note 26, Art. 57(b)

a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated,"[83] and paragraph (2)(a)(iii) of Article 57 further provides that combatants should "refrain from deciding to launch any 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."[84]

In the cyber realm, direct injury, death, damage or destruction from an attack is rare – at least as of 2011 - whether aimed at civilian or military objectives. Direct harm to people from a virus infecting a computer - as distinguished from a denial of service attack - has not been documented. In terms of damage to military or civilian objects, the most common example would be the destruction or corruption (damage) of stored data in computers or computer networks. Though cyber attacks may be viewed as far less destructive to human life and the environment, there are huge potential threats posed from activities in the cyber realm. The secondary effects of a cyber attack can be profound and, depending on whether the attack extends beyond its intended target in a significant way, it can violate the principle of *proportionality* and therefore one should not trivialize its impact in a time of war.

What then would a cyber attack violating the principle of *proportionality* look like?

An often-cited example would be a network attack that disabled a state's telephone and electrical systems. While the hypothetical attacker might argue that the attack was necessary to deny communications and computer network capability to the opponent's military operations during the conflict, had the collateral effect resulted in the disabling of a considerable portion of the civilian telephone system and the interruption of power for the civilian population, it could likely be seen as disproportional to

[83] *See Id.*, Art. 51(5)(b).
[84] *See Id.*, Art. 57(2)(a)(iii)

its intended, legal purposes. A balancing test weighing the military necessity of an attack against its collateral effects on civilians or civilian objects is crucial.

In the context of the Stuxnet scenario, how could such an attack "be aimed accurately at the intended target and, even if one is capable of doing this, not at the same time create a magnitude of unforeseen and unforeseeable effects upon civilian infrastructure? . . . Even if introduced only into the military network of a State, if the virus is virulent enough, it would soon seep out of that network and into civilian systems of the targeted State or even beyond to neutral or friendly States."[85] In fact, this is exactly what happened with the Stuxnet virus.

With Stuxnet, had the software code contained in the virus itself functioned to disable any computer control system it encountered, in addition to the destruction it inflicted on the Natanz systems, its effects on civilian objects would have been profound given the tens of thousands of computer control systems actually infected. But Stuxnet did not function in that fashion.

While it infected many systems, its harmful effects were not unleashed and in fact, the virus self-destructed when it found that the system it encountered did not fit the target profile.[86] Though the immediate incidental effects of the Stuxnet virus were inconsequential, were there any secondary effects caused by the virus? All of the evidence so far suggests that there were none.

---

[85] Dormann, *supra* note 40, at 5.

[86] Gregg Keizer, *Stuxnet code hints at possible Israeli origin, researchers say*, Computerworld (September 30, 2010) http://www.computerworld.com/s/article/9188982/Stuxnet_code_hints_at_possible_Israeli_origin_researchers_say.

Second Tier Consequences

Second tier or "knock-on" effects can create significant consequences in cyber conflicts. "Knock-on effects have a bearing on proportionality analysis because they must be considered when balancing collateral damage and incidental injury against military advantage. Unfortunately, when caused by computer network attack such damages and injuries, whether direct or indirect, are difficult to assess without knowing how the computer systems involved function and to which other systems they are linked."[87] For instance, disabling an oil refinery can have an immediate effect on the spot price of oil in the global markets. This was seen in the Niger Delta when a Nigerian rebel group known as "MEND announced itself in early 2006 in a series of attacks on oil multinationals operating in the area [and conducted] . . . with a sophisticated media campaign that involved e-mailing press releases to coincide with attacks . . . While an attack in Nigeria may not shut in that much [oil output], the headlines are enough to push jittery markets up," says Sebastian Spio-Garbrah, an analyst with the Eurasia Group in New York. Threats to Nigeria's output are not new, but they've never before coincided with such high prices."[88]

Drawing on the earlier example where a cyber attack disrupts the telecommunications network in a community and renders the emergency 911 networks inoperative, the unintended but potential deadly consequences seem apparent. Individuals seeking access to emergency medical care who subsequently die from lack of rapid treatment would fall within the scope of second tier effects.[89]

The issue becomes more complicated when a computer virus becomes widely distributed to many tens or hundreds of thousands of computer systems that are not the intended target of an attack. The principle of

---

[87] Schmitt, *supra* note 27, at 393.
[88] Will Connors, *The Nigerian rebel Who Taxes Your Gasoline*, Time (May 28, 2008) http://www.time.com/time/world/article/0,8599,1809979,00.html
[89] *See* note 44.

proportionality would possibly be violated if the virus in question caused a kinetic effect to occur, such as shutting down an entire telecommunications system or a power grid supplying power to both the military and the civilian population. Employing a balancing test that looks at the collateral effects of an otherwise legitimate attack could result in a determination that a computer network attack is unlawful.

Applying this rationale to a computer network attack, if a virus were to delete the contents of any computer it found itself on – whether used for civilian or military purposes - and the result was widespread destruction of data in the civilian population, the principle of proportionality would be violated. The knock on effect of such damage could include the destruction of urban traffic signal systems or the disruption of air traffic control systems, for example. The consequence of either of these scenarios could be profound. Thus, in determining whether the principle has been violated, it is critical to consider whether the unintended effects of the cyber attack have been minimized.

In the final analysis, the Stuxnet virus was unique in that it infected many thousands of computers but caused no harm to any system but to the intended military target. An analogous example would be the deployment of ground troops into the opponent's territory. Passing through civilian centers, billeting in towns and occupied rural areas during a military occupation does not constitute a violation of Article 51 if in the course of the occupation, protected civilians and civilian objects were not targeted. In a similar vein, viruses, transmitted from one computer to the next without any corresponding destructive effect would not be a violation of IHL. Thus, in the case of the Stuxnet virus, its destructive effect was localized to the specific computer controlled centrifuges at the Natanz facility and thereby avoided the pitfalls of a disproportionate attack on all systems it encountered.

Conclusion

The Stuxnet attack has drawn considerable public attention, melding several often-discussed topics in the public eye, including the state of Iran, global conflict and the Internet. While the Stuxnet narrative is a compelling one, opinions about cyber war drawn from the events surrounding Stuxnet do not adequately address the legal issues raised with respect to this conflict. While characterizing Stuxnet as an act of war plays well with the national security mindset, a more reasoned view urges perhaps a different conclusion. That said, it appears that the events surrounding the computer network attack on the Natanz facility constitute an attack within the meaning of IHL. The necessary damage and destruction is present as evidenced by the physical damage to the nuclear enrichment operations at Natanz. Moreover, the attack was precise, targeting only dual-use objects that could be used for military purposes if it is not being used for that purpose already. Though distributed over a wide range of computer systems in many countries, the Stuxnet virus did not inflict any appreciable collateral effects rendering harm to civilians or non-military objects. For these reasons, the attack was unique in that it adhered to the principles of distinction and proportionality, targeting its military objective with precision and with virtually no collateral damage.

Whether Stuxnet is a model or perhaps portent for future cyber wars is debatable. What is certain however is that with the exponential growth in sophistication of computer and network technology, unique cyber weapons and novel methods of attack will be the norm in the cyber realm. Whether international law can limit if not prevent harm to innocent people and restrain combatants in cyber space from damaging an important "place" for billions of people in the 21st century is a critical challenge. Adapting humanitarian law to address the rapidly changing cyber landscape and its future battlefields is the key.