Fordham International Law Journal

Volume 35, *Issue* 3 2012 *Article* 1

Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?

Jeremy Richmond[*]

[*]Fordahm University School of Law

NOTE

EVOLVING BATTLEFIELDS: DOES STUXNET DEMONSTRATE A NEED FOR MODIFICATIONS TO THE LAW OF ARMED CONFLICT?

Jeremy Richmond[*]

[*] J.D. Candidate, 2012, Fordham University School of Law; B.A. in Anthropology, 2006, Skidmore College. The Author would like to thank his family for their love and support and Mary Claire Dekar for her love, encouragement, and unfailing patience. Much of this Note was inspired by conversations with Professor Eric Talbot Jensen, who the Author would like to thank for his enthusiasm, expertise, and friendship.

"If you think Stuxnet is revolutionary then you slept through the revolution."[1]

INTRODUCTION

In 2010, a tech-security firm in the Republic of Belarus first detected the piece of computer malware now known as "Stuxnet."[2] Computer experts first knew Stuxnet as a hack of the Windows operating system, itself a substantial feat.[3] Subsequent analysis of Stuxnet's code, however, revealed something of far greater significance: Western governments, most probably Israel and the United States, had likely designed the computer worm to target an Iranian nuclear weapons facility.[4] Specifically, the worm appears to have been constructed to destroy uranium enrichment centrifuges at Iran's Natanz nuclear facility, in an

[1] Christopher Williams, *Stuxnet: Cyber Attack on Iran 'Was Carried Out by Western Powers and Israel,'* TELEGRAPH (London), Jan. 21, 2011, http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html (quoting cyber-security expert Tom Parker).

[2] *See* Jonathan Fildes, *Stuxnet Worm 'Targeted High-Value Iranian Assets,'* BBC NEWS, Sept. 23, 2010, http://www.bbc.co.uk/news/technology-11388018 (stating that Stuxnet was discovered in Belarus in June 2010); Michael J. Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011, at 152, 155 (describing how Sergey Ulasen, the head of the Belarusian tech-security firm VirusBlokAda, first received a report of an Iranian computer that was infected with Stuxnet). The name Stuxnet derives from the file names ".stub" and "MrxNet.sys" contained in Stuxnet's code. Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED, (July 11, 2011, 7:00 AM), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1; *A Worm in the Centrifuge: The Stuxnet Outbreak*, ECONOMIST, Oct. 2, 2010, at 63, 63–64 (stating that Stuxnet's name is derived from words found in its code). Malware is defined as "software that is intended to damage or disable computers and computer systems." OXFORD AMERICAN DICTIONARY 1060 (3d ed. 2010).

[3] *See* John Borland, *A Four-Day Dive into Stuxnet's Heart*, WIRED (Dec. 27, 2010, 8:27 PM), http://www.wired.com/threatlevel/2010/12/a-four-day-dive-into-stuxnets-heart (describing Microsoft's sophisticated response to Stuxnet's impressive infiltration of the Windows operating system); Liam O. Murchu, *Stuxnet Using Three Additional Zero-Day Vulnerabilities*, SYMANTEC: OFFICIAL BLOG (Sept. 14, 2010), http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities (reporting that Symantec, a tech-security firm, had discovered that Stuxnet exploited four vulnerabilities in the Windows operating system).

[4] *See generally* William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1 (arguing that Israel aided the United States in developing Stuxnet specifically to strike the Natanz nuclear facility); Gross, *supra* note 2, at 196 (describing how various computer scientists concluded that Western governments created Stuxnet to hinder the Iranian nuclear program).

attempt to impede Iran's nuclear weapons program.[5] Although Iranian officials initially denied that nuclear sites suffered any damage from Stuxnet, Iranian President Mahmoud Ahmadinejad later confirmed that Stuxnet had infected a "limited number of [] centrifuges" at Iranian nuclear facilities.[6] There is, however, strong evidence that significantly greater damage was done to Iran's nuclear program than President Ahmadinejad suggested.[7]

Stuxnet seems to have had two predominant purposes. First, it includes code that, when executed, dramatically raised and lowered the centrifuges' rotational speed, causing the centrifuges to destroy themselves.[8] Second, the worm sent signals to plant operators indicating that the centrifuges were working normally, so that the operators were not alerted to the problem and were unable to prevent the centrifuges from self-destructing.[9]

[5] *See* Broad et al., *supra* note 4 (opining on how Israel and the United States tested Stuxnet on centrifuges identical to those used at the Natanz nuclear facility); Zetter, *supra* note 2 (noting that Stuxnet's code targeted devices configured in groups of 164, and that centrifuges in Natanz were arranged in groups of 164).

[6] Janine Zacharia, *In Arab States' Fears, Israel Sees Impetus for Action Against Iran,* WASH. POST, Nov. 30, 2010, at A15; *see Iran Denies Stuxnet Disrupted Its Nuclear Programme,* BBC NEWS (Nov. 24, 2010, 11:17 AM), http://www.bbc.co.uk/news/technology-11821011 (noting that Iranian officials stated they had caught Stuxnet before it did any damage to the Iranian nuclear program).

[7] *See* Broad et al., *supra* note 4 (noting that the Iranians took 984 centrifuges at Natanz out of service after Stuxnet infiltrated Natanz's network); Zetter, *supra* note 2 (stating that International Atomic Energy Agency surveillance footage showed over 1000 centrifuges being replaced at Natanz after Stuxnet).

[8] *See* DAVID ALBRIGHT ET AL., INST. FOR SCI. & INT'L SEC., DID STUXNET TAKE OUT 1,000 CENTRIFUGES AT THE NATANZ ENRICHMENT PLANT? 4 (2010), *available at* http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf (noting that Stuxnet destroyed centrifuges by raising the centrifuge rotation frequency as high as 1410 hertz); Broad et al., *supra* note 4 (explaining that Stuxnet sent centrifuges at Natanz "spinning wildly out of control").

[9] *See* Broad et al., *supra* note 4 (stating that Stuxnet recorded normal operations at Natanz and then played the recording back to plant operators, as robbers might during a bank heist); Ralph Langer, *How to Hijack a Controller: Why Stuxnet Isn't Just About Siemens' PLCs,* CONTROL GLOBAL (Jan. 13, 2011), http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html?page=full (describing the signals sent to controllers and comparing them to a Hollywood movie where prerecorded video is sent to security guards).

The origins of the worm are unknown.[10] The United States has refused to confirm or deny any involvement in Stuxnet's development or deployment.[11] There is, however, strong evidence supporting the theory that Israel and the United States created Stuxnet specifically to target and damage Iran's nuclear program, which, if true, represents one of the first excursions of governments into the murky waters of cyber war.[12]

The occurrence of an event like Stuxnet is no surprise in light of the explosion of internet and computer technology in recent decades.[13] Today, computers connected to the Internet are responsible for controlling most national infrastructure and, therefore, are essential to states' everyday commercial functioning.[14] As states increasingly depend upon information structures to enable commercial and government functions,

[10] *See* Gross, *supra* note 2, at 196 (speculating that Jordan may have been involved in Stuxnet's development); Bruce Schneier, *The Story Behind the Virus*, FORBES.COM (Oct. 7, 2010, 6:00 AM), http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html (noting that the theory that Western governments developed Stuxnet is speculative).

[11] *See* Christopher Williams, *Stuxnet Virus: US Refuses to Deny Involvement*, TELEGRAPH (London) (May 27, 2011, 3:23 PM), http://www.telegraph.co.uk/technology/news/8541587/Stuxnet-virus-US-refuses-to-deny-involvement.html (reporting that US Deputy Defense Secretary William Lynn refused to answer a question from a reporter for CNBC's "CodeWars" television program asking if the Department of Defense was involved in the development of Stuxnet); Kim Zetter, *Senior Defense Official Caught Hedging on US Involvement in Stuxnet*, WIRED (May 26, 2011, 2:33 PM), http://www.wired.com/threatlevel/2011/05/defense-department-stuxnet (characterizing US Deputy Defense Secretary Lynn's response as "hedging").

[12] *See Cyberwar: The Meaning of Stuxnet*, ECONOMIST, Oct. 2, 2010, at 14 (stating that after years of speculation, Stuxnet is one of the first real-life incidents to demonstrate cyber war's potential); *infra* Part II (describing the legal construct for cyber war).

[13] *See* Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303, 305 (2010) (stating that whether governments are prepared or not, cyber weapons are becoming commonplace). Targeting government infrastructure with malware is not a novel idea; the film *Live Free or Die Hard*, produced years before Stuxnet's deployment, featured hackers attempting to destroy government infrastructure. *See* LIVE FREE OR DIE HARD (20th Century Fox 2007).

[14] *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKLEY J. INT'L L. 192, 200 (2009) (remarking that information technology is "ubiquitous" and essential to "the US's entire infrastructure"); Swanson, *supra* note 13, at 306 (describing the Internet as "a powerful tool for government functions, information, and mobilization, as well as commerce and social networking").

these structures "tend to become [militarily desirable] targets."[15] The low cost, anonymity, and the ability to target installations without necessarily causing civilian casualties make cyber-operations an appealing method of warfare.[16] As the Internet becomes a primary vehicle for societal function, it could also be used as a means to harm society.[17]

This reality has not gone unnoticed by most governments. Over 120 countries have developed information operations systems.[18] Security experts have gone as far as designating cyber threats as the greatest danger to US national security outside of weapons of mass destruction.[19] Indeed, the Russian government considers cyber threats so serious that they have retained the right to use nuclear weapons in response to a cyber attack.[20]

[15] Swanson, *supra* note 13, at 305.

[16] *See id.* at 304 (noting that cyber weapons are attractive to governments because of their low cost and wide availability); Shackelford, *supra* note 14, at 200 (discussing the problem with attributing cyber attacks to specific parties); *see also* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 897 (1999) (stating that cyber weapons are how parties can conduct "war on the cheap").

[17] *See* Swanson, *supra* note 13, at 306 (noting that the Internet can "serve as a tool for conducting operations that lead to confusion, destruction, and even death"); *see also* Glenn Derene, *How Vulnerable Is U.S. Infrastructure to a Major Cyber Attack?*, POPULAR MECHANICS (Oct. 1, 2009, 12:00 AM), http://www.popularmechanics.com/technology/military/4307521 (highlighting the "growing concern" over a cyber attack on civilian infrastructure).

[18] *See* U.S. GEN. ACCOUNTING OFFICE, GAO/AIMD-96-84, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 27 (1996) ("[The US] Department of Energy and [the US National Security Agency] estimate that more than 120 countries have established computer attack capabilities."); *see also Government-Sponsored Cyberattacks on the Rise, McAfee Says*, NETWORK WORLD, (Nov. 29, 2007, 3:41 PM), http://www.networkworld.com/news/2007/112907-government-cyberattacks.html ("120 countries including the United States are said to be launching Web espionage operations.").

[19] *See* Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 123 (2009) (noting that cyber weapons are the biggest threat to the United States "other than a weapon of mass destruction or a bomb on one of our major cities"); Fred Hetner, *Cyber Attacks Ranked 3rd Danger Behind Nuclear War*, EXAMINER.COM, Dec. 6, 2009, http://www.examiner.com/ny-in-new-york/cyber-attacks-ranked-3rd-danger-behind-nuclear-war ("Some experts have said that cyber attacks pose the greatest threat to the United States after nuclear war and weapons of mass destruction . . . .").

[20] *See* Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 166 n.124 (2005) (quoting V.I. Tsymbal, a Russian military officer, as stating: "Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself"); Danny Bradbury, *The Fog of Cyberwar*,

The seriousness with which governments consider cyber attacks highlights the emerging reality of computer network attacks ("CNA") as a weapon of war and underscores the need for a legal framework that can adequately regulate the use of these new weapons. A consensus appears to exist that current law of armed conflict ("LOAC") regulations are applicable to the use of cyber weapons, despite the absence of any LOAC provision explicitly stating so.[21] There is an ongoing debate, however, as to whether current LOAC paradigms can adequately regulate these types of attacks.[22]

In an effort to address this question, this Note analyzes the facts surrounding one of the few publicly known cyber attacks, Stuxnet, but assumes a hypothetical situation in which the LOAC applies. This Note thus addresses whether the deployment of Stuxnet conforms to the LOAC. Part I presents the facts of Stuxnet's development and deployment. Part II briefly discusses the history of the LOAC and then describes LOAC principles relevant to Stuxnet. Part III then applies the current LOAC to Stuxnet, identifying possible violations. This Note concludes that, with the possible exception of certain "knock-on" effects, current LOAC rules adequately address

GUARDIAN (U.K.), Feb. 4, 2009, http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access (reporting V.I. Tsymbal as stating that Russia may use nuclear weapons against sources of cyber war).

[21] Knut Dörmann, *Computer Network Attack and International Humanitarian Law*, INT'L COMM. OF THE RED CROSS, ¶ 29 (May 19, 2001), http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/5p2alj (stating that the law of armed conflict ("LOAC") applies to cyber weapons just as it would to any other new technology); *see* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INT'L REV. RED CROSS 365, 369 (2002) (stating that cyber weapons are covered under the LOAC and that there is "no lawless void" during an armed conflict).

[22] *Compare* Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1148–49 (2003) (arguing that the application of traditional analysis, including distinction, proportionality, and the balance between military necessity and humanity, sufficiently regulates computer network attacks ("CNAs"), and that new agreements are not needed), *with* Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N. ADMIN. L. JUDICIARY 602, 667 (2011) ("[D]elay in the formation of international treaties, limiting the use of and defining the status of cyber warfare under international law, risks devastating global repercussions.").

Stuxnet and that Stuxnet therefore demonstrates the LOAC's capability of regulating cyber war.[23]

I. *STUXNET*

In order to understand the application of the LOAC to Stuxnet, this Part offers an overview of the Stuxnet worm and the consequences of its deployment at the Natanz enrichment facility in Iran. First, Section A provides a general explanation of computer worms and a comparison to other types of malware. Next, Section B describes how Stuxnet worked. Section C then turns to the theories behind the development of Stuxnet and Section D recounts the damage that Stuxnet caused at the Natanz facility. Section E describes Stuxnet's proliferation and its effects worldwide. Finally, Section F draws conclusions about the Stuxnet worm and sets forth a set of hypothetical facts that the rest of this Note assumes.

A. *Computer Worms Generally*

Simply put, a computer worm is a piece of computer code that replicates without a human user's commands by copying itself onto another computer in a network.[24] Malware such as worms can therefore contain nothing other than an instruction to self-replicate.[25] While this may seem harmless, a worm that has located a vulnerability in a network or computer's security system can "clog" both the computer itself and the servers on the network with useless self-replications, thereby causing

[23] *See* Jensen, *supra* note 22, at 1149 (implying that knock-on effects are consequences from an attack that a commander did not intend or plan to occur); Schmitt, *supra* note 21, at 392 (describing knock-on effects as "second-tier" effects not "directly and immediately caused by the attack, but nevertheless the product thereof").

[24] *See* PETER SZOR, THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE 314 (2005) ("[W]orms usually do not need to infect files but propagate as standalone programs."); *What Is a Computer Worm?*, ANTIVIRUS WORLD, http://antivirusworld.com/articles/computer-worm.php (last visited Feb. 10, 2012) ("A computer worm is a self-replicating computer program . . . [that is] self-contained and does not need to be part of another program to propagate itself."). This differs from a computer "virus," which is a piece of code that "attaches itself" to an existing program on the computer and modifies that program in a harmful way. *See What Is a Computer Worm?*, *supra* (noting a virus attaches to, and becomes a part of, an executable file).

[25] *See* SZOR, *supra* note 24, at 296 ("[T]he majority of computer viruses do nothing but replicate."); *What Is a Computer Worm?*, *supra* note 24 (noting that a self-replicating worm can do significant damage).

significant damage.[26] Program designers therefore attempt to prevent the introduction of worms into their systems by upgrading their programs, while malware designers search for new weaknesses in the program's defense.[27]

B. *Stuxnet's Code and Its Effects*

Like most worms, Stuxnet's code causes it to spread to a new computer on the network whenever it detects one, regardless of the type of programs the new computer is running.[28] Stuxnet, however, differs from many worms in that, in addition to containing code for self-replication, it also contains a "payload" designed to give specific commands to other programs.[29] A payload is code that typically accomplishes the "purpose" of the malware.[30] After Stuxnet infects a computer, it attempts to find out whether Siemens' WinCC/PCS7 Supervisory Control and Data Acquisition software ("Siemens' SCADA software") is present on the computer.[31] Siemens'

[26] *See* SZOR, *supra* note 24, at 297 (explaining the danger of excessive self-replication); *What Is a Computer Worm?*, *supra* note 24 (describing the Mydoom worm, which caused a worldwide internet slowdown through its unchecked self-replication).

[27] *See, e.g.*, *Microsoft Issues Biggest Patch on Record*, REUTERS, Oct. 13, 2009, http://www.reuters.com/article/2009/10/13/us-microsoft-security-idUSTRE59C5EJ20091013 (stating that Microsoft updated its operating system to fix vulnerabilities); Matthew J. Schwartz, *Microsoft, Adobe Patch Vulnerabilities*, INFORMATIONWEEK (Sept. 14, 2011, 12:10 PM), http://www.informationweek.com/news/security/app-security/231601407 (noting that Adobe updated its software to fix "critical security issues").

[28] *See* ALEKSANDRA MATROSOV ET AL., ESET, STUXNET UNDER THE MICROSCOPE 10, *available at* http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf ("Once self-replicating code is released, it's difficult to exercise complete control over where it goes, what it does, and how far it spreads . . . ."); Gross, *supra* note 2, at 158 (explaining how Stuxnet moves through a computer network).

[29] *See* NICOLAS FALLIERE ET AL., SYMANTEC SEC. RESPONSE, W32.STUXNET DOSSIER 2 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf ("[Stuxnet] modifies code on the Siemens PLCs to potentially sabotage the system."); MATROSOV ET. AL, *supra* note 28, at 10 (noting that Stuxnet's "payload" is targeted at Siemens' WinCC/PCS7 Supervisory Control and Data Acquisition software ("Siemens' SCADA software")).

[30] *See Payload Definition*, PC MAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=payload&i=48909,00.asp#fbid=56CJhRA5C9H (last visited Nov. 8, 2011) ("In the analysis of worms . . . it refers to the software's harmful results.").

[31] *See* FALLIERE ET AL., *supra* note 29, at 33 ("When [Siemens' SCADA software] is found inside a project folder, the project may be infected."); *see also* Gross, *supra* note 2, at 158 (stating that Stuxnet specifically searches for Siemens' software).

SCADA software is a system that coordinates certain types of industrial hardware, overseeing and controlling basic components of an industrial system.[32] If Siemens' SCADA software is not present, Stuxnet "deactivates" and becomes an inert piece of code.[33]

If Stuxnet detects Siemens' SCADA software, it then looks to see if the software is being used to control a programmable logic controller ("PLC").[34] PLCs are small computers that typically control simple industrial tasks such as regulating motors and opening and closing valves.[35] Once Stuxnet detects the PLC, it searches to see if a certain type of machinery is attached to the PLC.[36] If Stuxnet finds the correct machinery, it checks to see if that component is operating under a specified set of conditions—most notably a specific speed at which the

[32] *See* Broad et al., *supra* note 4 (describing Supervisory Control and Data Acquisition systems as running "whole symphonies of industrial instruments, sensors and machines"); Kim Zetter, *SCADA System's Hard-Coded Password Circulated Online for Years*, WIRED (July 19, 2010, 5:29 PM), http://www.wired.com/threatlevel/2010/07/siemens-scada/ ("SCADA, short for 'supervisory control and data acquisition,' systems are programs installed in utilities and manufacturing facilities to manage their operations.").

[33] *See* FALLIERE ET AL., *supra* note 29, at 3 (describing how Stuxnet only deploys its payload on a computer with Siemens' SCADA software installed); Gross, *supra* note 2, at 158 (stating that Stuxnet "becomes a useless, inert feature on the network" if Siemens' SCADA software is not detected).

[34] *See* FALLIERE ET AL., *supra* note 29, at 36 (noting that Stuxnet attempts to monitor programmable logic controllers ("PLCs")); Gross, *supra* note 2, at 158 ("When Stuxnet moves into a computer, it attempts to spread to every machine on that computer's network and to find out whether any [PLCs] are running Siemens software.").

[35] *See* Paul Marks, *Why the Stuxnet Worm Is Like Nothing Seen Before*, NEWSCIENTIST (Jan. 18, 2011, 2:16 PM), http://www.newscientist.com/article/dn19504-why-the-stuxnet-worm-is-like-nothing-seen-before.html (describing PLCs as controlling the process of industrial automation); Zetter, *supra* note 2 (noting that PLCs are involved in the control of "everything from motors in packaging assembly lines to critical valves in gas pipelines").

[36] *See* Broad et al., *supra* note 4 (stating that Stuxnet only "kicked into gear" in the presence of specific machinery); Gross, *supra* note 2, at 158 (explaining that Stuxnet "fingerprints" the PLC and looks for a specific type of machinery).

machinery rotates.[37] Finally, if the conditions are met, Stuxnet delivers its payload.[38]

Stuxnet's payload appears to be designed to achieve two things. First, it sends instructions to the PLCs to initiate quick changes in the centrifuge's rotational frequencies.[39] These quick speed changes "sabotage[] the normal operation of the industrial control process."[40] Although other machines or equipment may be unaffected by these changes in motor speed, the shifts cause harm to uranium centrifuges.[41] Second, the worm also installs a rootkit—software that enables undetectable access to a computer—which is able to send signals to facility operators that the PLCs are functioning normally.[42] System operators are therefore unable to recognize the problem and disconnect the motors from the PLC.[43]

To achieve all this, Stuxnet itself must also be able to effectively hide from detection. When Stuxnet spreads, it uses a "digital signature" to verify its authenticity with the newly infected host computer.[44] Digital signatures are likened to "passports for software: proof of identity for programs crossing

[37] *See* FALLIERE ET AL., *supra* note 29, at 41 (stating that Stuxnet's designers expected "the frequency drives to be running between 807 Hz and 1210 Hz"); Gross, *supra* note 2, at 158 (noting that Stuxnet checks to see if the PLC component is operating under specific conditions).

[38] *See* FALLIERE ET AL., *supra* note 29, at 2 (noting that Stuxnet's goal is to modify code on the Siemens PLCs); Gross, *supra* note 2, at 158 (stating that if the conditions are met, Stuxnet delivers its "rogue code").

[39] *See* William J. Broad & David E. Sanger, *Worm in Iran Was Perfect for Sabotaging Nuclear Centrifuges*, N.Y. TIMES, Nov. 19, 2010, at A1 ("Stuxnet does its damage by making quick changes in the rotational speed of motors, shifting them rapidly up and down."); FALLIERE ET AL., *supra* note 29, at 43 ("Stuxnet sabotages the system by slowing down or speeding up the motor to different rates at different times.").

[40] Broad & Sanger, *supra* note 39.

[41] *See supra* note 8 and accompanying text (noting that Stuxnet caused the PLCs to change the centrifuges' rotational frequencies).

[42] *See* FALLIERE ET AL., *supra* note 29, at 24 (noting that Stuxnet installs both windows and PLC rootkits); *Definition of Rootkit*, PC MAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=root+kit&i=55733,00.asp (last visited Nov. 8, 2011).

[43] *See* FALLIERE ET AL., *supra* note 29, at 49 ("Stuxnet records the previous operating frequencies for the frequency controllers. This data is played back . . . during the sabotage routines."); Broad et al., *supra* note 4 (stating that because of the rootkit Stuxnet made it "appear[ed] that everything was operating normally while the centrifuges were actually tearing themselves apart.").

[44] *See* FALLIERE ET AL., *supra* note 29, at 24 (describing how Stuxnet contains an authentic certificate); Gross, *supra* note 2, at 155 (comparing Stuxnet's use of an authentic digital signature to a teenager's use of a fake ID to get into a bar).

the border between one machine and the next."[45] Initially, Stuxnet's signature was obtained from Realtek Semiconductor Corporation ("Realtek"), an electronics manufacturer.[46] This signature enabled Stuxnet to gain access to computers it would otherwise have been prevented from infecting.[47]

The features described in this Section make Stuxnet a remarkable piece of malware.[48] It is a worm that, when released into any network in the world, can seek out a well-defined target, deliver its payload, and then hide the fact that it caused any damage.[49] Indeed, Stuxnet has been called a "self-directed stealth drone."[50] Not only does Stuxnet locate specific targets, but it also limits its destructive forces to those targets in a way that kinetic weapons cannot.[51] In essence, Stuxnet is a computer worm that can perform the function of a traditional kinetic weapon, only with greater precision.[52] It represents a major new development in warfare technology.[53]

[45] Gross, *supra* note 2, at 155.

[46] *See* FALLIERE ET AL., *supra* note 29, at 24 ("The [Stuxnet] driver file is a digitally signed with a legitimate Realtek digital certificate."); MATROSOV ET AL., *supra* note 28, at 13 (noting that Stuxnet was initially signed with a certificate from Realtek Semiconductor Corporation ("Realtek")).

[47] *See* Gross, *supra* note 2, at 155 (stating that the Realtek signature was the equivalent of "carrying a cops badge"); Zetter, *supra* note 2 (explaining that Stuxnet used the Realtek signature "in order to fool systems into thinking the malware was a trusted program from Realtek").

[48] *See* Ken Dilanian, *Iran and the Era of Cyber War*, L.A. TIMES, Jan. 17, 2011, at A1 (calling Stuxnet "game-changing"); *Cyberwar: The Meaning of Stuxnet*, *supra* note 12 (noting that computer security experts have described Stuxnet as "amazing," "groundbreaking," and "impressive").

[49] *See* Gross, *supra* note 2, at 159 (stating that Stuxnet can hide "both its existence and its effects until after the damage is done"); *see also supra* notes 28–53 and accompanying text (describing how Stuxnet works generally).

[50] Gross, *supra* note 2, at 159.

[51] *See* Dilanian, *supra* note 48 (quoting White House terrorism advisor Richard Clarke as calling Stuxnet "precision-guided munition"); *Cyberwar: The Meaning of Stuxnet*, *supra* note 12 (noting Stuxnet's obvious appeal to military advisors because of its ability to disable a specific target while avoiding a traditional kinetic military strike).

[52] *See* Dilanian, *supra* note 48 ("The Stuxnet worm seems to have inflicted significant damage on Iran's nuclear program, cyber experts say, with none of the dangerous repercussions of a U.S. or Israeli airstrike, at least so far."); *Cyberwar: The Meaning of Stuxnet*, *supra* note 12 (calling Stuxnet a "cyber missile").

[53] Gross, *supra* note 2 ("Stuxnet is the Hiroshima of cyber-war"); *Cyberwar: The Meaning of Stuxnet*, *supra* note 12 (referring to Stuxnet as a "new kind of cyber attack").

C. *Stuxnet's Development and Deployment*

As set forth in Section B, Stuxnet is an extremely unique piece of malware. The identity of its creators, however, is unclear. To substantiate the theories that allege that Israel and the United States created and deployed Stuxnet, this Section examines Stuxnet's distinguishing characteristics and other pieces of evidence relating to its development and deployment.

The limitation of Stuxnet's payload delivery to such a small, well-defined group of computers is unusual in malware.[54] Typically, malware designers attempt to infect and cause harm to as many computers as possible.[55] A worm that "activates" only when specific parameters are met runs contrary to the objectives of most malware programmers.[56] This specialization alone differentiates Stuxnet from most pieces of malware.

The worm also remarkably contains four "zero-day" Windows hacks, as well as a "zero-day" hack of the Siemens' SCADA software.[57] A zero-day hack exposes a vulnerability in a piece of software that was previously unknown to the developer.[58] Since most computers worldwide run Windows, a

[54] *See infra* note 56 and accompanying text (describing the uniqueness of a narrow range of payload delivery in malware).

[55] *See, e.g.*, Stefanie Hoffman, *Conficker Worm Spreads Fast, Infects Millions*, CRN, (Jan. 23, 2009, 5:17 PM), http://www.crn.com/news/security/212902319/conficker-worm-spreads-fast-infects-millions.htm (stating that the Conficker worm has infected at "least nine million" computers); Eric Larkin, *Protecting Against the Rampant Conficker Worm,* PCWORLD (Jan. 16, 2009, 2:31 PM), http://www.pcworld.com/article/157876/protecting_against_the_rampant_conficker_worm.html (noting that in less than four days the number of Conficker infections leapt from 2.4 million to 8.9 million). For example, the Conficker worm spread indiscriminately and delivered its payload to more than nine million computers worldwide. *See* Hoffman, *supra.*

[56] *See, e.g.*, Sharon Gaudin, *Storm Worm Botnet More Powerful Than Top Supercomputers*, INFORMATIONWEEK, (Sept. 6, 2007, 3:50 PM), http://www.informationweek.com/news/201804528 (stating that the Storm Botnet is used for attacks that snowball, becoming more effective as additional computers are infected). An example of a more typical piece of malware is the Storm Botnet worm that may have infected up to fifty million computers in 2007, with each infection helping to accomplish its purpose of creating a network of "zombie computers." *See id.*

[57] *See* Murchu, *supra* note 3 (stating that Stuxnet uses four zero-day vulnerabilities and that was the first time Symantec has encountered this kind of malware); *see also* FALLIERE ET AL., *supra* note 29, at 55 ("[Stuxnet] exploit[s] four 0-day vulnerabilities."); Zetter, *supra* note 2 (noting the presence of four zero-day hacks).

[58] *See* BYRON ACOHIDO & JON SWARTZ, ZERO DAY THREAT 5 (2008) (explaining that a zero-day threat "refers to a virus designed to take advantage of a security hole for which no patch exists. No patch exists because the bad guys discover the hole"); Zetter,

zero-day Windows hack is quite valuable.[59] As such, programmers almost never use more than one in a single piece of malware.[60]

The presence of four zero-day hacks speaks to the extremely high value of Stuxnet's target, the Iranian nuclear facility. A zero-day hack can only be effectively utilized one time; once the malware is distributed and the computing world becomes aware of the zero-day hack, updates from the software manufacturer quickly eliminate the vulnerability.[61] Since the four zero-day hacks have an estimated value of hundreds of thousands of dollars—excluding the value of the Realtek signature—it would only seem logical to use them together in Stuxnet only if the target was extremely valuable to the attacker.[62]

Additionally, the use of zero-day hacks demonstrates the possibility of numerous programmers working with a substantial

supra note 2 ("[Zero-day hacks] exploit vulnerabilities in software that are yet unknown to the software maker or antivirus vendors.").

[59] *See* Robert Lemos, *Bug Brokers Offering Higher Bounty,* SECURITYFOCUS (Jan. 23, 2007), http://www.securityfocus.com/news/11437 (noting that zero-day exploits can sell for upwards of US$100,000); *see also* CHARLES MILLER, INDEP. SEC. EVALUATORS, THE LEGITIMATE VULNERABILITIES MARKET: THE SECRETIVE WORLD OF 0-DAY EXPLOIT SALES, *available at* http://securityevaluators.com/files/papers/0daymarket.pdf (estimating that the value of some exploits had reached US$250,000).

[60] Miltiadis, *Is Stuxnet the 'Best' Malware Ever?*, TECH.BOX (Dec. 13, 2011), http://www.the-techbox.com/news/is-stuxnet-the-best-malware-ever-part-13/ (calling Stuxnet's use of multiple zero-day hacks "unprecedented"). Zero-day hacks also are quite rare. *See* Zetter, *supra* note 2 (noting that of the millions of pieces of malware developed each year, fewer than a dozen exploit zero-day vulnerabilities).

[61] *See, e.g.*, *Adobe Issues Patch for 'Critical' Zero-Day Vulnerability in Flash*, GOV'T COMPUTER NEWS (Sept. 22, 2011), http://gcn.com/articles/2011/09/22/adobe-flash-patch-zero-day-exploit.aspx (explaining that when Adobe learned of a zero-day exploit they issued an "out of cycle" patch to eliminate the vulnerability); *see also* John E. Dunn, *'Duqu' Zero-Day Windows Flaw Patched This Week*, ITWORLD (Dec. 13, 2011, 9:48 AM), http://www.itworld.com/operating-systems/232703/duqu-zero-day-windows-flaw-patched-week (reporting that Microsoft reacted to a zero-day exploited by the so-called Duqu malware by patching their software about a month later).

[62] *See* Zetter, *supra* note 2 ("[G]iven that they were using four zero-days to do it, the targets had to be high-value."). There is no doubt that the United States considers disabling Iran's nuclear program to be extremely valuable. In 2007, President George W. Bush said that a nuclear-armed Iran could mean "World War III." *See, e.g.*, Holly Rozenkrantz & Roger Runningen, *Bush Says a Nuclear-Armed Iran Risks 'World War III,'* BLOOMBERG (Oct. 17, 2007, 11:39 AM), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aNfIRh0cknik&refer=home (reporting President George W. Bush's concern that a nuclear-armed Iran constituted a "threat to world peace").

budget.[63] Some analysts have estimated that it could have taken five to ten programmers upwards of six months to create Stuxnet.[64] Put simply, Stuxnet is a significant technological achievement and represents the work of a well-financed, well-connected, and well-organized group of programmers, not a few individual hackers.[65] The novelty of the worm, combined with attack mechanisms that targeted several previously unknown vulnerabilities in Windows, has led to Stuxnet's description as "one of the most sophisticated pieces of malware ever."[66]

While this evidence establishes that Stuxnet's developers were both well-financed and well-organized, there is additional evidence supporting the theory that Israel and the United States were involved. First, it is hard to imagine another purpose for such a highly specialized piece of malware. The narrow range of circumstances in which Stuxnet would deploy its payload makes it unlikely that Stuxnet had another purpose besides destroying nuclear centrifuges.[67] Second, the governments' responses to news of the worm are suspicious; when Israeli officials were asked about their involvement in the worm they "broke[] into wide smiles."[68] The United States has refused to deny involvement in Stuxnet.[69] Perhaps most convincingly, a video tribute played at the retirement party of a former Israeli Defense

[63] *See infra* notes 64–66 and accompanying text (describing the resources necessary to develop malware as sophisticated as Stuxnet).

[64] *See* FALLIERE ET AL., *supra* note 29, at 3 ("The full cycle may have taken six months and five to ten core developers not counting numerous other individuals, such as quality assurance and management."). Others have put the number closer to thirty. *See* Gross, *supra* note 2, at 158 (noting that as many as thirty programmers may have worked on Stuxnet).

[65] *See Iran Accuses Siemens over Stuxnet Cyber Attack*, TELEGRAPH (London) (Apr. 17, 2011, 11:26 PM), http://www.telegraph.co.uk/technology/news/8457658/Iran-accuses-Siemens-over-Stuxnet-cyber-attack.html (noting that an Iranian commander speculated that Siemens may have given proprietary information to the US government to aid in the development of Stuxnet); Williams, *supra* note 1 (positing that the designers of Stuxnet would have needed both programming expertise and access to tightly regulated nuclear equipment to produce malware capable of harming Iran's nuclear program).

[66] Fildes, *supra* note 2.

[67] *See supra* notes 28–38 and accompanying text (describing the limits placed on delivery of Stuxnet's payload).

[68] Broad & Sanger, *supra* note 39.

[69] *See supra* note 11 and accompanying text (describing how US Deputy Defense Secretary William Lynn refused to deny that the United States was involved in Stuxnet).

Force Chief of General Staff featured references to Stuxnet as one of the general's operational successes.[70]

Traditional covert operations were probably necessary to infect the Natanz facility's network as well. Natanz's control system is a closed-network that is not connected to the Internet.[71] This means that Stuxnet would probably have needed to infect Natanz through a removable drive or a personal computer plugged directly into the network.[72] Alternatively, someone could have infected a Natanz employee's personal computer, then waited for that employee to attach the computer to the network and unwittingly infect the network.[73]

Stuxnet's code also contains numerous commands that appear, counterintuitively, to limit the ability of the worm to spread. The worm contains a "self-destruct" command that will destroy Stuxnet on June 24, 2012.[74] One of the hallmarks of Stuxnet's code is that, once infected, a computer can only transmit the worm to three other computers, which is a restriction that runs contrary to the traditional objectives of malware programmers.[75] These "fail-safes" appear to be add-ons

[70] *See Video Links Israel to Cyber Attack on Iran*, TELEGRAPH (London), Feb. 16, 2011, at 17 ("The video of Lt Gen Gabi Ashkenazi's operational successes included references to Stuxnet . . . ."); Gross, *supra* note 2, at 197 ("[G]uests at a retirement party for Israel Defense Forces chief of staff Lieutenant General Gabi Ashkenazi watched a video tribute to his career highlights—which included a reference to Stuxnet.").

[71] ALBRIGHT ET AL., *supra* note 8, at 2 ("[T]he Natanz control systems are not connected to the internet . . . ."); Kim Zetter, *Surveillance Footage and Code Clues Indicate Stuxnet Hit Iran*, WIRED (Feb. 16, 2011, 6:03 AM), http://www.wired.com/threatlevel/2011/02/isis-report-stuxnet ("Natanz's PLCs are not connected to the internet . . . .").

[72] *See* ALBRIGHT ET AL., *supra* note 8, at 2 ("[Stuxnet] needed to travel on a removable drive . . . to the Natanz control system."); FALLIERE ET AL., *supra* note 29, at 3 (noting that Stuxnet "may have been introduced by removable drive").

[73] *See* ALBRIGHT ET AL., *supra* note 8, at 2 (speculating that Stuxnet's controllers could have targeted Natanz personnel's personal computers); FALLIERE ET AL., *supra* note 29, at 3 (hypothesizing that Stuxnet may have spread through a "willing or unknowing third party").

[74] *See* Kim Zetter, *New Clues Point to Israel As Author of Blockbuster Worm, or Not*, WIRED (Oct. 1, 2010, 3:45 PM), http://www.wired.com/threatlevel/2010/10/stuxnet-deconstructed ("An apparent 'kill' date in the code indicates that Stuxnet is designed to stop working June 24, 2012."); *see also* Schneier, *supra* note 10 (stating Stuxnet has a self-destruct date of June 24, 2012).

[75] *See* FALLIERE ET AL., *supra* note 29, at 29 (noting that once Stuxnet infects three removable drives, the original is deleted); Gross, *supra* note 2, at 196 ("The USB-spreading code, for instance, limits the number of devices that each infected device can itself infect. (The limit is three, enough to create a moderate chain reaction, but not so

by programmers that are concerned about subsequent infections by Stuxnet.[76] Former US counterterrorism czar Richard Clarke stated Stuxnet's code "just says lawyers all over it."[77] As discussed later in the Note, this suggests that Stuxnet's programmers considered the LOAC, and designed Stuxnet to conform to its principles.[78]

D. *The Natanz Facility and Stuxnet's Damage*

The Natanz uranium enrichment facility is located outside of the city of Natanz, with a large portion of the facility buried underground.[79] It runs centrifuges that spin gaseous uranium to "separate fissile U-235 atoms from the denser U-238 atoms."[80] Uranium with higher percentages of U-235, or "enriched uranium," is an essential component in nuclear weapons.[81] Iran

many that its effects would rage out of control.)"); *supra* notes 54–56 and accompanying text (explaining that, traditionally, malware is designed to infect as many systems as quickly as possible).

[76] *See* Gross, *supra* note 2, at 196 (quoting Richard Clarke as saying that a "responsible government . . . [would] have to prevent collateral damage").

[77] *Id.*

[78] *See infra* Part III (noting that although the LOAC did not apply to Stuxnet, its programmers gave up operational effectiveness to comply with LOAC rules).

[79] *See* David Albright & Corey Hinderstein, Inst. Sci. & Int'l Sec., The Iranian Gas Centrifuge Uranium Enrichment Plant at Natanz: Drawing from Commercial Satellite Images (2003), *available at* http://www.isis-online.org/publications/iran/natanz03_02.html (describing the Natanz facility as a high-security uranium enrichment facility that includes numerous underground buildings); *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 (stating that the Natanz uranium enrichment is located underground).

[80] *Iran Increases Uranium Enrichment—IAEA*, BBC NEWS, Aug. 10, 2010, http://www.bbc.co.uk/news/world-europe-10925381 (stating that Natanz centrifuges spin uranium hexafluoride gas to separate U-235 from U-238 atoms); *see Iran and Syria: Next Steps: Hearing Before the H. Comm. on Foreign Affairs*, 112th Cong. 2 (2011) (statement of Olli J. Heinonen, Senior Fellow, Belfer Center for Science and International Affairs, Harvard University) (stating that Natanz produces enriched uranium).

[81] *See Fissile Materials and Nuclear Weapons*, INT'L PANEL FISSILE MATERIALS, http://www.fissilematerials.org/ipfm/pages_us_en/fissile/production/production.php (last visited Nov. 8, 2011) (citing INT'L PANEL FISSILE MATERIALS, 2006 GLOBAL FISSILE MATERIAL REPORT) (explaining that isolating the U-235 isotope is essential for the production of a nuclear weapon); Mark D. Sameit, Note, *Killing and Cleaning in Combat: A Proposal to Extend the Foreign Claims Act to Long-Term Environmental Damage*, 32 WM. & MARY ENVTL. L. & POL'Y REV. 547, 575 (2008) ("The enriched U-235 is known as 'enriched uranium' and can be used in commercial or military reactors, or as fuel for nuclear weapons.").

has repeatedly stated that their nuclear program is peaceful and its only purpose is to generate nuclear power.[82] US officials, however, doubt Iran's claims, and believe that the purpose of the facility at Natanz is to secure weapons-grade uranium.[83]

As previously explained, Stuxnet was most likely designed to destroy centrifuges at Natanz by systematically raising and lowering their rotational speed.[84] Stuxnet seems to have succeeded in this respect. Subsequent to the date of infection, international inspectors reported that Iran was experiencing severe problems with its centrifuges and that several hundred had been shut down.[85] An inspection in late 2009 revealed that close to 1000 centrifuges had been removed from Natanz since the previous summer.[86] It appears that this has caused significant delays to Iran's nuclear weapons program.[87]

The extent of the damage done to the Iranian nuclear program is unknown. There are reports that Iran successfully contained much of the damage caused by Stuxnet and replaced

[82] *See Iran's President Says Bush Pushing for War*, NBC NIGHTLY NEWS, Sept. 19, 2006, http://www.msnbc.msn.com/id/14911603/ns/nightly_news/t/irans-president-says-bush-pushing-war/ (quoting President Ahmadinejad in an interview with NBC as saying, "[w]e are against the atomic bomb"); *see also* Alan Cowell & Michael Slackman, *Iran Boasts of Capacity to Make Bomb Fuel*, N.Y. TIMES, Feb. 12, 2010, at A4 (quoting President Ahmadinejad as saying, "[w]hen we say we won't build [a nuclear weapon] that means we won't").

[83] *See* Charles J. Moxley, *Obama's Nuclear Posture Review: An Ambitious Program for Nuclear Arms Control but a Retreat from the Objective of Nuclear Disarmament*, 34 FORDHAM INT'L L.J. 734, 767 (2011) (noting that the Obama administration has stated it seeks to reverse Iran's ambition to acquire a nuclear weapon); Mark Landler, *Clinton Says Sanctions Have Stalled Iran's Effort to Make Nuclear Weapons*, N.Y. TIMES, Jan. 11, 2011, at A4 (describing US Secretary of State Hillary Clinton's concern over Iran's effort to acquire nuclear weapons).

[84] *See supra* notes 39–43 and accompanying text (describing the method by which Stuxnet destroyed the centrifuges at Natanz).

[85] *See* Broad & Sanger, *supra* note 39 (stating that reports issued by international inspectors show Iran removed hundreds of centrifuges in 2009); Zetter, *supra* note 71 (explaining that surveillance footage from the United Nations showed Iranian workers dismantling ten percent of the plant's centrifuges).

[86] *See* Broad et al., *supra* note 4 ("[W]hen 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."); Zetter, *supra* note 2 (stating that International Atomic Energy Agency surveillance footage at Natanz showed between 1000 and 2000 centrifuges being replaced after the Stuxnet attack).

[87] *See* Broad et al., *supra* note 4 (commenting that the destruction of centrifuges at Natanz helped delay, but not destroy, Iran's nuclear weapons program); Williams, *supra* note 1 (stating that Iranian officials confirmed that Stuxnet had set back their nuclear program).

many of the broken centrifuges.[88] It is likely, however, that Stuxnet affected the Iranian nuclear program in other ways. Iran appears to be suffering from a shortage of certain types of metals that are needed to run the machines, and usable metal was lost because of Stuxnet.[89] Additionally, Stuxnet almost certainly had a psychological effect on the Iranians; a facility they thought to be completely secure was infected with malware whose designers possessed a high degree of knowledge about Natanz's centrifuges and the facility generally.[90] Finally, to be fully rid of the worm, Iran would most likely have to replace all the computer systems in the nuclear program, an exceedingly difficult proposition for a country under strict trade sanctions.[91] Consequently, Israeli intelligence officials delayed their estimates for when Iran will acquire a nuclear weapon to 2015.[92]

This was not the first time that Western nations attempted to hinder an Arab country's nuclear program. In 2007, Israel launched F-15 fighter jets to bomb a Syrian facility believed to be an underground nuclear reactor.[93] The facility was completely

[88] *Iran's Centrifuges Again Enriching Uranium at Full Speed, Late 2010 Lull Attributed to Stuxnet Computer Worm*, JERUSALEM POST, Feb. 9, 2011, at 20 (stating that after a decline in production because of Stuxnet, uranium enrichment regained "full speed"); Joby Warrick, *Iran Recovered Swiftly in Wake of Cyberattack*, WASH. POST, Feb. 16, 2011, at A1 (stating Iran responded with an effort to "contain the damage and replace broken parts").

[89] *See* DAVID ALBRIGHT ET AL., INST. SCI. & INT'L SEC., STUXNET MALWARE AND NATANZ: UPDATE OF ISIS DECEMBER 22, 2010 REPORT 4 (2011), *available at* http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf (noting that Iran is facing a shortage of raw materials to build centrifuges); Joby Warrick, *Iran 'Set Back' on Nuclear Program*, WASH. POST, Oct. 17, 2011, at A1 (reporting that a shortage in materials caused Iran to construct centrifuges from an inferior type of metal).

[90] *See* FALLIERE ET AL., *supra* note 29, at 3 (noting that "reconnaissance" was necessary for Stuxnet's designers to understand how PLCs were configured at the attack site); Warrick, *supra* note 89 ("[Stuxnet's] designers possessed highly detailed knowledge of Natanz's centrifuges and how they are interconnected . . . .").

[91] *See* Dilanian, *supra* note 48 (quoting cyber security expert Ralph Langner as saying that replacing all the nuclear program's computer systems would be necessary to delete the worm and would constitute "a tall order for a country under sanctions").

[92] *See* Mark Landler, *Clinton Urges Gulf States to Maintain Iran Sanctions*, N.Y. TIMES, Jan. 10, 2011, at A4 (stating that Meir Dagan, an Israeli intelligence official, said that Iran's nuclear program will not produce a nuclear weapon before 2015); Warrick, *supra* note 89 (["Israel's] outgoing intelligence chief estimated . . . that the Islamic republic could not have a bomb before 2015.").

[93] *See* Con Coughlin, *The Real Reason Why a Syria Base Was Wiped Off the Map*, TELEGRAPH (London), Apr. 25, 2008, at 23 (explaining that Israeli F-15's struck the

destroyed, leaving only "a big hole in the desert."[94] In comparison, Stuxnet managed to strike only the centrifuges at Natanz, without affecting the civilians working in the plant, or causing damage to civilian computer systems connected to the Natanz network.[95]

E. *Stuxnet's Proliferation Outside Natanz*

Stuxnet's discovery triggered a sense of panic among many industrial firms. Western nations, after a cursory analysis of Stuxnet's code, feared that the worm might attack all PLCs worldwide.[96] Such an attack could cause the shutdown of factories, power plants, and other facilities vital to the functioning of civil society.[97] These fears, however, were never realized.

Because Stuxnet spreads indiscriminately, despite the limitations described above, it has spread throughout the globe.[98] As of this moment, it is unclear how many computers Stuxnet has infected, but a September 2010 Symantec study

Syrian facility); David E. Sanger & Mark Mazzetti, *Analysts Find Israel Struck a Syrian Nuclear Project*, N.Y. TIMES, Oct. 13, 2007, at A1 (stating that Israel struck a site "analysts judged was a partly constructed nuclear reactor").

[94] *Syria Complains to U.N. About Israeli Airstrike*, CNN WORLD, Sept. 11, 2007, http://articles.cnn.com/2007-09-11/world/israel.syria_1_israeli-airstrike-syrian-foreign-minister-walid-syrian-government?_s=PM:WORLD (discussing the magnitude of the destruction caused by the Israeli airstrike).

[95] *See infra* notes 100–02 and accompanying text (detailing the lack of damage to civilian computers); *supra* notes 49–51 and accompanying text (proving the lack of any physical harm to individuals at Natanz).

[96] *See* Gross, *supra* note 2, at 155 (noting that Stuxnet had "the potential to bring industrial society to a halt"); Zetter, *supra* note 2 (explaining that Stuxnet's intial researcher's website was "beseiged" with visits and that he "perfom[ed] a huge public service to help protect critical infrastructures").

[97] *See* Gross, *supra* note 2, at 155 (stating that PLCs, in addition to controlling the speed of the centrifuges at Natanz, are more commonly involved in the operation of factories, power plants, and construction projects all over the world); Schneier, *supra* note 10 (noting that PLCs control systems that operate in factories, chemical plants, oil refineries, and nuclear power plants).

[98] *See* FALLIERE ET AL., *supra* note 29, at 3–5 (noting that Stuxnet infected computers in Azerbaijan, Great Britain, India, Indonesia, Iran, Pakistan, the United States, and numerous others); MATROSOV ET AL., *supra* note 28, at 15 (citing Iran, Indonesia, and India as the three countries with the most Stuxnet infections).

showed over 100,000 infections worldwide.[99] The worm, however, appears to have done little harm. Stuxnet infected only twenty-four industrial systems outside Iran, and there have been no documented cases, outside of the Iranian nuclear facilities, in which Stuxnet's payload was activated and delivered.[100] As such, there seem to be no incidents of industrial damage linked to Stuxnet.[101] At this point, Stuxnet's main impact on the general computing world has been limited to the nuisance of deleting the worm off infected systems, and even that has been minor, as Stuxnet does not replicate to a point that it inhibits computer or network functions.[102]

This, however, may not be the end of the story for damage traceable to Stuxnet. Computer-science experts warned that Stuxnet's code could be a model for third parties to attack other industrial facilities and hypothesized that Stuxnet's proliferation has increased the risk of similar cyber attacks worldwide.[103] This hypothesis appears to have been accurate: internet-security firms detected a "relative" of Stuxnet, one that appears to utilize

[99] *See* FALLIERE ET AL., *supra* note 29, at 5 (noting over 100,000 Stuxnet infections); Zetter, *supra* note 2 (stating that there have been more than 100,000 Stuxnet infections).

[100] *See SIMATIC WinCC / SIMATIC PCS 7: Information About Malware / Viruses / Trojan Horses*, SIEMENS INDUSTRY SERVICE & SUPPORT, http://support.automation.siemens.com/WW/llisapi.dll?func=ll&objid=43876783&nodeid0=10805583&caller=view&lang=en&siteid=cseus&aktprim=0&objaction=csopen&extranet=standard&viewreg=WW#Recommended_procedure%200408 (last updated Mar. 11, 2011) (stating that a total of twenty-four Siemens customers in the industrial sector reported infections, and that "[i]n none of these cases did the infection have an adverse impact").

[101] *See id.* (noting the absence of instances in which Stuxnet had an "adverse impact" on an industrial system); *see also US Also Vulnerable to Stuxnet Virus, Official Warns*, AOL NEWS (Dec. 7, 2010, 3:51 PM), http://www.aolnews.com/2010/12/07/us-also-vulnerable-to-stuxnet-virus-official-warns/ (quoting a US Department of Homeland Security official as saying that "it's not clear there are [sic] any particular process within the United States that would have triggered the software").

[102] *See supra* notes 75–76 and accompanying text (noting the restrictions Stuxnet has on self-replication).

[103] *See Securing Critical Infrastructure in the Age of Stuxnet: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. 1 (2010) (statement of Michael J. Assante, President and Chief Executive Officer, National Board of Information Security Examiners of the United States) (stating that Stuxnet could serve as a "blueprint for future attackers"); Ellen Nakashima, *Stuxnet Malware Is Blueprint for Computer Attacks on U.S.*, WASH. POST, Oct. 2, 2010, at A3 ("[T]he possibility that Stuxnet could be used by copycats, even those who don't intend to do harm with it, is causing concern among experts.").

pieces of code from Stuxnet, in October 2011.[104] Called the "Duqu" virus, this code differs substantially from Stuxnet in its apparent goals. Duqu appears to gather data from host computers, possibly compiling information for a future attack.[105] Duqu's authors are unknown. A third party may have acquired Stuxnet's code and altered it to further its own purposes, or the original designers of Stuxnet may also have programmed Duqu.[106] The next phase of the Duqu attack is also unknown.[107]

F. *Assumptions for the Remainder of this Note*

The facts described in Part I.A–E allude to the possibility that Israel and the United States developed Stuxnet to target Iran's Natanz nuclear facility. The high value of Stuxnet's zero-day hacks, the discriminating nature of Stuxnet's payload, the substantial budget necessary to create Stuxnet, and statements made by Israeli and US officials suggest that both countries likely played a role in Stuxnet's development and deployment.[108]

[104] *See* Zulfikar Abbany, *'Son of Stuxnet' Hits European Computer Networks*, DEUTSCHE WELLE, Oct. 21, 2011, http://www.dw-world.de/dw/article/0,,15478105,00.html (calling Duqu a "relative" of Stuxnet); Jim Finkle & Supantha Mukherjee, *Duqu Computer Virus Prompts Indian Authorities to Seize Computer Equipment*, HUFFINGTON POST (Oct. 29, 2011, 2:56 PM), http://www.huffingtonpost.com/2011/10/29/duqu-computer-virus-prompts_n_1065217.html (stating Duqu's code is similar to Stuxnet).

[105] SYMANTEC SEC. RESPONSE, W32.DUQU: THE PRECURSOR TO THE NEXT STUXNET 1 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf ("Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party.").

[106] *Compare id.* (stating that Duqu probably came from the same author as Stuxnet), *with* SecureWorks Counter Threat Unit Research Team, *Duqu Trojan Questions and Answers*, DELL SECUREWORKS (Oct. 26, 2011), http://www.secureworks.com/research/threats/duqu/ (suggesting that Duqu and Stuxnet may be unrelated).

[107] *See* Abbany, *supra* note 104 (describing Duqu as "waiting" and stealing information); Tony Bradley, *Duqu: New Malware Is Stuxnet 2.0*, PCWORLD (Oct. 18, 2011, 2:22 PM), http://www.pcworld.com/businesscenter/article/242114/duqu_new_malware_is_stuxnet_20.html (speculating that Duqu may be gathering information to launch a subsequent attack).

[108] *See supra* notes 57–62 and accompanying text (describing the high value of Stuxnet's zero-day hacks); *supra* notes 28–53 and accompanying text (explaining how Stuxnet proliferates and delivers its payload); *supra* notes 63–66 and accompanying text

For academic purposes, this Note assumes that to be true. All other facts about Stuxnet, such as how the worm worked and the damage that it did to the nuclear installations, are analyzed based entirely on available evidence.

This Note also assumes that the LOAC applies to Stuxnet. This is necessary to analyze whether Stuxnet violates the LOAC and whether the LOAC properly regulates Stuxnet. In fact and in law, however, the LOAC—which fully applies only during an armed conflict—did not apply to Stuxnet because Israel and the United States are not involved in an armed conflict with Iran.[109] Applying the LOAC to Stuxnet is an important exercise because there have been few, if any, other recorded cyber attacks to which the LOAC applies. It is understandably difficult to analyze the effectiveness of the LOAC in regulating cyber war when there have been no instances in which it is applicable. It is therefore worthwhile to analyze an actual event—Stuxnet—under the LOAC, even though the requisite conditions for the LOAC to apply were not present. This Note engages in such a hypothetical analysis.

II. *THE HISTORY AND SUBSTANCE OF LOAC PRINCIPLES RELATING TO CYBER WAR*

Despite appearing chaotic, war takes place within a legal framework of rules.[110] International law regulates the conduct of

(detailing the significant resources required to program Stuxnet); *supra* notes 11, 68, 70 and accompanying text (illustrating the American and Israeli reactions to Stuxnet).

[109] *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention) art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter First Geneva Convention] (stating the LOAC applies during an "armed conflict" or conflict between two parties to the treaty even if the parties have not formally recognized a state of war between them); Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) ("[A]n armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups . . . . [The LOAC] applies from the initiation of such armed conflicts . . . until a general conclusion of peace is reached . . . .").

[110] *See* ROBERT KOLB & RICHARD HYDE, AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICTS 15 (2008) ("War . . . does not take place in a vacuum of legal rules."); INT'L COMM. OF THE RED CROSS, WHAT IS INTERNATIONAL HUMANITARIAN LAW? (2004), *available at* http://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf (stating that the LOAC is a set of rules that "limit the effects of armed conflict").

belligerents during an armed conflict, irrespective of the legality of the initial use of force.[111] Historically, these rules were referred to by the Latin expression *jus in bello*, which means the rules that regulate warfare.[112] Today, they are called the LOAC.[113]

There is no specific provision in the LOAC stating that LOAC restrictions apply to the use of cyber weapons.[114] There appears, however, to be a consensus among scholars and nations that LOAC principles do apply to cyber war.[115] As discussed below, the LOAC developed over many centuries and is codified primarily in the Hague Conventions, Geneva Conventions, and Additional Protocols.[116] These treaties were signed in 1907, 1949, and 1977 respectively.[117] As such, cyber weapons are

[111] *See* LORI FISLER DAMROSCH ET AL., INTERNATIONAL LAW 1276 (5th ed. 2009) (explaining that traditionally, under the laws of war, "deviations from the laws of war . . . [are] violations of international law")*;* MALCOLM N. SHAW, INTERNATIONAL LAW 1167 (6th ed. 2008) (stating that international law "seeks to regulate the conduct of hostilities"); Schmitt, *supra* note 21, at 368 (showing that the LOAC concerns itself with what is and is not permissible during an armed conflict "irrespective of the legality of the initial resort to force by the belligerents").

[112] *See* KOLB & HYDE, *supra* note 110 ("*[J]us in bello* means the rules relating to the conduct of warfare."); SHAW, *supra* note 111 (stating that *jus in bello* regulates the conduct of hostilities).

[113] *See* Dep't of Def., Directive 2311.01E: DoD Law of War Program (2006) (designating the term "law of armed conflict" as the official term used by the US Department of Defense to describe "international law that regulates the conduct of armed hostilities"). The term "international humanitarian law" is sometimes used for and is interchangeable with the LOAC. *See, e.g.*, Nicholas Rostow, *Wall of Reason: Alan Dershowitz v. the International Court of Justice*, 71 ALB. L. REV. 953, 980 n.92 (2008) (asserting that the term "laws of war" is "[a]lso known, interchangeably, as 'international humanitarian law' or 'the law of armed conflict'").

[114] *See* DAMROSCH ET AL., *supra* note 111, at 1304 (noting that whether the LOAC applies to cyber war remains to be resolved); Schmitt, *supra* note 21, at 368 ("[T]here is no provision in any humanitarian law instrument that directly addresses CNA . . . .").

[115] *See, e.g.*, Jensen, *supra* note 22, at 1187 ("The law of war clearly applies to the use of CNA in armed conflict."); Schmitt, *supra* note 21, at 375 ("[C]omputer network attacks are subject to humanitarian law if they are part and parcel of either a classic conflict or a "cyber war" in which injury, death, damage or destruction are intended or foreseeable."). The official US position is that the LOAC applies to CNAs. *See* OFFICE OF GEN. COUNSEL, DEPT. OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 8 (1999) (stating that the use of cyber weapons to "cause injury, death, damage, and destruction" will be judged by applying the LOAC).

[116] *See infra* notes 136–37 and accompanying text (describing the primary sources of the LOAC).

[117] Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277 [hereinafter Hague Convention IV]; First Geneva

regulated by rules created at times in which cyber war was either unimaginable or confined to the realms of science fiction; indeed, the earliest cyber weapons appeared in 1970s science-fiction novels.[118] Academics have therefore questioned whether these rules are capable of effectively regulating cyber war.[119]

Scholars generally divide into two camps on whether current LOAC rules adequately regulate cyber war: those that believe that current LOAC rules can adequately address cyber war and those that believe new treaties will be necessary to regulate it effectively.[120] Governments, by and large, have argued that new rules are not necessary to regulate cyber war.[121] To determine whether current LOAC rules adequately regulate cyber war, one must first ask what the purposes of the applicable rules are. If the rules, as applied to Stuxnet, accomplish those policy objectives, then Stuxnet represents one piece of evidence that current LOAC paradigms adequately regulate cyber war.

There are two primary policy purposes behind all *jus in bello* rules. First, the LOAC aims to lower the level of violence that occurs during an armed conflict.[122] This is most easily

Convention, *supra* note 109; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea (Second Geneva Convention), Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Fourth Geneva Convention]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

[118] *See, e.g.*, JOHN BRUNNER, THE SHOCKWAVE RIDER (1975) (describing how a computer worm—called a "tapeworm" in the novel—is used to alter data kept by a government entity).

[119] *See, e.g.*, Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 274 (1996); Schmitt, *supra* note 21.

[120] *See supra* note 22 (comparing two differing positions on the adequacy of current LOAC rules).

[121] *See* Schaap, *supra* note 19, at 124 (stating that governments have "resisted calls to craft new rules of international law to govern attacks on or by computers"); Duncan B. Hollis, *Rules of Cyberwar?*, L.A. TIMES, Oct. 8. 2007, at A15 (noting government hesitancy to design new rules to regulate cyber war).

[122] *See* I MARCO SASSÒLI & ANTOINE A. BOUVIER, INT'L COMM. OF THE RED CROSS, HOW DOES LAW PROTECT IN WAR? CASES, DOCUMENTS AND TEACHING MATERIALS ON CONTEMPORARY PRACTICE IN HUMANITARIAN LAW 81–82 (2d ed. 2006) (noting that a goal of the LOAC is "limiting the violence" of the armed conflict); Michael N. Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 YALE HUM.

demonstrated in rules that "prohibit [the] use of particular weapons or forbid the creation of unnecessary suffering."[123] Second, the LOAC attempts to protect individuals who are not participating in the conflict from suffering physical harm or damage to their property.[124] Part III of this Note explores whether the LOAC furthers these objectives when applied to Stuxnet.

A. *History of the LOAC*

Throughout the majority of history, war was mostly devoid of formal rules regulating the conduct of participants.[125] There is evidence, however, that some ancient civilizations regulated combatants' actions on the battlefield and their treatment of non-combatants and prisoners to some extent.[126] Most of these rules stemmed from religious principles that called for compassion in certain situations.[127] Compared with the explosion of LOAC rules in recent centuries, however, these rules were sparse.[128]

The 1862 book, *A Memory of Solferino* ("*Memory*"), written by the Swiss businessman Henri Dunant, is cited as the intellectual birth of the modern LOAC.[129] After witnessing more than 40,000

RTS. & DEV. L.J. 143, 145 (1999) ("The first [LOAC goal] is a desire to ratchet down the level of violence that occurs in armed conflict . . . .").

[123] Schmitt, *supra* note 122, at 145.

[124] *See* KOLB & HYDE, *supra* note 110, at 15 (stating that the LOAC is necessary to protect the potential civilian victims of war, as well as wounded, sick, or prisoner combatants); Schmitt, *supra* note 122, at 145 (stating that the LOAC's second purpose is to "shield those who are not directly participating in the conflict from its effects").

[125] *See* INGRID DETTER, THE LAW OF WAR 151 (2d ed. 2000) (discussing early war rules and noting that victors in a war typically used "barbaric practices").

[126] *See id.* (noting the Egyptians had agreements regarding the treatment of prisoners of war); GEOFFREY S. CORN ET AL., LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH (forthcoming May 2012) (manuscript ch. 2, at 2–3) (noting that the "Just War" theory used by Christians in the Roman Empire had beneficial effects on the practice of war, at least when both sides were Christian).

[127] *See* CORN ET AL., *supra* note 126, ch. 2, at 2–3 (discussing religious belief as a basis for early laws regulating war).

[128] *See* KOLB & HYDE, *supra* note 110, at 39 (explaining that, as time passed, the number of LOAC regulations increased); CORN ET AL., *supra* note 126, ch. 2, at 3 (noting the lack of a "comprehensive set of guidelines" prior to the 18th century).

[129] *See, e.g.*, SHAW, *supra* note 111, at 1168 (noting that the law began developing in the middle of the nineteenth century thanks to Henri Dunant's writing); CORN ET AL., *supra* note 126, ch. 2, at 4 (crediting Dunant's writing as the impetus for the First Geneva Convention).

wounded soldiers left to die after a massive battle between Austrian, French, and Sardinian forces, Dunant wrote *Memory* in an attempt to advocate for the formation of some inviolate "international principle" that would give legal protection to wounded military personnel.[130] Dunant's proposals eventually prompted the formation of the First Geneva Convention for the Amelioration of the Condition of the Wounded Armies in the Field, which provided certain forms of protection to soldiers injured in battle.[131]

The LOAC continued to grow during the nineteenth and twentieth centuries, most notably through treaties. The Hague Conventions of 1907 created laws regulating the means and methods of war, while the Geneva Conventions of 1949 expanded on principles designed to protect individuals not participating in the hostilities.[132] In 1977, the Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts ("AP I") supplemented existing regulations under the Geneva Conventions.[133] AP I updated principles limiting the means and methods of war for parties to an armed conflict.[134] It also codified principles that limited attacks to military objectives.[135]

[130] *See* KOLB & HYDE, *supra* note 110, at 37–38 (depicting how Dunant witnessed 40,000 wounded soldiers left to die on the battlefield after the battle of Solferino); CORN ET AL., *supra* note 126, ch. 2, at 4 (stating that witnessing these horrors inspired Dunant to write *A Memory of Solferino*).

[131] *See* SHAW, *supra* note 111, at 1168 (commenting that as a result of Dunant's writing, the First Geneva Convention was adopted); CORN ET AL., *supra* note 126, at 4 ("[Dunant's] suggestions were taken up by others, and led to the formation of . . . the first Geneva Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, which among other things provided for use of the red cross symbol to distinguish hospitals, ambulances and evacuation parties.").

[132] *See, e.g.*, Hague Convention IV, *supra* note 117, art. 23(e) (prohibiting weapons "calculated to cause unnecessary suffering"); Fourth Geneva Convention, *supra* note 117, art. 3(1) (stating that "[p]ersons taking no active part in the hostilities . . . shall in all circumstances be treated humanely").

[133] *See* AP I, *supra* note 117, art. 1(3) (stating that the Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts ("AP I") supplements the Geneva Conventions and applies in the same circumstances).

[134] *See, e.g.*, *id.* art. 57(2) (articulating the principle of proportionality).

[135] *See id.* art. 48 ("Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objectives and military objectives . . . .").

B. *LOAC Sources*

International law can be found in several different sources that are enumerated in Article 38(1) of the International Court of Justice statute, which is recognized as the definitive statement on the sources of international law.[136] As defined in the Statute of the International Court of Justice, these sources are: (1) international treaties, (2) customary international law, (3) general principles of law, and (4) judicial decisions and publications.[137] The remainder of this Section focuses on treaties and customary law, as cyber war principles are predominantly drawn from these sources.

1. Treaties

Treaties are written agreements through which nations legally bind themselves to behave in a particular way. [138] Although a comparatively modern method for creating LOAC rules, the number of LOAC treaties has exploded over the last century, making treaties one of the first places to find the LOAC.[139] Some scholars consider treaties to be superior to other sources of international law, including customary law, because they reflect the express consent of the treaty signatories.[140]

[136] *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 5 (7th ed. 2008) (noting that Article 38 is "regarded as a "complete statement of the sources of international law"); *see also* DAMROSCH ET AL., *supra* note 111, at 55 (beginning an explanation of the sources of international law with Article 38).

[137] Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 1060 [hereinafter ICJ Statute].

[138] *See* BROWNLIE, *supra* note 136, at 13 (stating that treaties are binding on parties to them).

[139] *See* DETTER, *supra* note 125, at 151–52 (explaining that although seventeenth century treaties regulating armed conflict exist, prohibitions on the use of force date back to 1400 BC); CORN ET AL., *supra* note 126, ch. 2, at 2–6 (citing the existence of the LOAC "since antiquity"); *see also* DAMROSCH ET AL., *supra* note 111, at 1277 (noting the importance of Hague Conventions, Geneva Conventions, and Additional Protocols and stating that the treaties have received "widespread multilateral adherence"); KOLB & HYDE, *supra* note 110, at 40–41 (positing that important recent developments in the law of conflict are the Hague Conventions, Geneva Conventions, and Additional Protocols, all of which are treaties).

[140] *See, e.g.*, SHAW, *supra* note 111, at 94 ("For many writers, treaties constitute the most important sources of international law . . . ."); Juliana Murray, *Assessing Allegations: Judicial Evaluation of Testimonial Evidence in International Tribunals*, 10 CHI. J. INT'L L. 769, 771 (2010) ("Treaties are also widely recognized by scholars as a valid

Only nations that are parties to a particular treaty are bound by the treaty itself.[141] In addition to creating law, however, treaties are also capable of codifying existing law.[142] Courts may therefore look to treaties to express principles of customary law that are applicable to states not party to the treaty in question.[143] As explained below, this is particularly important to Israel and the United States, who are not parties to AP I, one of the more important post-World War II treaties.[144]

2. Custom

Customary law is an important source of the LOAC.[145] In fact, without a treaty on point, customary law is frequently the only source of law that addresses a particular LOAC topic.[146] For a rule of law to apply to states through "international custom," the behavior must be a "practice accepted as law."[147] Customary law therefore has two requirements: (1) demonstrated state

source of international law that may in some circumstances be superior to custom, when treaties can more clearly reflect the parties' specific intentions.").

[141] *See* BROWNLIE, *supra* note 136, at 13 ("[T]reaties are in principle binding only on parties."); SHAW, *supra* note 111, at 95 (explaining that treaties create rules that are binding upon the parties).

[142] *See* DAMROSCH ET AL., *supra* note 111, at 124 (noting that the Vienna Convention was invoked even prior to its entry into force because it was "largely declaratory of customary international law"); SHAW, *supra* note 111, at 95 ("[W]here treaties reflect customary law then non-parties are bound, not because it is a treaty provision but because it reaffirms a rule or rules of customary international law.").

[143] *See* Rebecca Crootof, *Judicious Influence: Non-Self-Executing Treaties and the* Charming Betsy *Cannon*, 120 YALE L.J. 1784, 1798 (2011) (explaining that US courts often look to treaties as evidence of customary law regardless of whether the United States is a party to the treaty); Eric W. Sievers, *Transboundary Jurisdiction and Watercourse Law: China, Kazakhstan, and the Irtysh*, 37 TEX. INT'L L.J. 1, 14 (2002) (stating that customary law "can be gleaned from a variety of sources," including treaties).

[144] *See* Samuel Estreicher, *Privileging Asymmetric Warfare? Part I: Defender Duties Under International Humanitarian Law*, 11 CHI. J. INT'L L. 425, 430 (2011) (noting that Israel and the United States continue their refusal to ratify AP I); *List of Signatories to AP I*, INT'L COMM. OF THE RED CROSS, http://www.icrc.org/IHL.nsf/WebSign?ReadForm&id=470&ps=P (last visited Mar. 13, 2012) (indicating that Israel and the United States are not parties to AP I). AP I is particularly important to this Note because it codifies the principles of distinction, discrimination, and proportionality.

[145] *See* KOLB & HYDE, *supra* note 110, at 51 (explaining that customary law is one of the main sources of the LOAC); CORN ET AL., *supra* note 126, ch. 2, at 18 (stating that customary law is an "important source of the [LOAC]").

[146] *See* CORN ET AL., *supra* note 126, ch. 2, at 18 (stating that customary law "may be the only source" of law on a particular LOAC topic).

[147] ICJ Statute, *supra* note 137, art. 38(1)(b).

practice, and (2) a subjective belief by the state that they are under a duty of law to follow the state practice.[148] That a state behaves in a particular way is therefore not sufficient to form customary international law; there must also be a subjective belief, termed *opinio juris*, on the part of the state that they had a legal duty to behave that way.[149]

For a custom to constitute "state practice," it must be of sufficient (1) duration, (2) uniformity, and (3) generality amongst the states.[150] There is no specific length of time that a practice must have existed for there to be sufficient duration.[151] Frequently, the length of time depends upon the type of practice in question.[152] In more modern or dynamic fields, rules can develop quickly.[153] In more established fields of law, customary law is slower to develop.[154] The custom need not be followed without fail, but needs to be of a consistent nature

[148] *See* BROWNLIE, *supra* note 136, at 7–8 (breaking "practice" down into elements of duration, uniformity, and generality, and describing *opinio juris* as a separate and necessary element of international custom); DAMROSCH ET AL., *supra* note 111, at 59 (explaining that custom has "two distinct elements: (1) 'general practice' and (2) its acceptance as law [i.e. *opinio juris*]").

[149] DAMROSCH ET AL., *supra* note 111, at 59 (noting the *opinio juris* element of customary law); CORN ET AL., *supra* note 126, ch. 2, at 19 ("Thus, the mere fact that States may engage in a practice (or not engage in a practice) is not enough to indicate that it required as a matter of customary law. States also must consider the practice or its omission to be a legal requirement.").

[150] *See* BROWNLIE, *supra* note 136, at 7–8 (breaking the "state practice" requirement into duration, uniformity, and generality of the practice); Anguel Anastassov, *Are Nuclear Weapons Illegal? The Role of Public International Law and the International Court of Justice*, 15 J. CONFLICT & SEC. L. 65, 79 (2010) (noting the general criteria for "state practice" is duration, uniformity, and generality).

[151] *See* SHAW, *supra* note 111, at 76 (stating that the time necessary can vary from "time immemorial" to a matter of decades).

[152] *Compare* SHAW, *supra* note 111, at 78 (stating that the law on airspace developed quickly following the invention of manned aircraft), *with* Paquete Habana, 175 U.S. 677, 686–700 (1900) (analyzing examples of state practice as far back as 1403 in an effort to establish state practice for customary laws regulating civilian fishing boats during a time of war).

[153] *See* BROWNLIE, *supra* note 136, at 7 ("[R]ules relating to airspace and the continental shelf have emerged from fairly quick maturing of practice."). *See generally* Benjamin Langille, Note, *It's "Instant Custom": How the Bush Doctrine Became Law After the Terrorist Attacks of September 11, 2001*, 26 B.C. INT'L & COMP. L. REV. 145 (2003) (arguing that "instant custom" formed in response to the September 11, 2001, terrorist attacks on the World Trade Center and Pentagon).

[154] *See, e.g.*, *Paquete Habana*, 175 U.S. at 686–700 (examining 600 years of history to establish customary law in regards to fishermen).

throughout the history of the practice.[155] Finally, the practice must be "widespread and representative" to satisfy the "generality" requirement.[156] Once the "state practice" element is established, courts examine the lens through which the state views its own behavior. The practice will only constitute customary law if the state also satisfies the *opinio juris* requirement.[157]

C. *Relevant LOAC Principles*

There are two cardinal principles of the LOAC: military necessity and humanity.[158] The principle of military necessity is articulated in the preamble to the St. Petersburg Declaration—the first formal agreement prohibiting the use of certain weapons in war—which states, "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy."[159] The principle is further illuminated in the United States Air Force manual, which states that military necessity has four basic elements: (1) that force is regulated; (2) that force is necessary to achieve as quickly as possible the partial or complete submission of the adversary; (3) that the force is no greater than needed to achieve this; and (4) that it is not otherwise prohibited.[160] The principle therefore requires that a belligerent use only such force as is necessary to overpower the enemy and result in the enemy's surrender.[161]

[155] *See id.* at 689 (noting that the practice had been violated by the French in a few instances); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 186 (June 27) ("It is not to be expected that in the practice of States the application of the rules in question should have been perfect . . . .").

[156] North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.), 1969 I.C.J. 3, ¶ 73 (Feb. 20).

[157] *See* S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 28 (Sept. 7) (noting that only if the state was "conscious of a duty" could there be customary international law); BROWNLIE, *supra* note 136, at 7–8 (describing *opinio juris* as a necessary element of international custom).

[158] *See* CORN ET AL., *supra* note 126, ch. 4, at 4.

[159] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Nov. 29–Dec. 11, 1868, 18 Martens Nouveau Recueil (ser. 1) 474, *translated and reprinted in* THE LAWS OF ARMED CONFLICTS 101, 102 (Dietrich Schindler & Jiri Toman eds., 3d rev. ed. 1988).

[160] U.S. DEP'T OF THE AIR FORCE, AIR FORCE PAMPHLET, AFP 110-31, at 1-5 to 1-6 (1976).

[161] *See* T.E. HOLLAND, THE LAWS OF WAR ON LAND 12 (1908) (stating that only actions indispensable for securing the submission of the enemy are permitting under

The principle of humanity places a prohibition upon undertakings that might otherwise be justified under only the principle of military necessity.[162]

These two cardinal principles provide the foundation from which all LOAC rules are drawn. The principles are somewhat abstract in nature, however, and require additional principles to more effectively "implement" the twin goals of military necessity and humanity.[163] The primary implementation principles for military necessity are the principles of distinction and proportionality.[164] Similar to, but conceptually different from, the principle of distinction, is the implementing principle of "discrimination."[165] These principles are described more fully in Part II.C.1–3 below. The implementation principles for "humanity" are the principles of "humane treatment and the prohibition against the infliction of unnecessary suffering."[166]

This Note focuses on the principles of distinction, discrimination, and proportionality.[167] A fact-sensitive inquiry is required to determine whether Stuxnet violated these principles and whether Stuxnet was properly regulated. While humane treatment and the prohibition on unnecessary suffering are obviously relevant to cyber law—it is possible that a cyber attack

the principle of military necessity); CORN ET AL., *supra* note 126, ch. 4, at 8 ("Military necessity supplies the authority to employ the means necessary to bring an enemy to submission.").

[162] *See* A.P.V. ROGERS, LAW ON THE BATTLEFIELD 7 (2d ed. 2004) ("Humanity is, therefore, a guiding principle that puts a brake on undertakings which might otherwise be justified by the principle of military necessity."); CORN ET AL., *supra* note 126, ch. 4, at 9 ("[A]uthority derived from the contemporary principle of military necessity is not absolute, but is instead qualified by humanitarian obligations.").

[163] *See* KOLB & HYDE, *supra* note 110, at 46–47 (noting that beneath the principles of military necessity and humanity are "a series of more concrete and operational principles"); CORN ET AL., *supra* note 126, ch. 4, at 11 (describing the necessity of these "implementing principles").

[164] *See* CORN ET AL., *supra* note 126, ch. 4, at 4 ("Complementing the principle of military necessity are the principles of military objective and proportionality.").

[165] *See infra* Part II.C.2 (describing the principle of discrimination).

[166] CORN ET AL., *supra* note 126, ch. 4, at 4.

[167] For a similar analysis of the targetability of the Natanz facility under the principle of distinction, see generally Brian L. Bengs, *Legal Constraints upon the Use of a Tactical Nuclear Weapon Against the Natanz Nuclear Facility in Iran*, 40 GEO. WASH. INT'L L. REV. 323 (2008).

could cause physical harm to humans—Stuxnet injured no one and therefore does not violate either principle.[168]

Part III of this Note hypothetically applies these principles to Israel and the United States, so it is also necessary to briefly discuss how the rules apply to those countries. As the following Sections explain, all three principles constitute "customary international law" that are also codified in AP I.[169] Although neither Israel nor the United States has ratified AP I, distinction, discrimination, and proportionality are widely recognized as principles of customary law with AP I merely "restating" the rule.[170] The principles are therefore applicable to all states, even those that never properly ratified the Geneva Convention. Thus, Israel and the United States are legally bound to follow these principles.

1. Distinction

The basic premise of distinction is described in Article 48 of AP I, which states: "Parties to [a] 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."[171] Distinction therefore has two primary elements: (1) combatants must distinguish military individuals, items, and objectives from civilians and civilian property, and (2) once this distinction has been made, commanders must direct their operations only

[168] *See supra* Part I.D–E (describing the effects of Stuxnet and highlighting the lack of physical injury).

[169] *See infra* Part II.C.1–3.

[170] *See* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, Remarks at the Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions, *in* 2 AM. U. J. INT'L L. & POL'Y 419, 422–29 (1987) (explaining the articles of AP I that the United States considers customary law and therefore is bound to follow); Matthew D. Thurlow, Note, *Protecting Cultural Property in Iraq: How American Military Policy Comports with International Law*, 8 YALE HUM. RTS. & DEV. L.J. 153, 155 (2005) (noting that the United States is bound by customary law and that AP I codifies customary law); *supra* note 144 and accompanying text (indicating that Israel and the United States are not parties to AP I).

[171] AP I, *supra* note 117, art. 48.

against combatants and military objectives.[172] The rule therefore provides a workable means for commanders to implement the principle of necessity.[173]

Distinction can be further broken down into two parallel but distinct aspects: first, distinguishing between civilians and combatants, and second, distinguishing between military objects and civilian property. The first aspect of distinction is inapplicable to Stuxnet because no persons were targeted by the attack.[174] The second aspect of distinction applies to Stuxnet because the worm targeted physical objects.[175] This Section therefore addresses only the second aspect of distinction.

While Article 48 of AP I states the basic rule of distinction, Articles 49 through 56 articulate more specific rules used in its application.[176] The prohibition against attacking civilian objects is described in Article 52(1) of AP I: "[C]ivilian objects shall not be the object of attack or reprisals."[177] It further defines "civilian objects" as "all objects which are not military objectives."[178] One must therefore determine whether an object is a "military objective" to determine if it is a valid target.

The test for whether an object or facility is a targetable "military objective" is (1) whether the object makes an effective military contribution, and (2) whether targeting that object results in a definite military advantage.[179] These elements are

[172] *See* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 98 (2010) ("'Distinction' . . . requires that combatants be distinguished from noncombatants and that military objectives be distinguished from protected property or protected places."); *see also* ROGERS, *supra* note 162, at 7 ("[W]ar is to be waged against the enemy's armed forces, not against its civilian population. Attacks are to be directed at military targets, not at civilian objects.")

[173] *See* ROGERS, *supra* note 162, at 7 (noting that the principle of distinction follows from the principle of necessity); *see also* KOLB & HYDE, *supra* note 110, at 125 ("Underlying [the rule of distinction] is the principle that, even in an armed conflict, the only legitimate military action is that which is aimed at weakening the military potential of the enemy.").

[174] *See supra* Part I.D–E (noting that Stuxnet harmed only property).

[175] *See supra* Part I.D–E (describing the impact of Stuxnet on the Iranian nuclear program and on computers worldwide).

[176] *See* AP I, *supra* note 117, arts. 49–56.

[177] *Id.* art. 52(1).

[178] *Id.*

[179] *Id.* art. 52(2); *see* KOLB & HYDE, *supra* note 110, at 125 (bifurcating the "military objective" analysis into whether the target makes an effective military contribution and whether the planned attack results in a military advantage).

determined by considering the object's "nature, location, purpose or use." [180] The AP I commentary explains that "potential or indeterminate advantages" do not meet the standard for a "definite" military advantage.[181] If the object does make an effective military contribution, usually discernable from the object's purpose, and destroying or disabling that object results in a definite military advantage, then the object is targetable under the principle of distinction.[182] If the object does not meet these criteria, then Article 52(3) creates a presumption that the object is civilian property and not a valid target.[183]

The fact that an installation is not technically considered part of the military does not mean that it cannot lawfully be targeted; if the target makes a military contribution and its destruction would result in a definite military advantage, then the facility is legally targetable despite its official designation as a nonmilitary structure.[184] For example, munitions plants always have been an acceptable target under the principle of distinction regardless of whether they were controlled by the military or by civilians.[185] Facilities with dual purposes, such as power plants that service both civilian and military installations, also may be an acceptable target under the principle of distinction.[186]

The amorphousness of the test for what constitutes a valid "military objective" renders few examples of targets that will be

[180] AP I, *supra* note 117, art. 52(2).

[181] CLAUDE PILLOUD ET AL., INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 636 (Yves Sandoz et al. eds., 1987) [hereinafter AP I COMMENTARY].

[182] AP I, *supra* note 117, art. 52.

[183] *Id.* art. 52(3) (stating that in cases of doubt, commanders should presume that the target is civilian property).

[184] *See id.* art. 52 (lacking any language indicating that an object's "official" status as nonmilitary has any bearing on the distinction analysis).

[185] *See, e.g.*, ROGERS, *supra* note 162, at 18 (explaining that a munitions factory is so important that the death of most civilians working there is not disproportionate); Kenneth B. Brown, *Counter-Guerilla Operations: Does the Law of War Proscribe Success?*, 44 NAVAL L. REV. 123, 155 n.140 (1997) (noting that even if civilians were killed in an attack on a munitions plant it would not necessarily violate the LOAC).

[186] *See, e.g.*, 1 RICHARD T. REYNOLDS, HEART OF THE STORM: THE GENESIS OF THE AIR CAMPAIGN AGAINST IRAQ 54 (1995) (stating that power plants were frequently targeted by the US military during the Gulf War).

valid in all situations.[187] Commentators have noted that the increased reliance of militaries upon a state's industrial facilities has made the distinction between civilian and military objects less well-defined and, perhaps, less important.[188] Even during the height of World War II, military leaders still espoused the principle of distinction as important; in 1938, British Prime Minister Neville Chamberlain stated to the House of Commons that "targets which are aimed at from the air must be legitimate military objectives and must be capable of identification."[189] The view that distinction is no longer valid law also fundamentally confuses the existence of the principle with its efficacy; just as individuals break criminal laws, nations can violate established LOAC principles without destroying the rule itself.[190] Despite the alleged decline in importance of the rule of distinction, the principle remains a fundamental part of the LOAC.

For a commander to be in compliance with the principle of distinction and Article 48 of AP I, he does not need to be "correct" in his decision about the site's targetability; he need only take "reasonable precautions" in reaching his decision that the target is legal.[191] He also must do "everything feasible" to verify that the target is not a civilian object and he must take "all feasible precautions" in choosing the means and methods of attack in order to minimize or avoid damage to civilian

[187] KOLB & HYDE, *supra* note 110, at 130 ("The modern LOAC has abandoned any attempt to provide a list of [objects that are military objectives], even a non-exhaustive, illustrative one."); AP I COMMENTARY, *supra* note 181, at 1997–99 (noting that lawmakers' attempts to create a list of targets that constitute "military objectives" were unsuccessful).

[188] Mika Nishimura Hayashi, *The Principle of Civilian Protection and Contemporary Armed Conflict*, *in* THE LAW OF ARMED CONFLICT: CONSTRAINTS ON THE CONTEMPORARY USE OF MILITARY FORCE 105, 109 (Howard M. Hensel ed., 2005) ("According to this view, practice in the two World Wars altered the legal status of the principle of distinction from a time-honored principle of the [LOAC] to a legally meaningless expression."); ROGERS, *supra* note 162, at 13 (citing the practice during World War II of bombing civilian centers of population).

[189] 337 PARL. DEB., H.C. (5th ser.) (1938) 937 (U.K.).

[190] *See* SHAW, *supra* note 111, at 6 ("[J]ust as incidents of murder, robbery and rape do occur within national legal orders without destroying the system as such, so analogously assaults upon international legal rules point up the weaknesses of the system without denigrating their validity or their necessity."); Hayashi, *supra* note 188, at 112 (noting the "vigorous defense" of the principle of distinction following World War II).

[191] AP I, *supra* note 117, art. 57(4).

objects.[192] "Feasibility" takes into consideration the circumstances in which the commander is making the determination.[193]

2. Discrimination

Discrimination is a principle related to, but conceptually different from, distinction. Article 51(4) of AP I outlines the principle of discrimination: states must not only distinguish between targets that are civilian and those that are legitimate military objectives, but must also use weapons that are capable of being "directed at a specific military objective."[194] Thus, if a weapon were to be faithfully aimed at an appropriate target, but physically was incapable of controlling the force released to a designated physical area, the weapon would violate the principle of discrimination.[195] Examples of weapons that might violate the principle are "long-range missile[s] with no, or only a rudimentary, guidance system . . . [or] biological weapons that spread contagious diseases."[196]

If a commander reasonably anticipates that the weapon will be able to properly "discriminate," then they are in compliance with the rule. A hypothetical example is a weapon that is typically able to focus on a target, but malfunctions and causes damage to surrounding areas; a commander would not violate the principle of discrimination if he had taken "reasonable precautions" to ensure that the weapon was capable of discriminating, even though in this instance it did not.[197] The "feasibility" standard described in the preceding Section applies to the amount of information a commander must gather before

[192] *Id.* art. 57(2).

[193] *See* Jensen, *supra* note 22, at 1184 (stating that rules will be applied to situations as they appeared to commanders at the time of the decision).

[194] AP I, *supra* note 117, art. 51(4).

[195] *See* DETTER, *supra* note 125, at 235 (noting that nuclear weapons may violate the principle of discrimination because they are, by nature, incapable of confining their destructive forces); KOLB & HYDE, *supra* note 110, at 136 ("[I]t is prohibited to use weapons that cannot be specifically targeted at military objectives because their action is inherently indiscriminate.").

[196] Schmitt, *supra* note 122, at 147.

[197] AP I, *supra* note 117, art. 57(4).

he may make his determination on the legality of the strike under the principle of discrimination, as well.[198]

Also relevant to an application of discrimination to cyber weapons is the possible existence of knock-on effects. Knock-on effects are consequences from an attack that a commander did not intend or plan to occur.[199] They happen because of the existence of an "unexpected agent or circumstance."[200] Whether knock-on effects cause an attack to be unlawful does not depend upon the damage actually done by the weapon; instead, it turns on whether the commander has "taken sufficient precautions . . . [to ensure] that his attack does not go beyond its intended target."[201]

Professor Michael Schmitt has argued that if a virus or worm has "no way to limit its subsequent retransmission" then it is prohibited as an indiscriminate weapon.[202] An important question is how certain a commander must be that knock-on effects will not render his "weapon" indiscriminate before he can lawfully deploy the weapon.[203] Article 51 states that the standard is what is "expected."[204] This would appear to give military commanders broad discretion in determining whether knock-on effects render an attack unlawful.[205] Furthermore, the commentary states that commander's expectations will be valid if they were made in "common sense and good faith."[206] With respect to CNAs, commanders have stated that it is US policy to determine whether the malware does "exactly" what it is intended to do without any "unintended consequences."[207]

[198] *See* AP I, *supra* note 117, art. 57(2); *see also supra* notes 192–93 and accompanying text (describing the feasibility standard and its application to distinction).

[199] *See* Jensen, *supra* note 22, at 1149 (defining knock-on effects).

[200] *Id.* at 1177.

[201] *Id.* at 1178.

[202] Schmitt, *supra* note 21, at 389.

[203] *See* Jensen, *supra* note 22, at 1179–86 (examining various possible standards of certainty for commanders in these analyses); *see also* AP I, *supra* note 117, art. 51(5)(b).

[204] AP I, *supra* note 117, art. 51(5)(b).

[205] AP I COMMENTARY, *supra* note 181, at 2209–10 (stating that the standard gives a "fairly broad margin of judgment" to commanders).

[206] *Id.* at 2208.

[207] Jensen, *supra* note 22, at 1149 n.12.

3. Proportionality

Commentators recognize that the principle of distinction is inadequate protection for civilians and civilian property in an armed conflict.[208] Without another rule, one could justify massive damage to civilians and civilian property simply by selecting an otherwise valid military target.[209] Proportionality, in conjunction with distinction, is the LOAC principle designed to protect civilians and civilian objects from harm through unnecessary "collateral damage."[210] While distinction attempts to prevent the targeting of civilians or civilian objects and discrimination attempts to prevent the use of weapons that cannot successfully focus on military targets, proportionality regulates attacks in which damage to civilian property is a foreseeable result of an attack on a valid military objective.[211] Proportionality, therefore, sets a limit on what amount of collateral destruction of civilian property, or death and injury to civilians, is allowable when attacking an otherwise-permissible military target.[212] Article 57(2) of AP I mandates that the

[208] *See* ROGERS, *supra* note 162, at 7 (stating that additional principles put a "brake" on attacks that would otherwise be permissible under the principle of military necessity); CORN ET AL., *supra* note 126, ch. 4, at 8 (noting that further regulations complement the principle of military necessity).

[209] *See* CORN ET AL., *supra* note 126, ch. 4, at 15 ("Determining that a person, place, or thing qualifies as a lawful object of attack does not however categorically establish the legality of attack."); *see also supra* note 162 and accompanying text (noting that implementing rules for the principle of humanity put further restrictions on military attacks).

[210] Amnon Rubinstein, *Human Shields in Modern Armed Conflicts: The Need for a Proportionate Proportionality*, 22 STAN. L. & POL'Y REV. 93, 100 (2011) ("[T]he principle of proportionality entails a duty on the military commander to assess the attack's collateral damage . . . ."); CORN ET AL., *supra* note 126, ch. 4, at 15 (explaining that proportionality requires commanders to consider the "collateral damage" of their attacks).

[211] *See* Jensen, *supra* note 22, at 1170–71 ("Even if the target is legitimate, the attacker is required to adjust his means and methods of attack so that the destruction or death of the target does not include or cause a chain of events that will lead to the death of civilians or destruction of civilian property that is excessive to the concrete and direct military advantage to be gained."); Schmitt, *supra* note 122, at 150 ("[P]roportionality operates in scenarios in which incidental injury and collateral damage are the foreseeable, albeit undesired, result of attack on a legitimate target.").

[212] *See* AP I, *supra* note 117, art. 57(2)(b) ("An attack shall be cancelled or suspended if it . . . 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."); Rebecca J. Barber, *The Proportionality Equation: Balancing Military Objectives with Civilian*

anticipated loss of life and damage to property incidental to attacks must not be "excessive" in relation to the concrete and direct military advantage expected to be gained.[213] Article 51(5) also states that an attack will violate the LOAC if the collateral damage is "excessive" when compared to the advantage gained. [214] Since combatants and military objectives are legitimate targets, loss of combatant's lives or damage to military objectives is not considered in the "proportionality equation."[215] Commanders are not required to have calculated this proportionality equation correctly ex post facto; the analysis is applied with the information available at the time of the attack.[216] The circumstances of the decision, such as the amount of time a commander has to make the decision and the amount of information reasonably obtainable, are considered.[217]

To weigh the military advantage gained against the loss of civilian life and property, one must first define what constitutes a military advantage. To confer any military advantage, the target must first have been deemed a valid "military objective" under

Lives in the Armed Conflict in Afghanistan, 15 J. CONFLICT & SEC. L. 476, 479 (2010) ("[I]n assessing proportionality, military commanders must attempt to weigh the expected loss of civilian life and/or damage to civilian property against the anticipated military advantage.").

[213] *See* AP I, *supra* note 117, art. 57(2) (stating that an attack shall be cancelled if it becomes apparent the collateral damage would be "excessive" when compared with the military advantage gained); JUDITH GARDAM, NECESSITY, PROPORTIONALITY AND THE USE OF FORCE BY STATES 98 (2004) (noting that proportionality is designed to ensure incidental civilian damage is not "excessive").

[214] AP I, *supra* note 117, art. 51(5)(b). Note that Article 51 places this balancing test under the rubric of "discrimination," conflating two conceptually different principles. *See* GARDAM, *supra* note 213, at 94 ("The designation of proportionality as a species of indiscriminate attack confuses the idea of proportionality with the requirement to distinguish between civilian and military targets.").

[215] *See* GARDAM, *supra* note 213, at 14 (explaining that harm to combatants is considered under the principles of superfluous injury or unnecessary suffering and not proportionality); Jensen, *supra* note 22, at 1171 ("[T]he rule of proportionality only applies to civilians and civilian property. It is not an attempt to ensure a 'fair fight' between combatants." (internal citations omitted)).

[216] *See* Barber, *supra* note 212, at 477 ("[I]t is important to note that commanders are not to be judged on the basis of an *ex post facto* assessment."); Jensen, *supra* note 22, at 1183 (noting that courts examine a commander's decisions as the situation appeared to the commander at the time).

[217] *See supra* note 198 and accompanying text (describing how the feasibility standard takes into consideration all the circumstances at the time of the decision).

the principle of distinction.[218] Once the object is deemed a valid target, the most important factor considered is the effect destroying or incapacitating the target will have on accomplishing a military objective; the more essential the target is to accomplishing an objective, the more damage to civilian property will be tolerated.[219] "Military advantage" is further defined in the AP I Commentary as consisting of "ground gained and in annihilating or weakening the enemy armed forces."[220] The military advantage must also be "concrete and direct."[221]

Next, the amount of collateral damage the attack is expected to cause must be determined.[222] Although AP I does not provide a list of factors that should be considered, there are some basic considerations that are likely applicable in most calculations.[223] The proximity of the target to civilians and civilian property, the density of the civilian population in the area, the timing of the attack, the possibility of the release of hazardous substances, and the ability of the weapon to target a specific physical area should be considered.[224] More fundamentally, human lives carry greater weight than physical property in the calculation.[225]

The calculation commanders must make is a difficult one. How is one to weigh the value of accomplishing a military

[218] *See* GARDAM, *supra* note 213, at 100 (arguing that the distinction analysis should occur prior to a proportionality analysis); *see also* Jensen, *supra* note 22, at 1170 (noting that the proportionality analysis occurs "[o]nce a commander has determined that a target is a military objective").

[219] GARDAM, *supra* note 213, at 100 ("The more integral the proposed target is to the military strategy, the higher the level of likely civilian casualties and damage to civilian objects that will be acceptable."); ROGERS, *supra* note 162, at 21–22 ("Clearly, the more important the military objective, the greater the incidental losses before it could be said that the rule of proportionality had been violated.").

[220] AP I COMMENTARY, *supra* note 181, at 2218.

[221] AP I, *supra* note 117, art. 57(2)(a)(iii).

[222] *See supra* notes 212–17 and accompanying text (describing the two-part test).

[223] *See generally* AP I, *supra* note 117 (failing to list any specific factors).

[224] *See* GARDAM, *supra* note 217, at 103 (listing considerations for the civilian damage side of the proportionality equation); ROGERS, *supra* note 162, at 23 (noting factors that should be considered during proportionality analysis).

[225] *See generally* Barber, *supra* note 212 (noting that human lives are considered more valuable than physical property).

objective against the value of human life and property?[226] Despite this difficulty, there is likely a consensus at the ends of the "proportionality continuum."[227] For example, it is likely that all governments would agree that a single injury to a civilian would not be excessive compared to capturing a high-ranking military commander, while neutralizing a single infantryman would not justify the deaths of thousands of civilians.[228] The more difficult analysis, however, is in the middle of the continuum.[229]

The existence of knock-on effects, discussed previously in Part II.C.2, is also relevant to a proportionality analysis.[230] The legality of an attack under the principle of proportionality will turn on whether the commander has taken sufficient "precautions" to ensure that proportionality is not violated."[231] Commanders are once again subject to Article 57(2)(b) of AP I, which applies an "expected" results test, as previously described under the principle of discrimination.[232] The analysis for a CNA is greatly complicated by the possible presence of knock-on effects; the collateral damage to civilians will be clear in a kinetic attack but not in a CNA.[233]

The principles of distinction, discrimination, and proportionality regulate combatants' actions during an armed conflict. They exist to further the LOAC goals of reducing overall destruction in warfare, and reducing unnecessary harm to civilians and civilian property. The principles apply to CNAs, although not explicitly stated anywhere in the LOAC.[234]

[226] *See* KOLB & HYDE, *supra* note 110, at 48 (stating that the military advantage gained and civilian losses must be put into "some form of balance," but not specifying what form); Barber, *supra* note 212, at 476 ("[T]he considerations being weighed on each side—the value of human lives on the one hand, the value of a military objective on the other—are in many respects simply not amenable to comparison.").

[227] *See* Schmitt, *supra* note 122, at 170.

[228] *Id.*

[229] *See id.* at 170 ("The complexity emerges when one moves from these extremes along the proportionality continuum toward the center.")

[230] *See supra* notes 199–201 and accompanying text (describing knock-on effects).

[231] AP I, *supra* note 117, art. 57.

[232] *Id.* art. 57(2)(b).

[233] *See* Jensen, *supra* note 22, at 1178 ("[W]hen using kinetic weapons, determining, at least in the short term, what injury and damage will occur can be much clearer. This may not be so clear in relation to CNA.").

[234] *See supra* note 21 and accompanying text.

III. *APPLICATION OF THE LOAC TO STUXNET*

The facts described in Part I.B–E support the conclusion that Stuxnet was developed by Israel and the United States to target Iran's Natanz nuclear facility. The high value of Stuxnet's zero-day hacks, the discriminating nature of Stuxnet's payload, the substantial budget required to create Stuxnet, and the suspicious reactions of Israeli and US officials demonstrate that they both likely played a role in Stuxnet's development and deployment.[235] This Note assumes that to be true. All other facts about Stuxnet, such as how the worm worked and the damage that it did to the nuclear installations, are analyzed based entirely on available evidence.

Part III applies the principles of distinction, discrimination, and proportionality to the facts of Stuxnet. It argues that, with one exception, application of the LOAC to Stuxnet accomplishes the LOAC goals and that Stuxnet therefore represents one piece of evidence that current LOAC paradigms adequately regulate cyber war. Section A of this Part applies the principle of distinction to Stuxnet. Section B applies the principle of discrimination. Section C applies the principle of proportionality.

This Note concludes that, as applied to Stuxnet, the US position that the LOAC adequately regulates cyber war is fundamentally correct: existing LOAC rules adequately address the issues Stuxnet raises. This is demonstrated in two ways. First, the fundamental policy goals behind the rules of the LOAC are furthered when applied to Stuxnet. Second, the LOAC has already accomplished some of these goals, namely that the programmers of Stuxnet appear to have specifically designed the worm to conform to the rules of the LOAC.

A. *Distinction Applied to Stuxnet*

The application of distinction to Stuxnet must come first because a determination that Natanz was not a valid military objective would render Stuxnet illegal, regardless of the worm's adherence to the principles of discrimination and

[235] *See supra* Part I.B–E.

proportionality.[236] It seems likely that the Natanz nuclear facility constitutes an appropriate military target under the principle of distinction. There are two possible purposes for the uranium enrichment at Natanz. First, Iran could enrich uranium as part of the creation of a nuclear weapon.[237] The enriched uranium it produces is a necessary component of nuclear weapons.[238] This would render Natanz a military target.[239]

Alternatively, the centrifuges could be enriching uranium to fuel Iranian nuclear power plants, which would also render Natanz an acceptable military target.[240] A power plant has the potential to power military structures. The power plant's "purpose"—providing electricity to military operations—certainly makes an effective "military contribution," considering the power plant's nature and function.[241] Disrupting power generation would likely result in a definite military advantage: military installations that would otherwise be operational would be incapacitated.[242] A nuclear power plant therefore would be a valid military objective under Article 51(2). Logically, a facility that provides essential component parts to power plants—here, the enriched uranium—also would be a valid military objective. Therefore, a commander would be "reasonable" in determining that it was a permissible military target.[243]

In simply "choosing" a target, there is no fundamental difference in distinction analysis between an attack on Natanz by traditional weapons or by Stuxnet. If, however, Stuxnet

[236] *See supra* note 218 and accompanying text (noting that the determination of an object or individual as a valid military objective is the first step of any LOAC analysis).

[237] *See supra* note 83 and accompanying text (explaining that there are some who believe Iran's is enriching uranium to acquire a nuclear weapon).

[238] *See supra* note 81 and accompanying text (stating that enriched uranium is required for the development of a nuclear weapon).

[239] *See supra* note 185 and accompanying text (explaining that munitions plants are traditionally valid military objectives under the principle of distinction).

[240] *See supra* note 82 and accompanying text (noting that Iran claims its nuclear program is only for the purposes of generating nuclear power).

[241] *See supra* notes 184–86 and accompanying text (stating that power plants have historically been valid targets under distinction and that analysis of whether an object is a valid military objective considers that object's purpose).

[242] *See supra* note 186 and accompanying text (explaining that power plants have been considered valid military objectives in the past).

[243] *See supra* notes 197–98 and accompanying text (describing the standard commanders will be held to when performing a distinction analysis).

intentionally infected civilian computers as a "stepping-stone" to infecting Natanz, those initial infections may have violated the principle of distinction. This would be true even if the civilian computers suffered no harm, so long as they were explicitly "targeted" by Stuxnet. Whether Stuxnet "targeted" these computers is therefore a crucial factor in determining whether Stuxnet violated the principle. In either scenario, however, the application of the principle to Stuxnet both lowers the level of overall destruction by requiring that the commander target only military objectives, such the Natanz facility, and also decreases the harm to civilians by requiring that the commander direct his attack at Natanz. Stuxnet is therefore properly regulated under the principle of distinction.

B. *Discrimination Applied to Stuxnet*

While Stuxnet's attack on Natanz largely conforms to the principle of distinction, application of the principle of discrimination is substantially more difficult. The primary issue for Stuxnet is whether it is capable of discriminating between its target and things that "surround" it.[244] With a traditional weapon, this manifests itself in "collateral damage" to the physical area surrounding the target.[245] With Stuxnet, it manifests itself in potential damage to connected computers or computer networks.[246] Professor Michael Schmitt, an authority on the law of cyber war, has argued that if a virus or worm cannot limit its transmission, then it may be prohibited as indiscriminate.[247] It seems, however, that there were some controls put onto Stuxnet in an effort to limit subsequent infections and direct its destructive effects solely at its intended target.[248]

[244] *See supra* notes 194–96 and accompanying text (noting that weapons that are incapable of confining their force to military objectives may violate the principle of discrimination).

[245] *See supra* note 196 and accompanying text (stating that a missile fired without a guidance system would likely violate the principle of discrimination).

[246] *See supra* notes 98–102 (describing the effect of Stuxnet on computers outside of Natanz).

[247] *See supra* note 202 and accompanying text (describing Professor Michael Schmitt's theory on indiscriminate malware transmission).

[248] *See supra* notes 74–76 and accompanying text (describing the instructions Stuxnet's creators put into its code to limit subsequent infections).

While Stuxnet closely controls the deployment of its payload, Stuxnet is fundamentally indiscriminate in that it does not distinguish among computers when spreading; it infects all of the computers using the Windows operating system that it can.[249] As stated previously, there have been over 100,000 estimated infections worldwide.[250] Stuxnet's programmers, however, designed the worm to only inflict damage upon the Iranian nuclear facilities.[251] By creating a series of conditions that had to be fulfilled before Stuxnet's payload would be delivered, the programmers essentially put a safety lid on an otherwise extremely dangerous weapon.[252] As a result, despite the 100,000 infections, it appears that Stuxnet's payload has never been deployed outside of the Iranian nuclear facilities.[253] Siemens, the company whose software and hardware Stuxnet targeted, has identified only twenty-four cases of infections at industrial plants worldwide.[254] In each case, Stuxnet's payload was not delivered and the company was able to detect the worm and remove it without harm to their computer system.[255] Thus, in reality Stuxnet's payload was deployed discriminately.

The damage actually done by Stuxnet is not what must be considered when analyzing the principle of discrimination.[256] What is relevant are the results commanders "expected" at the time of deployment, and whether the commander in charge had done "everything feasible" to gather information prior to that deployment.[257] Since there is no information available on the

[249] *See supra* note 28 and accompanying text (describing Stuxnet's indiscriminate nature).

[250] *See supra* note 99 and accompanying text (describing a Symantec study tracking the number of Stuxnet infections).

[251] *See supra* notes 74–76 and accompanying text (describing various limitations hindering Stuxnet's proliferation).

[252] *See supra* notes 29–38 (describing the narrow circumstances in which Stuxnet's payload will be deployed).

[253] *See supra* note 101 and accompanying text (stating that there has not been a recorded deployment of Stuxnet's payload outside of Natanz).

[254] *See supra* note 100 and accompanying text (stating that a Siemens report identified twenty-four industrial infections).

[255] *See supra* note 102 and accompanying text (noting the successful removal of Stuxnet from industrial hardware).

[256] *See supra* notes 191–93 and accompanying text (explaining the standard to which commanders are held).

[257] *See supra* notes 191–93 and accompanying text (describing the "expected results" and "everything feasible" standards of AP I).

process by which the American or Israeli commanders investigated the potential effects of Stuxnet's payload, it is difficult to draw a firm conclusion about Stuxnet's expected impact.[258] Stuxnet's code and its actual effects, however, can help us surmise what a commander would have known.[259]

Stuxnet's payload was unlikely to cause destruction outside of the Iranian nuclear facilities—or at least outside of the few facilities in the world that met the specific criteria required to activate Stuxnet's payload.[260] Stuxnet's designers put a great amount of effort into ensuring only Natanz's centrifuges would be struck by its payload.[261] To develop such a highly specialized cyber weapon, the commanders must have done substantial investigation into whether Stuxnet's payload was likely to be deployed on non-Natanz PLCs.[262] This means that the commander in charge likely satisfied the "everything feasible" investigation requirement, and acted in "good faith" when making the judgment that they "expected" Stuxnet to successfully discriminate.[263]

It is also stated US policy to require commanders to fully investigate possible unintended consequences of malware.[264] As such, it seems likely that at the time of deployment, a commander would have satisfied the requirement that he does everything feasible to determine the discriminatory nature of Stuxnet.[265] After satisfying that requirement, it appears that the commander would have been reasonable in expecting Stuxnet

[258] *See supra* note 10 and accompanying text (stating that Stuxnet's origins are currently unknown).

[259] *See supra* Part I.B–E (describing Stuxnet's code and its effects).

[260] *See supra* notes 29–38 and accompanying text (noting that by programming Stuxnet's payload to be delivered in such narrow circumstances, Stuxnet's programmers rendered delivery of the payload outside of Natanz highly unlikely).

[261] *See supra* note 74–77 and accompanying text (noting the attention paid by Stuxnet's programmers to ensuring Stuxnet's payload was not discharged outside of Natanz).

[262] *See supra* note 201 and accompanying text (noting that US commanders are required to perform substantial investigations into knock-on effects).

[263] *See supra* notes 197–98 and accompanying text (describing the standard to which commanders are held).

[264] *See supra* note 207 and accompanying text (stating that US commanders are required to make sure malware does "exactly" what it is supposed to).

[265] *See supra* note 191–93 and accompanying text (describing the feasibility standard).

to discriminate effectively between lawful military targets and prohibited ones, at least with regards to its payload.[266]

Another issue is whether Stuxnet could be considered indiscriminate despite never deploying its payload outside of Natanz.[267] Despite more than 100,000 infections, Stuxnet should not be considered indiscriminate under the LOAC.[268] The extent of the damage that the civilian computers suffered is unknown, but thought to be extremely minor.[269] Although civilians have struggled to completely rid their computers of Stuxnet, as have technicians at Natanz, the worm does not replicate indefinitely when it infects a computer.[270] It therefore is incapable of "clogging" up a system as some worms can.[271] A few lines of code sitting "inert" in a computer system are unlikely to cause any damage to a computer system.[272]

Application of the principle of discrimination to Stuxnet demonstrates that Stuxnet successfully furthered LOAC policy goals.[273] Although extremely effective, Stuxnet almost certainly would have had a better chance of destroying the centrifuges at Natanz if it had not been so discriminating. There was almost certainly a risk that the centrifuges that Stuxnet's designers wished to destroy might not fall within the specific parameters Stuxnet required to deliver its payload.[274] If destroying the centrifuges was the only factor that Stuxnet's designers considered, increasing the range of parameters necessary to

[266] *See supra* note 197 and accompanying text (describing the reasonableness standard).

[267] *See supra* note 101 and accompanying text (explaining that Stuxnet's payload has not been delivered outside of Natanz).

[268] *See supra* note 99 and accompanying text (explaining that Stuxnet has infected more than 100,000 computers)

[269] *See supra* Part I.D (describing Stuxnet's negligible damage to civilian computers).

[270] *See supra* notes 74–75 and accompanying text (noting the limitations Stuxnet's code places on its ability to replicate).

[271] *See supra* note 26 and accompanying text (describing how a worm can harm computer networks despite the absence of a malicious payload).

[272] *See supra* note 33 and accompanying text (describing Stuxnet as an "inert feature" on the network when the parameters necessary to trigger its payload are not present).

[273] *See supra* notes 122–24 and accompanying text (describing the two primary LOAC policy objectives).

[274] *See supra* notes 29–38 and accompanying text (describing the "narrow" parameters in which Stuxnet's payload would be deployed).

deliver Stuxnet's payload would have been an easy way to accomplish that objective.[275] The designers, however, did not do that. They gave up some operational effectiveness in return for assuring that PLCs other than those controlling the centrifuges would not be affected.[276] This demonstrates that not only would the principle of discrimination theoretically further LOAC policy objectives, it likely *already has* furthered those objectives.[277] The designers of Stuxnet obeyed the LOAC rules, even though *jus in bello* did not apply, and the policy objectives of the LOAC were furthered. The application of the principle of discrimination to Stuxnet assured that civilian objects were not harmed and that the overall level of destruction caused by the worm was minimalized.

C. *Proportionality Applied to Stuxnet*

In one respect, those who designed and deployed Stuxnet acted in strict conformity with the principle of proportionality; human lives are considered more valuable than physical property and Stuxnet avoided any civilian casualties.[278] If the options being considered by Israel and the United States to delay the Iranian nuclear program were: (1) bomb the facility, or (2) use the Stuxnet worm, then Stuxnet was almost certainly less likely to violate the principle of proportionality than a kinetic attack.[279]

Stuxnet enabled the commander in charge to target and destroy the uranium centrifuges with no loss of life and comparatively little damage to civilian objects.[280] In comparison, Israel's 2007 strike on Syria, which also targeted a nuclear facility buried underground, resulted in the physical destruction of the

[275] *See supra* notes 74–77 and accompanying text (suggesting that Stuxnet's designers considered factors other than its operational effectiveness).

[276] *See supra* note 100 and accompanying text (noting that Stuxnet's payload has not been deployed outside of Natanz).

[277] *See supra* notes 122–24 and accompanying text (describing the LOAC policy goals).

[278] *See supra* note 225 and accompanying text (explaining that civilian lives are given greater weight in the proportionality analysis than civilian property).

[279] *See supra* notes 93–94 and accompanying text (describing the massive property damage that occurred when Israel struck a Syrian nuclear facility).

[280] *See supra* notes 101–02 and accompanying text (noting that Stuxnet caused minimal damage to civilian property).

entire site.[281] While wholesale destruction previously may have been the only way to accomplish a valid military objective, now a commander may be able to simply "turn off" an enemy facility. Stuxnet seems to follow this logic, although the centrifuges were not simply "turned off" and instead were destroyed in a manner similar to a traditional kinetic attack.[282]

In fact, without considering knock-on effects, it seems extremely unlikely that Stuxnet violated the principle of proportionality. The centrifuges and PLCs were both lawful military targets under the principle of distinction, so without the subsequent delivery of Stuxnet's payload to civilian computers, there would be almost no way for the principle to be violated, simply because there was no collateral damage.[283]

Civilian computers *were* infected subsequently, however, and it was certainly foreseeable, so one must consider whether the infections constitute a violation of the principle of proportionality.[284] To do so, one must first ask exactly what military advantage was gained by deploying Stuxnet.[285] As stated above, Stuxnet destroyed almost 1000 centrifuges.[286] The damage was extensive and multifaceted.[287] While Israel's government has previously said Iran was on the brink of acquiring nuclear weapons, the country's outgoing intelligence chief estimated recently that Iran could not obtain nuclear weapons before 2015.[288] If that is true, the military advantage gained is significant.

[281] *See supra* notes 93–94 and accompanying text (describing Israel's attack on a Syrian nuclear site).

[282] *See supra* notes 39–43 and accompanying text (describing how Stuxnet destroyed centrifuges at Natanz).

[283] *See supra* note 218 and accompanying text (explaining that determining that the target is a valid military objective is the first step of the analysis).

[284] *See supra* note 99 and accompanying text (noting more than 100,000 civilian computer infections).

[285] *See supra* note 218 and accompanying text (explaining that analyzing the military advantage gained by the attack is the first step of the proportionality test).

[286] *See supra* note 86 and accompanying text (stating that the Iranian government removed 984 centrifuges from Natanz).

[287] *See supra* notes 88–91 and accompanying text (explaining the numerous ways in which Stuxnet may have damaged the Iranian nuclear program).

[288] *See supra* note 92 and accompanying text (noting that Israeli officials now estimate that Iran will not acquire a nuclear weapon until 2015).

The second part of the test requires assessment of the collateral damage inflicted on civilians and civilian objects.[289] As stated above, the actual damage to civilian computers appears minimal: the payload was never delivered to civilian computers; the "inert" worm caused little to no damage to civilian computers; and the worm has a "self-destruct" deadline that is rapidly approaching. [290] The military advantage gained by deploying Stuxnet—setting back Iran's nuclear program several years—was significantly greater than the harm to civilian objects. API Article 57(2) requires that the damage to civilian objects be *excessive* when compared with the military advantage gained; Stuxnet was not excessive since essentially no damage was done to civilian computers and the military advantage was so great.[291] In fact, as far as its actual effects are considered, Stuxnet is at the end of the "proportionality continuum," in which a broad consensus would exist that it did not violate the principle.[292] It is not the actual effects of the worm, however, that must be analyzed; the relevant issues are what results commanders "expected" at the time of deployment.[293] Given the minimal amount of collateral damage caused by Stuxnet, Stuxnet's commanders were almost certainly reasonable in their calculations.[294] This is not conclusive, however: should further analysis reveal that a common circumstance exists where Stuxnet's payload deployment parameters are met, and it was simply fortunate that Stuxnet never encountered this circumstance, the commander's reasonability could be questioned.

Analysis of knock-on effects will also be similar to the analysis of the distinction principle in Part III.A. The test is

[289] *See supra* notes 222–25 and accompanying text (listing factors used during the evaluation of collateral damage in the proportionality equation).

[290] *See supra* notes 74, 100–02 and accompanying text (describing the self-destruct deadline, the absence of payload deployment, and the lack of damage done to civilian computers).

[291] *See supra* note 213 and accompanying text (noting the "excessive" requirement in the proportionality test).

[292] *See supra* notes 227–29 and accompanying text (describing the "proportionality continuum").

[293] *See supra* notes 192–93, 204 and accompanying text (explaining the "expected results" and "everything feasible" standards of AP I).

[294] *See supra* note 197 and accompanying text (describing the reasonableness standard).

whether a "reasonable" commander would have thought the attack conformed to the principle of proportionality, given that he took all "feasible" steps to obtain relevant information under the circumstances.[295] Again, while it is impossible to know what steps were taken, circumstantial evidence points strongly toward the conclusion that American and Israeli commanders took great care to limit any possible unintended consequences of the worm. Stuxnet's self-destruct instructions, limits on self-replication, and specific requirements for deployment of its payload all support the conclusion that it was objectively reasonable to believe that Stuxnet would pass the proportionality test.

The application of the proportionality principle to Stuxnet also furthers the policy goals of the LOAC.[296] Complying with the principle of proportionality required the developers of the worm to carefully program it so that any harm to civilian computers would not be excessive.[297] This lessened the impact of the attack on civilians. As noted in the analysis of discrimination in Part III.B, commanders could have ensured the destruction of the centrifuge by simply bombing the site, or by using a variation of Stuxnet that did not limit deployment of its payload so narrowly, but they did not do this. They lessened "collateral damage" to civilians and civilian property and designed Stuxnet in a way that sacrificed operational efficiency.

Falling under "proportionality," however, is the area in which current LOAC rules most likely fail to regulate an aspect of Stuxnet: the "release" of the worm's code to the public at large. When a worm or virus is released into a computer network, it does not destroy itself in the process of doing its damage, as a kinetic weapon does.[298] The individuals who released Stuxnet thus gave others a powerful weapon with which to attack their enemies. The recent development of the Duqu

[295] *See supra* notes 191–93 and accompanying text (explaining the standard to which commanders are held).

[296] *See supra* notes 122–24 and accompanying text (describing the LOAC policy goals).

[297] *See supra* notes 214–17 and accompanying text (describing the "excessive" requirement).

[298] *See supra* notes 98–99 and accompanying text (noting the proliferation of Stuxnet to numerous computers after its initial deployment).

virus demonstrates this principle.[299] While it is not known who developed Duqu, commentators have speculated that a third party, unrelated to Stuxnet's initial development, may have taken Stuxnet's code and modified it for their own uses.[300]

Should future use of Stuxnet's code by third parties factor into a proportionality analysis? Under current LOAC rules, the issue is still governed by whether a commander should rationally "expect" the resulting harm.[301] With this in mind, it is not unreasonable to "expect" that someone with malicious intent could redesign Stuxnet to cause harm. There are numerous unanswered questions that must be considered in a rational expectation test: how likely it is that the source code will be decrypted?; how likely it is that the decrypted code will be made publicly available?; what kind of damage could reasonably be caused by new versions of the malware?; how central to the new malware would the original code have to be to connect the subsequent harm to the original attack?; and how far into the future would these connections extend? It seems impossible to answer some of these questions realistically. Predicting what every criminal group, terrorist cell, hacker, and government would do with the code of a cyber weapon seems to be an unworkable test for a commander to apply. While the "rational expectation" standard is straightforward and easy to administer on a physical battlefield, and also seems to apply well to both the immediate and knock-on consequences of a cyber attack, it is questionable whether it can effectively regulate subsequent third party action following the release of a cyber weapon. New regulations therefore may be necessary.

CONCLUSION

Stuxnet almost certainly foreshadows a fundamental change in modern warfare. It demonstrates that a well-orchestrated CNA can strike a target with greater precision, greater damage to the enemy, and less collateral loss of life and property than a kinetic weapon. Will the change in warfare,

[299] *See supra* notes 104–07 and accompanying text (describing the Duqu virus).

[300] *See supra* note 106 and accompanying text (speculating about who may be responsible for Duqu).

[301] *See supra* note 204 and accompanying text (noting the proportionality analysis is covered by the "expectation" standard).

however, be so drastic that it also necessitates a change in the LOAC? The answer appears to be both "yes" and "no."

The principles of distinction, discrimination, and proportionality, when applied to Stuxnet, further the LOAC policy goals of reducing overall destruction in warfare and reducing unnecessary harm to civilians and civilian property. Further, evidence that Stuxnet's programmers may have designed it to conform with the LOAC, and the subsequent benefits that that conformity brought, demonstrates that compliance with the LOAC is possible, practical, and beneficial. In this respect, the LOAC seems to adequately regulate Stuxnet. Stuxnet therefore should be considered a piece of evidence that fundamental alterations to the LOAC are not necessary to regulate cyber weapons.

The current LOAC principles, however, appear unable to properly address the dangers associated with the acquisition of Stuxnet's source code by third parties. The worldwide proliferation of such a weapon may require additional treaties to regulate this potential danger. Whether such a treaty is feasible, given the proven effectiveness of cyber weapons, remains to be seen.