Stuxnet and the Limits of Cyber Warfare

Jon R. Lindsay
University of California Institute on Global Conflict and Cooperation
jrlindsay@ucsd.edu
Version: 15 January 2013
(Accepted by *Security Studies*; final copyedited version may differ from this draft)

Abstract

Stuxnet, the computer worm which disrupted Iranian nuclear enrichment infrastructure in 2010, is the first instance of computer network attack known to cause physical damage across international boundaries. Some have described Stuxnet as the harbinger of a new form of digital warfare which threatens even the strongest military powers. The influential but largely untested Cyber Revolution thesis holds that the internet gives militarily weaker actors asymmetric advantages; that offense is becoming easier while defense is growing harder; and that the attacker's anonymity undermines deterrence. However, the empirical facts of the Stuxnet attack can also be interpreted to support the opposite conclusions: cyber capabilities can marginally enhance the power of stronger over weaker actors; the complexity of weaponization makes cyber offense less easy and defense more feasible than generally appreciated; and cyber options are most attractive when deterrence is intact. Stuxnet suggests that considerable social and technical uncertainties associated with cyber operations may significantly blunt their revolutionary potential.

Author

Jon Lindsay is a postdoctoral scholar at the University of California Institute on Global Conflict and Cooperation in La Jolla, CA. He received his Ph.D. in political science from the Massachusetts Institute of Technology and M.S. in computer science and B.S. in symbolic systems from Stanford University. He has served as a U.S. Navy officer in the Middle East, Balkans, and Latin America.

Acknowledgements

I thank Erik Gartzke, Eugene Gholz, Brendan Green, Robert Giesler, Sean Lawson, Carrie Lee Lindsay, Joshua Rovner, and the anonymous reviewers for helpful comments and advice.

Introduction

On June 17, 2010 an obscure antivirus firm in Belarus received an email from a customer in Iran: a machine was stuck rebooting itself over and over again. This glitch prompted discovery of a mysterious piece of malicious software (malware) which forensic investigators christened "Stuxnet" based on a filename in the code.[1] Computer security experts have described Stuxnet as "the most technologically sophisticated malicious program developed for a targeted attack to date"[2] and as "a precision, military-grade cyber missile."[3] Allegedly a joint U.S.-Israeli component of a broader U.S. cyber campaign against Iran code-named "Olympic Games," the attack damaged over a thousand centrifuges at the Natanz uranium enrichment facility.[4] Shortly after the attack became public, a senior Mossad official assessed that Iran's sudden technical difficulties could delay acquisition of a nuclear device to 2015.[5] Breathless media accounts have portrayed Stuxnet, which physically injured no one, as "the cyber equivalent of the dropping of the atom bomb"[6] and "a new era of warfare".[7] Concerns soon surfaced about unbridled proliferation of Stuxnet code, now openly available on the internet, and potential collateral

[1] The original announcement of "Rootkit.TmpHider" was posted by Sergey Ulasen of VirusBlokAda on an information security forum on 12 July 2010 (archived at http://www.anti-virus.by/en/tempo.shtml). For an accessible account of Stuxnet's discovery see Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired Threat Level Blog, 11 July 2011 (http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet)

[2] Aleksandr Matrosov, Eugene Rodionov, David Harley and Juraj Malcho, "Stuxnet under the Microscope," ESET White Paper, 20 January 2011. The dubious honor of "most sophisticated malware" has perhaps passed to a Stuxnet relative named Duqu or to the Flame spyware (which is twenty times the filesize as Stuxnet).

[3] Mark Clayton, "Stuxnet Malware is 'Weapon' Out to Destroy…Iran's Bushehr Nuclear Plant?," *Christian Science Monitor* (21 September 2010).

[4] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times* (1 June 2012)

[5] William J. Broad, John Markoff and David E. Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times* (15 January 2011).

[6] Mark Clayton, "The New Cyber Arms Race," *Christian Science Monitor* (7 March 2011). In this vein the cover of *The Economist* (3 July 2010) depicted a digitized mushroom cloud.

[7] CBS News, "Stuxnet: Computer Worm Opens New Era of Warfare," *60 Minutes*, Transcript (4 March 2012)

damage beyond Natanz. As the Russian ambassador to NATO worried, "These 'mines' could lead to a new Chernobyl."[8]

According to General Michael V. Hayden, former director of the Central Intelligence Agency (CIA) and the National Security Agency (NSA), Stuxnet is "the first attack of a major nature in which a cyberattack was used to effect physical destruction."[9] The attack obviously did not permanently derail Iran's nuclear program: enrichment recovered within a year, and concerns mounted throughout 2012 that Israel or the U.S. might launch airstrikes to address the worsening problem. Nevertheless, Stuxnet's technical performance did demonstrate that cyber weapons are not just science fiction. As a proof-of-concept, it appears to support claims that ubiquitous digital technologies create a potent new form of warfare. Many see Stuxnet as the harbinger of even more devastating attacks to come, or the leading edge of a cybersecurity Revolution in Military Affairs (RMA). Now that the genie is out of the bottle, many argue, even weak states and other political actors are encouraged to acquire cyber capabilities, and these increasingly threaten the U.S. and other advanced industrial countries.[10]

The notion of a Cyber Revolution, once just a preoccupation of information age futurists, has become widely influential in defense policy circles. Defense Secretary Leon Panetta claimed that "A cyber attack perpetrated by nation states or violent extremists groups could be as

[8] "Russia says Stuxnet could have caused new Chernobyl," *Reuters* (26 January 2011)
[9] Sanger, "Obama Order"
[10] Arguments for the Cyber Revolution thesis by former senior U.S. officials include Mike McConnell, "Cyberwar is the New Atomic Age," *New Perspectives Quarterly* vol. 26, no. 3 (2009): 72-77; Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York, NY: Harpercollins, 2010); Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011). On Stuxnet as an RMA see James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* vol. 53, no. 1 (2011): 23-40; Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011); Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal* (April 2011); Sean Collins and Stephen Mccombie, "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications," *Journal of Policing, Intelligence and Counter Terrorism* vol. 7, no. 1 (2012): 80-91; James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* vol. 54, no. 4 (2012): 107-120.

destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation."[11] President Barack Obama wrote that "the cyber threat to our nation is one of the most serious economic and national security challenges we face."[12] In Senate testimony, Federal Bureau of Investigation (FBI) Director Robert S. Mueller III predicted that "down the road, the cyber threat, which cuts across all programs, will be the number one threat to the country."[13] A recent Chairman of the US Joint Chiefs of Staff went even further: "The single biggest existential threat that's out there, I think, is cyber."[14] The drumbeat of threat rhetoric has inspired the creation of new bureaucracies like U.S. Cyber Command and increased spending for cyber capabilities in an era of defense budget austerity. Other countries, notably China, Russia, Israel, Germany, and the United Kingdom among others, have also stepped up investment in cyber capabilities.[15]

Analytical assessment of the Cyber Revolution, however, has lagged behind all the considerable governmental interest. Most work on international cybersecurity originates from the policy analysis community and has tended to be supportive of Cyber Revolution ideas.[16] By contrast, the handful of scholars from the academic security studies field who have addressed

[11] Remarks By Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
[12] Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal* (19 July 2012)
[13] Defense Intelligence Agency, "TRANSCRIPT: Senate Select Intelligence Committee Holds Hearing on Worldwide Threats," 31 January 2012, http://www.dia.mil/public-affairs/testimonies/2012-01-31.html
[14] Admiral Mike Mullen, quoted in Marcus Weisgerber, "DoD to Release Public Version of Cyber Strategy," *Defense News*, 8 July 2011. This is an incredible claim coming from a man well familiar with the world's nuclear arsenals.
[15] James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, DC: Center for Strategic and International Studies, for the United Nations Institute of Disarmament Research, 2011)
[16] See, *inter alia*, Nicholas Burns and Jonathon Price, *Securing Cyberspace: A New Domain for National Security* (Aspen, CO: Aspen Institute, 2012); Kristin M. Lord and Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age* (Washington DC: Center for a New American Security, 2011); David J. Betz and Timothy C. Stevens, "Cyberspace and the State: Toward a Strategy for Cyber-Power," *IISS Adelphi Paper*, no. 424 (2011); Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, "On Cyber Warfare," Royal Institute of International Affairs, Chatham House Report (November 2010); Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington DC: National Defense University Press, 2009).

cyber warfare have generally (but not exclusively) been skeptical of the notion that the internet revolutionizes war.[17] Their criticism has relied mainly on deductive arguments and skepticism of threat inflation rather than empirical evaluation of propositions about cyber warfare, largely due to a dearth of reliable data. Fortunately, information has recently emerged through open technical sources and journalist reportage about Stuxnet.[18] This important case provides inspiration for prophets of cyber war and presents the only opportunity for empirical assessment of their ideas. Most accounts of Stuxnet have focused on its unprecedented technical wizardry rather than evaluation of its strategic consequences. While very different types of cyber attack than Stuxnet are imaginable in principle, this case has the distinction of being the only historical case available for scrutiny. A complete account of this episode must await disclosure of data from both sides of the attack, but it is now at least possible to begin testing theoretical claims of the strategic consequence of cybersecurity.

---

[17] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* vol. 35, no. 3 (2012), Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* vol. 35, no. 1 (2011): 5-32; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); Evgeny Morozov, "Cyber-Scare: The Exaggerated Fears over Digital Warfare," *Boston Review* (July/August 2009); Myriam Dunn Cavelty, "Cyber-Terror: Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology & Politics* vol. 4, no. 1 (2008): 19-36; Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007); Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Bradley A. Thayer, "The Political Effects of Information Warfare: Why New Military Capabilities Cause Old Political Dangers," *Security Studies* vol. 10, no. 1 (2000): 43–85; Peter D. Feaver, "Blowback: Information Warfare and the Dynamics of Coercion," *Security Studies* vol. 7, no. 4 (1998): 88-120.

[18] On the direct technical effects of Stuxnet on Iranian computer systems, I draw on forensic investigation by computer security firms Symantec, ESET, and Langner Communications: Nicolas Falliere, Liam O Murchu and Eric Chien, "W32.Stuxnet Dossier, version 1.4," Symantec, 4 February 2011; http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; Aleksandr Matrosov, Eugene Rodionov, David Harley and Juraj Malcho, "Stuxnet under the Microscope, version 1.31," ESET, 20 January 2011, http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; Ralph Langner, "Stuxnet Attack Code Deep Dive," Presentation at Digital Bond SCADA Security Scientific Symposium (S4) in Miami, Florida, January 18-19, 2012, http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video; a synthesis of technical details accessible to lay readers and a detailed interactive timeline can be found in Zetter, "How Digital Detectives Deciphered Stuxnet". To assess Stuxnet's indirect strategic effects on Natanz, I rely on International Atomic Energy Agency (IAEA) inspection reports (http://www.iaea.org/newscenter/focus/iaeairan/iaea_reports.shtml) and Institute for Science and International Security (ISIS) analyses of Iranian enrichment operations (http://isisnucleariran.org/). I supplement these with contemporary press reporting, particularly David E. Sanger's investigation of Olympic Games in the *New York Times*.

The emerging literature on the Cyber Revolution is uneven, but three widely held beliefs can be identified. Together these can be taken as a thesis that critical economic and military infrastructure is dangerously vulnerable because: the internet gives militarily weaker actors asymmetric advantages; offense is becoming easier while defense is growing harder; and the difficulty of attributing the attacker's identity undermines deterrence. However, the empirical facts of the only major, publicly-known case of deliberate mechanical disruption via cyber means do not bear these assumptions out. Indeed, Stuxnet can be interpreted to support to the opposite conclusions: cyber capabilities can marginally enhance the power of stronger over weaker actors; the complexity of weaponization makes cyber offense less easy and cyber defense more feasible than generally appreciated; and cyber options are most attractive when strategic deterrence is intact. There is reason to believe that the considerable social and technical uncertainties associated with cyber operations will significantly blunt their revolutionary potential.

This paper proceeds in four parts. First I review contemporary ideas and evidence about cybersecurity in order to distinguish strategic cyber warfare from lesser irritants. Second I provide a brief technical overview of the Stuxnet attack. Third I use the details of the case to evaluate Cyber Revolution claims about asymmetry, offense-dominance, and deterrence. I conclude with a discussion of Stuxnet's more general implications for the future of cyber warfare.

The Cyber Revolution

Over the past half-century, digital technology has become deeply-embedded in the fabric of political and economic life. Networked computers underwrite the performance of the global financial system, industrial services and manufacturing, public utilities and government

bureaucracy, and military surveillance and power projection. Systems which connect organizations across borders and automate routine processes have greatly improved operating efficiency over the long run. Unfortunately, an asset can become a liability in the presence of a creative opponent. Connective networks create access vectors for adversaries who can instruct deterministic machines to behave in ways designers and users never intended. The potential injurious applications of information technologies are as diverse as the legitimate uses of so ubiquitous a technology; as a result a lot of different threats tend to be conflated in cybersecurity discourse. It is important to distinguish the lower intensity but more frequent types of irritants in cyberspace from the more dramatic but relatively unrealized threats of cyber warfare.[19]

The majority of malicious activity in cyberspace is financially motivated. Profitable activity includes advertisement through email spam or optimization of search engine results, fraudulent scams and theft of digital credentials or bank accounts, and trading in commoditized support infrastructure such as malware, domain registration, or compromised hosts (i.e., botnets). Estimated damages of cybercrime tend to be wildly exaggerated, but may run over a hundred billion dollars annually worldwide. However, only a small proportion of cyber criminals actually make this money because the risks and imperfections of criminal markets limit profitability for the majority of participants.[20]

---

[19] For a detailed history of computerization in the American private and public sector see James W. Cortada, *The Digital Hand*, 3 Vol. (New York: Oxford University Press, 2004, 2006, 2008). The "productivity paradox" debate over the relationship between IT inputs and firm performance has been resolved following clarification of the critical role of organizational structure and process: Erik Brynjolfsson, Lorin M. Hitt and Shinkyu Yang, "Intangible Assets: Computers and Organizational Capital," *Brookings Papers on Economic Activity* vol. 2002, no. 1 (2002): 137-181. For a textbook introduction to technical cybersecurity see Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition* (Indianapolis: Wiley Publishing, 2008). For a good introduction to offensive cyber operations, including attack/disruption and exploitation/theft, see William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009).

[20] Ross Anderson, Chris Barton, Rainer Bohm, Richard Clayton, Michel J.G. Van Eeten, Michael Levi, Tyler Moore and Stefan Savage, "Measuring the Cost of Cybercrime," *Proceedings of the Workshop on the Economics of*

The same underground infrastructure that is useful for stealing monetizable data can also be used to steal secrets from a firm or government. A major variant of the Cyber Revolution thesis is that sustained campaigns to raid intellectual property and commercial secrets can enable a rising power to undermine a stronger victim. This scenario is oft described as "death by a thousand cuts" to contrast with a catastrophic "digital Pearl Harbor" or "digital 9/11." Oft-cited examples include Chinese intrusions into Western networks known by names like Titan Rain, Byzantine Haydes, Aurora, and Shady RAT. It is easy to exaggerate and difficult to estimate the scope of real damage to commercial or military competitiveness: the cyber spy may vacuum up much information but little of value, or be unable to recognize or act on that which is valuable. Whatever the strategic effects of large-scale espionage, its rising incidence does tend to reinforce fears of more destructive cyber warfare. As discussed below, cyber reconnaissance can support cyber attack by identifying targets and defenses, just as intelligence collection precedes most conventional military assaults. Moreover, the same methods and vulnerabilities used to steal data can also be used to disrupt system functioning; the only difference is the logical content of the malicious payload. For example, spyware known as Duqu, Flame, and Gauss was discovered on computers in the Middle East and found to share a number of technical characteristics with Stuxnet, suggesting that they were built from the same software toolkit. The interaction between

Information Security (June 2012); Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon Mccoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker and Stefan Savage, "Click Trajectories: End-To-End Analysis of the Spam Value Chain," *Proceedings of the IEEE Symposium and Security and Privacy* (May 2011): 431-446; Misha Glenny, *DarkMarket: How Hackers Became the New Mafia* (New York: Vintage, 2011); Cormac Herley and Dinei Florêncio, "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy," *Economics of Information Security and Privacy* (2010): 33-53

computer network exploitation and infrastructure attack complicates intelligence warning considerably, but logically they are different activities with different ultimate consequences.[21]

A third category of computer abuse is political protest or "hacktivism." Tools can be cheaply obtained online to deface websites, overload web servers with spurious requests through distributed denial of service (DDoS) attacks, or shame firms or governments through public revelation of compromised secrets (e.g., Anonymous and Wikileaks). Outbursts of malicious internet nationalism have been regular features of China's periodic spats with Taiwan, Japan, or the U.S. Temporary disruption of internet services can indeed be financially costly, as demonstrated by the Russian nationalist DDoS attacks against Estonia in 2007 which caused banks to suspend services. Russian civilians again unleashed a wave of DDoS attacks in 2008 against Georgian government servers, allegedly with advance notification of the Russian invasion. The military result of Russia's assault against a far weaker victim was completely over-determined: Georgia would have been handily defeated even without the crowd-sourced barrage jamming, but this case does raise the possibility that targeted DDoS attacks *in conjunction with traditional military operations* might provide some marginal improvement to military effectiveness. These episodes all highlight an emerging arena for nationalist expression and raise nettlesome diplomatic questions of state complicity in online misbehavior. Yet nuisance attacks in this category are usually reversible and mitigation techniques are readily available, so their tactical utility as a destructive weapon is limited. A related claim regarding the political potency

[21] Bryan Krekel, Patton Adams and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp (7 March 2012); Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011, October 2011; *Shadows in the Cloud: An Investigation into Cyber Espionage 2.0*, Joint Report of the Information Warfare Monitor and Shadowserver Foundation (6 April 2010), http://shadows-in-the-cloud.net; Kaspersky Lab, "Gauss: Abnormal Distribution," Kaspersky Lab Global Research and Analysis Team Report (August 2012), http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution.

of the internet is that online social movements can pose serious democratizing threats to authoritarian regimes; yet such regimes have also proved adept at using the internet to suppress dissent. It is well beyond this paper's scope to assess this diverse but ultimately nonviolent online political activity. As with espionage, its rising incidence feeds fears that mass movements in cyberspace may someday soon gain the capacity for more destructive activity.[22]

Cyber warfare, in contrast with all of the above, employs computer network attack as a use of force to disrupt an opponent's physical infrastructure for political gain.[23] This includes military cyber operations that degrade enemy data processing to facilitate an integrated assault during wartime. Such tactical measures are a functional outgrowth of the electronic warfare tradition, as exemplified in the 2007 Israeli airstrike on a Syrian reactor which may have relied on cyber attacks to blind Syrian radars.[24] Lt. Gen. Richard P. Mills, U.S. Marine Corps, said that "as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact…I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."[25] Most advanced industrial militaries are actively experimenting with cyber attacks for command and control surveillance, deception, and disruption (and defense

[22] Christian Czosseck, Rain Ottis and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Journal of Cyber Warfare and Terrorism* vol. 1, no. 1 (2011); John Bumgarner and Scott Borg, "Overview By the US-CCU of the Cyber Campaign Against Georgia in August of 2008," US Cyber Consequences Unit Report, August 2009; Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambirdge, MA: MIT Press, 2011); Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011).

[23] Military doctrine has not yet stabilized for cyber concepts yet, and debate continues on the distinctions between cyber warfare, computer network operations, information operations, electronic warfare, *etc*. I focus in this paper on the use of computer hacking to cause mechanical damage in the service of strategic objectives. Cyber warfare clearly encompasses the tactical modalities of cyber attack (degredation of normal hardware or software functionality), exploitation (covert theft or use of data or computational resources), and defense (efforts to prevent adversarial attack or exploitation); my emphasis in this paper is on the primary aggressive move of attack.

[24] David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis," *Aviation Week*, Ares Blog, 3 October 2007. Some sources dispute whether the Israelis used cyber attack or more traditional forms of electronic jamming: Ellen Nakashima, "U.S. Accelerating Cyberweapon Research," *Washington Post* (18 March 2012).

[25] Raphael Satter, "US General: We Hacked the Enemy in Afghanistan," *Associated Press* (24 August 2012)

against similar enemy efforts) as an adjunct to conventional combined-arms operations. Yet due to the secrecy surrounding cyber operations, the extent of their use or effectiveness on contemporary battlefields is largely unknown.

The most provocative claims for cyber warfare go beyond wartime military use and involve its ability to wreck critical industrial control systems (ICS) and create strategically significant effects *in lieu* of conventional military operations altogether. Nightmare scenarios of the Cyber Revolution usually feature small groups of state-sponsored or terrorist hackers who exploit the same methods criminals use to steal passwords to disrupt the ICS that regulate factory automation, electrical power grids, air traffic control, water distribution, financial networks, and military weapons control systems. The catastrophic failure of ICS thereby causes mass havoc, with little cost or risk to the perpetrator. Cyber attacks at this scale are strategic in the sense of "strategic bombing" in that they bypass direct battlefield confrontation in order to devastate civilian economic or military infrastructure targets. Cyber warfare thus becomes a strategic substitute for rather than an operational complement to conventional military force.[26]

The idea of strategic cyber warfare has been around for decades.[27] Leon Panetta warned of a "digital Pearl Harbor" in his 2011 Senate confirmation hearing, but the phrase has appeared

[26] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), distinguishes "operational cyberwar—cyberattacks to support warfighting" from "strategic cyberwar, cyberattacks to affect state policy" (p. 6). The Cyber Revolution thesis treated in this paper emphasizes the latter threat, particularly via ICS attack. ICS are the industrial plant equivalent of military command and control (C4ISR) systems; they include the embedded controllers which drive machines like generators, valves, production lines, etc., embedded sensors which monitor their performance, Supervisory Control and Data Acquisition (SCADA) systems which allow human operators to visualize and manage the process, and the network architecture which connects it all together. For a primer on ICS security see Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats* (New York: Momentum Press, 2010).

[27] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* vol. 27, no. 5 (2012): 781-799; James Adams, *The Next World War: The Weapons and Warriors of the New Battlefields of Cyberspace* (London: Arrow, 1998).

regularly since at least 1991.[28] At the same time, the use of cyber weapons to cause physical damage is conspicuously absent in the historical record. Other than Stuxnet, examples of computer hacking causing serious physical damage are few and far between: a dubious account of CIA sabotage of Russian pipeline equipment in 1982;[29] electrical malfunctions mistaken for attacks;[30] various computer pranks.[31] In 2007 the Idaho National Laboratory demonstrated that alterations to the software controlling an electrical turbine could drive the generator beyond its mechanical limits and cause it to explode. Yet until Stuxnet there were no major cyber attacks on ICS in real-world circumstances.[32]

In the absence of evidence of strategic cyber warfare, many look to industrial accidents to illustrate its lethal potential. General Keith Alexander, commander of U.S. Cyber Command and the National Security Agency, points to events like Russia's Sayano-Shushenskaya dam catastrophe of 2009. In this instance a computer operator 500 miles away mistakenly sent a command to start a hydroturbine generator then undergoing maintenance; this human error

---

[28] Anna Mulrine, "CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack," *Christian Science Monitor*, 9 June 2011. According to Scott Berinato, "The Future of Security," *Computerworld* (30 December 2003), the first use of the phrase "digital Pearl Harbor" was in 1991 by then RSA president D. James Bidzos.

[29] Widely cited as an example of supply-chain sabotage is an elaborate 1982 counterintelligence operation in which the CIA allegedly tampered with Canadian software that the Soviets planned to steal. Once the Soviets installed it in controllers on the Trans-Siberian oil pipeline, this Trojan horse caused "the most monumental non-nuclear explosion and fire ever seen from space" and "significant damage to the Soviet economy," according to Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York, NY: Random House, 2004), 268-9. However, Rid, "Cyber War Will Not Take Place," finds little corroborating evidence for Reed's story, which should have had eyewitnesses aplenty.

[30] Electrical blackouts in Brazil in 2007 and 2009 have been blamed on hackers, but no supporting evidence has emerged while simpler explanations have been offered in each case: Marcelo Soares, "Brazilian Blackout Traced to Sooty Insulators, Not Hackers," *Wired Threat Level Blog*, 9 November 2009, http://www.wired.com/threatlevel/2009/11/brazil_blackout; also, a Wikileaks cable from the American Embassy in Brasilia dated 011127Z DEC 09 discounts the possibility of a cyber attack in the 2009 blackout.

[31] Other examples of physical damage include malicious experiments likely created for hacker bragging rights, like the 1999 Chernobyl or Spacefiller virus which could overwrite Basic Input Output System (BIOS) data and effectively turn a computer into a useless brick.

[32] On the INL Aurora demonstration see Jeanne Meserve, "Staged cyber attack reveals vulnerability in power grid," CNN, 26 September 2007. On the historical absence of cyberwar see Sean Lawson, "Beyond Cyber Doom: Cyber Attack Scenarios and the Evidence of History," George Mason University Mercatus Center Working Paper (January 2011); Michael Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?" *Crime, Law and Social Change* vol. 46 (4-5 2006): 223-238.

resulted in a flood that killed 75 people and ruined eight of the remaining turbines.[33] Such examples are meant to show that because ICS accidents can and do happen, they *could* also be triggered intentionally via cyber attack. They tell us little, however, about how hard or easy it is to cause such failures *predictably at will*, an important distinction between an unforeseen accident and a controlled attack, let alone the conditions under which it would make sense to employ such a weapon against an actual adversary.

In the universe of cybersecurity, therefore, we observe a high frequency of low intensity cyber attacks resulting in computer crime, espionage, and hacktivism, but a remarkably low frequency of high intensity cyber warfare resulting in serious infrastructure damage. Thus in order to describe the phenomenon of cyber warfare, most Cyber Revolution proponents must either speculate deductively from the assumed properties of cyber technology or inductively through analogy with more prevalent cyber irritants. The first rhetorical option risks ignoring the effects of strategic context while the second risks ignoring the effects of increasing scale and complexity. As we shall see in the case of Stuxnet, context and complexity matter tremendously. In all of the diverse discourse on cyber warfare, three related beliefs about cyber warfare are often assumed but rarely evaluated. U.S. Deputy Secretary of Defense William J. Lynn III lists them all in a recent article describing Pentagon cyber strategy: (1) "cyberwarfare is asymmetric," (2) "the offense has the upper hand", and (3) "deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack's

[33] Bill Gertz, "Computer-Based Attacks Emerge As Threat of Future, General Says," *Washington Times* (13 September 2011). Alexander also cited "the August 2003 electrical power outage in the Northeast U.S. that was caused by a tree damaging two high-voltage power lines. Electrical power-grid software that controlled the distribution of electricity to millions of people improperly entered "pause" mode and shut down all power through several states."

perpetrator."[34] Before evaluating these propositions, I will first briefly summarize the conventional wisdom on each.

A Weapon of the Weak

Materially weaker actors can use cyber warfare, so the argument goes, to counter the military advantages of stronger adversaries. As President Obama states, "In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home."[35] The logic of asymmetric advantage in cyberspace assumes that barriers to entry for weak actors are falling while the vulnerabilities of strong actors are increasing. Offensive capability can be procured through online criminal markets; hacker support communities disseminate technical expertise; and the internet provides free targeting intelligence such as commercial satellite imagery from Google and social network graphs from Facebook and the like. Furthermore, weak actors can use cyberspace anonymously to evade detection and retaliation.[36]

As weak actors are empowered, strong actors become vulnerable. Advanced industrial countries are far more dependent on cyberspace than are less wired countries, and great powers in particular live in a glass house full of tempting computer targets. Network connections across critical infrastructures create potentials for intrusions and cascading failures that can greatly magnify the impact of a small attack; e.g., a successful ICS attack on a generator might shut down a power grid, which might imperil air traffic control and spark national panic. A former

[34] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* vol. 89, no. 5 (2010): 97-108, quote at pp. 98-99.
[35] Obama, "Taking the Cyberattack Threat Seriously"
[36] These and other trends lowering barriers to entry for cyber attack are described in Kenneth J. Knapp and William R. Boulton, "Cyber-Warfare Threatens Corporations: Expansion Into Commercial Environments," *Information Systems Management* (Spring 2006)

NSA expert thus claimed that North Korea could defeat the U.S. in three years with only 600 cyber warriors and $50 million, stating that "One of North Korea's biggest advantages is that it has hardly any Internet-connected infrastructure to target…On the other hand, the US has tons of vulnerabilities a country like North Korea could exploit."[37]

Cyberspace is Offense Dominant

The asymmetry between weak and strong is amplified by the ease of cyber attack relative to defense. At a technical level, it is impossible to block all attacks for the simple reason that a computer, if it is to be useful at all for control and communications, has to accept incoming connections. A deterministic machine will accept a superficially well-formed input, but then this code can instruct the machine to enter a state and perform some behavior the designer never intended.[38] The internet was designed to make connections easy and reliable even when the true identity of the connector and the path of the connection were unknown; security did not figure strongly in its early design. A hacker can thus reach across the world, safely anonymous within a foreign jurisdiction or an internet café, and attack repeatedly with varied techniques. Attackers especially prize "zero-day" vulnerabilities which have not been catalogued and patched by software vendors; zero-days can be purchased in underground markets.[39] Similarly, intrusion detection systems and anti-virus software rely largely on databases of malware signatures, but

[37] Clayton, "The New Cyber Arms Race." On cascading attacks see Scott Borg, "Economically Complex Cyberattacks," *IEEE Security and Privacy* vol. 3, no. 6 (2005): 64-67.

[38] A classic example of malformed input is a buffer overflow attack in which the attacker provides an input parameter larger than the space allocated for it by the programmer, who has failed to check the length of the input; the input string thus overwrites memory for the function's internal control variables, which were supposed to be inaccessible but can now be changed arbitrarily. Note that some types of attacks exploit physical connections rather than logical inputs. Although most malware goes through the front door to exploit programming flaws, side channel attacks can exploit information from the physical implementation of a system, such as excess heat generated by correct passwords. Furthermore, even the best designed systems can and often do fail through social engineering techniques such as phishing scams which exploit human gullibility.

[39] Andy Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," *Forbes* (23 March 2012), Http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

novel malware or permutations of existing malware can be undetectable. Offense is easier than defense, in this technical sense, because the attacker can vary vectors and signatures faster than the defender can detect and close them.[40] Furthermore, if the goal of technical defense is to prevent the compromise a system, then the defender has to succeed every time against every attack, but the attacker only has to succeed once.

The costs of cyber defense scale up steeply, it is argued, as networks connect more and more people. The U.S. Director of National Intelligence, James R. Clapper Jr., describes "a cyber environment in which emerging technologies are developed and implemented before security responses can be put in place."[41] Offensive capabilities improve quickly while network defense improves slowly because technology takes time to develop and defenders lack incentives to cooperate. A mélange of different actors with different interests often fail to coordinate defenses: vendors lack incentives to prioritize security development; users prize convenience over security; firms fail to report compromises in order to protect their reputations; government agencies responsible for national defense lack authority over private sector technology; legislation languishes in deadlock among the competing interests of national security, economic productivity, and civil liberty. The defense of critical infrastructure is particularly difficult because ICS engineers focus on efficiency and reliability rather than intrusion prevention. Haphazard connection of ICS to the internet for remote maintenance opens up new attack

[40] For a typical statement of the cyber offense dominance claim see: Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," Brookings Institution, February 2012, pp. 14-16. One interesting area where the problem of identifying and solving a novel signature has been inverted between offense and defense is in the "CAPTCHA" phrases websites use to discriminate humans from machines: the defender can rapidly generate new phrases while the attacker has a more costly solving problem. Criminals have solved this problem, however, not technically but through outsourcing CAPTCHA solving to people willing to solve a thousand per dollar. See Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon Mccoy, Geoffrey M. Voelker and Stefan Savage, "Re: CAPTCHAs -- Understanding Captcha-Solving from an Economic Context," *Proceedings of the USENIX Security Symposium, Washington, D.C.* (August 2010).

[41] Clapper, 1/31/12 Testimony

vectors; moreover, ICS operating systems tend to be harder to patch than their mainstream counterparts. Industrial culture and misaligned incentives combine to undermine computer security.[42] To paraphrase Lord Stanley Baldwin, the cyber attack will always get through.

Deterrence is Ineffective in Cyberspace

As discussed above, anonymity in cyberspace helps to empower weak actors and creates offensive advantage. It does so, many argue, because it undermines deterrence. Clapper notes that one of "our greatest strategic cyber challenges" is "definitive real time attribution of cyber attacks. That is, knowing who carried out such attacks and where these perpetrators are located."[43] Attackers can disguise themselves through aliased accounts, multiple user identities, forged or stolen credentials, obfuscated file properties, strong encryption, proxy servers, virtual private networks, and the ability to route attacks across multiple organizational and international jurisdictions. Criminal investigation across borders is a difficult and time-consuming process with uncertain results. Different levels of effort are required to discover the country of origin, the computer components employed, a particular individual perpetrator, of the organization sponsoring the attack. Forensics takes months, whereas the anonymous attack can present itself and perhaps complete in milliseconds.

[42] Ross Anderson and Tyler Moore, "The Economics of Information Security," *Science* vol. 27, no. 5799 (2006): 610-613; Terrence August and Tunay I. Tunca, "Network Software Security and User Incentives," *Management Science* vol. 52, no. 11 (2006): 1703–1720; Johannes M. Bauer and Michel J. G. Van Eeten, "Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options," *Telecommunications Policy* vol. 33, no. 10 (2009): 706-719; Ludovic Pietre-Cambacedes, Marc Tritschler and Goran N. Ericsson, "Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs," *IEEE Transactions on Power Delivery* vol. 26, no. 1 (2011): 161 – 172.

[43] DIA, "TRANSCRIPT," 31 January 2012. On the complexity of attribution see David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks*, ed. by National Research Council (Washington, DC: National Academies Press, 2010): 25-40.

Unlike a military invasion or missile launch, the origin of a cyber attack is often quite ambiguous. If attacks "have no return address," then victims can't credibly threaten retaliation against would-be attackers. Retaliating against the wrong country just because an attack originated there would be foolish: the attack could have simply been routed through another country, initiated by some group unconnected to the state, or be a "false flag" operation designed to cast suspicion on a third party. If deterrence by threat of punishment becomes infeasible, then states might be better off with deterrence by denial through improved defenses. Unfortunately, because cyber defense is harder than offense, it is difficult to deny access to the shadowy attacker and impair his ability to cause significant damage. If even weak actors can counter stronger ones through cyber operations, then they may be tempted to attack even nuclear-armed powers, expecting to remain anonymous or to paralyze command and control. Moreover, in the unlikely event that the victim does eventually attribute or even suspect the identity of the attacker, then he will not be deterred from launching unattributable cyber attacks in retaliation.[44]

All three of these conventional wisdoms about the Cyber Revolution—asymmetry, offense-dominance, and deterrence failure—infer strategic consequences directly from the supposedly inherent nature of information technology. They draw support from prevalent examples of crime, espionage, and hacktivism. All depend on a growing sense of pervasive vulnerability to ubiquitous computers rather than demonstration of some specific threat of catastrophic attack. As Chairman of the Joint Chiefs of Staff General Martin Dempsey put it, "cyber is the black swan because we don't know exactly what capabilities exist out there, but we do know our vulnerabilities." He then concludes, "cyber is the threat that concerns me the

[44] For richer discussion of the challenges of cyber deterrence—which might mean deterring cyber attacks or using the threat of cyber attack to deter other activity—see National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks*, and Libicki, *Cyberdeterrence and Cyberwar*.

most."[45] Yet what type of technical and organizational work does it actually take to convert infrastructural vulnerability to harm into useful harm? The case of Stuxnet, the only historical case of strategic cyber warfare, suggests that the path from technical potential to strategic consequence is not at all straightforward.[46]

The Technical Attack

Cyber warfare is a complicated business. There are no general purpose munitions that can simply be aimed and fired to destroy a complex industrial target at will. Cyber planners must gather detailed intelligence on the mechanical and organizational dimensions of their target, gain access to the target's computer network, exploit system vulnerabilities to navigate through the network to the ICS, and then activate a custom-engineered payload to sabotage it. Stuxnet's technical particulars reveal a devious genius on the part its developers and highlight the challenges of network defense. Yet when viewed in its strategic context, this same complexity also suggests that much can go wrong along the way.

The Target

A number of United Nations Security Council Resolutions between 2006 and 2008 demanded that Iran suspend uranium enrichment and reprocessing and submit to additional safeguards. Iran refused to cooperate fully and pressed ahead with further nuclear research and enrichment, ostensibly to meet its future domestic energy requirements as permitted by the Nuclear Non-Proliferation Treaty. International Atomic Energy Agency (IAEA) inspectors were

[45]General Martin Dempsey, speech delivered at the Commonwealth Club of California, 27 July 2012, http://www.commonwealthclub.org/events/archive/podcast/general-martin-dempsey-chairman-joint-chiefs-staff-72712

[46] I am grateful to Erik Gartzke for framing the gap between the "logic of possibility" and the "logic of consequence" in cyber warfare discourse; see *idem*, "The Myth of Cyber War: Bringing War on the Internet Back Down to Earth," paper presented at the International Studies Association Annual Convention, San Diego (April 2012).

not able to rule out a weapons program, however, either through the higher enrichment of uranium or through plutonium reprocessing. Iran had advanced furthest with the former, using centrifuge technology derived from Pakistani designs. While lightly enriched uranium (LEU) is appropriate for peaceful nuclear power, the same centrifuge infrastructure could also be used to produce highly-enriched fissile material (HEU).[47]

The U.S. and Israel began to secretly consider military options to delay Iranian nuclearization. The most important node in Iran's enrichment program at the time was Natanz, a remote facility 150 miles south of Tehran, which began industrial operations in February 2007. Natanz has two underground production halls with enough total room for 50,000 centrifuges; by mid-2009 the Iranians had installed about 8,000 centrifuges in one hall. Destruction of this underground facility by direct airstrike would have been feasible, but it would have required a large package to suppress air defenses and to deliver sufficient munitions with some creative weaponeering. This course of action was fraught with risk of casualties and severe diplomatic fallout regardless of the tactical outcome. Furthermore, a November 2007 U.S. National Intelligence Estimate assessed that Tehran had not decided to restart its nuclear weapons program. This undermined justification for a kinetic strike.[48]

---

[47] IAEA, "Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1835 (2008) in the Islamic Republic of Iran," GOV/2010/10, 18 February 2010

[48] Whitney Raas and Austin Long, "Osirak Redux? Assessing Israeli Capabilities to Destroy Iranian Nuclear Facilities," *International Security* vol. 31, no. 4 (2007): 7-33; Office of the Director of National Intelligence, "Iran: Nuclear Intentions and Capabilities," November 2007, http://www.dni.gov/press_releases/20071203_release.pdf. The FEP layout is described in IAEA *op cit*. and in David Albright and Corey Hinderstein, "The Iranian Gas Centrifuge Uranium Enrichment Plant at Natanz: Drawing from Commercial Satellite Images," Institute for Science and International Security, 14 March 2003. Natanz enriches uranium hexafluoride (UF_6) gas, which it obtains from the Isfahan uranium conversion facility, to make LEU in two facilities: a small above-ground pilot fuel enrichment plant (PFEP) for research, and a much larger underground fuel enrichment plant (FEP) for industrial production. While inspectors have never detected enrichment over 5% LEU at the FEP, the PFEP has produced small amounts of 20% LEU, ostensibly for medical and scientific research. If Iran were to make a breakout dash to enrich enough 93% HEU for a few bombs within a few months, it would almost certainly have to use the industrial-sized fuel enrichment plant at Natanz. See David Albright, Paul Brannan, Andrea Stricker, Christina Walrond and Houston

Strategic planners thus sought a less provocative way to set back enrichment and, from an American perspective, to persuade Israel to avoid launching an airstrike. Instead, they targeted the ICS which controlled centrifuge operations at Natanz. The facility used a popular industrial automation package from Siemens called SIMATIC STEP 7. SIMATIC software runs on Microsoft Windows operating systems and provides human interfaces to monitor and control the peripheral devices which drive equipment such as centrifuge rotors. To modify SIMATIC, an attacker would have to penetrate through components from multiple vendors and several concentric layers of defenses. These would have included an enterprise network for everyday computing, a firewall-protected perimeter network for administration, and internal control networks running the centrifuge cascades.[49]

Access to the Network

The ICS networks at Natanz could not be reached directly from the internet (although there may have been indirect connections for maintenance). Most likely, a human being had to

---

Wood, "Preventing Iran from Getting Nuclear Weapons: Constraining Its Future Nuclear Options," Institute for Science and International Security, 5 March 2012.

[49] The precise configuration of Natanz' networks has not been revealed to IAEA inspectors, but we can gain some insight into the defensive challenge from Siemens-recommended best practices for ICS security and through analysis of the pattern of exploits employed by Stuxnet, as discussed in Eric Byres, Andrew Ginter and Joel Langill, "How Stuxnet Spreads: A Study of Infection Paths in Best Practice Systems," Tofino Security White Paper, 22 February 2011. The Iranians probably diverged significantly from best practices, but the operational implications of this are ambiguous, as discussed below: it may either have provided more vulnerabilities to exploit, or it may have invalidated target intelligence. According to Byres *et al*., the outer level of the FEP would have been the enterprise network, which hosted most of the everyday business and administrative computers. Within that was the perimeter network—sometimes called "the demilitarized zone" among ICS administrators—where servers managed the computer equipment in the control systems and provided data to end users in the enterprise network. Firewall servers on the perimeter network gateways would have been set to "deny by default" so that they only allowed incoming connections from authorized users with legitimate credentials and outgoing connections only to specifically approved servers for maintenance. This network may indeed have had physical connections from the FEP's exterior networks to sensitive ICS to facilitate remote management and troubleshooting—there might not have been an "air gap"—but there would have been, nonetheless, multiple logical layers of defenses to penetrate. The perimeter network protected SIMATIC systems, and there may have been different system partitions for each of the different cascade modules in the FEP's two production halls. Each of these included the process control network which hosted human interface servers for the SIMATIC operator and engineering systems as well as the control system network which hosted the automation system running the controllers and peripherals driving industrial processes.

span the "air gap." Stuxnet infections have been traced to five different industrial companies within Iran, all of which dealt in ICS equipment and had been suspected of violating non-proliferation conditions. These domains were infected on multiple occasions with an average of nineteen days between malware compilation and the date of infection.[50] To infect these four sites, human saboteurs in place could have deliberately loaded malware from removable media like a USB memory stick. Alternately attackers could have used social engineering such as "spear phishing" emails disguised as communications from trusted colleagues to lure targeted users into clicking on fraudulent websites or running infected programs. More likely, a human agent provided infected media at a prior time and remote location to an unwitting employee who had access to the infection points.[51] "That was our holy grail," according to one of the American

[50] David Albright, Paul Brannan and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," Institute for Science and International Security (15 February 2011), 2. Symantec has not publicly released the names of these companies. Epidemiological data came from Stuxnet itself: as it copies itself from computer to computer, each instance keeps a log of all the machines infected by the lineage (evidence of developers interested in debugging or accountability). From samples of the worm collected in the wild, Falliere *et al*. traced a total 12,000 infections to five internet domain names, the names of which haven't been publicly disclosed. One of these domains was infected on three separate occasions, one was infected twice, two were infected only once, and one had three different computers infected at once (as if an infected thumb drive was repeatedly connected), for a total of ten known initial infections. There are three known versions of Stuxnet, but based on IAEA inspection data only the first version appears to have done any damage at Natanz. The three different compilations of Stuxnet attacked multiple sites in three waves: June and July 2009, March 2010, and April and May 2010. The IAEA observed that about 1,000 centrifuges were disconnected in January 2010, as covered later, but in subsequent inspections, the Iranians were already bringing them back under vacuum when the second and third waves hit. These second and third versions thus appear to have had no dramatic effect as the total number of enriching cascades began to increase after August 2010. Considering only insertions of the first version, Stuxnet's damage thus resulted from four initial infections, each in a different domain in Iran. The delay between compilation and infection could have been due to the logistic challenges of testing and getting the worm to the human agents who would launch the attack, or to internal bureaucratic processes within the attacking organization such as legal review. I assume that compilation, the process which packages human-readable programs into the executable binary file, occurred on computers at the attack's home facility, although remote compilation is technically possible. The attack waves, defined as the infections associated with a single compilation, are distributed across the ten initial infections: four, one, and five. The minimum time between compile and infect time was twelve hours, the next least was over six days, and the maximum was twenty eight days.

[51] Contractors might have been especially attractive as mules, as they could have unwittingly received the malware at tradeshows. Employees or contractors might also carry infected SIMATIC files directly to computers in the interior control system while performing maintenance, thus bypassing safeguards in the perimeter network altogether and vastly simplifying Stuxnet's infiltration. Alternatively, attackers could have sent phishing emails to employees with infected attachments which would open and drop the worm. See Byres et al, 13. A lot of attention has been paid to a zero-day vulnerability in Windows shortcut (.lnk) files which enables a hacked shortcut to surreptitiously load malware binaries as soon as the icon is simply viewed onscreen (MS10-046). This vulnerability appeared for the first time in the second version of Stuxnet, compiled on 1 March 2010. As I argue elsewhere, most

planners, “It turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.”[52] Iran did later report that it arrested “nuclear spies” in 2010 in connection with the worm.[53]

Exploiting Vulnerabilities

Once a human being dropped an executable binary file into a machine connecting to the ICS, then automated processes could perform further propagation and mischief.[54] Stuxnet has an impressive toolkit for replicating itself while remaining undetected. It can travel through different pathways via removable media or through shared network resources like print servers. Hiding and encrypting its files along the way, the worm varies its behavior depending on which type of antivirus software it encounters.[55] It exploits four zero-days (two of which escalate privileges to the administrator level), which by definition would not be defended, as well as several known vulnerabilities in case Iranian patches weren’t up to date.[56] Like a spy who enters a secure building with stolen bona fides, Stuxnet used two valid digital certificates from the Taiwanese firms Realtek and JMicron to install a rootkit (a program which can boot up with complete control over a machine). The rootkit detects tell-tale SIMATIC files and, using a

---

of the centrifuge damage attributed to Stuxnet occurred prior to March 2010; thus it might not have been the celebrated .lnk vulnerability which delivered the payload which actually did the work at Natanz. The first version of Stuxnet used a less sophisticated autorun.inf vulnerability to propagate via removable media (Falliere et al, 31-32).

[52] Sanger, “Obama Order”

[53] William Yong, "Iran Says It Arrested Computer Worm Suspects," *New York Times* (10 October 2010). Of course, Iran was likely to arrest anyone as a scapegoat after the fact, so we can’t put too much weight on this report.

[54] A binary file of executable machine instructions is more or less just like any other data file until an operating system loads it up and treats it as a program. Thus attackers need first to find a way to get their binary into the proper runtime context on target computers. All of Stuxnet’s functionality is packaged as a single 1.18 Mb library file (.dll). This file can export thirty-two different functions, each of which has a different purpose in controlling the worm for infiltration, communication, and sabotage, as well as other resource files these functions use.

[55] Upon being run on a host for the first time, the worm checks which type of antivirus program is protecting it—Symantec, ESET, McAfee, Kapersky, etc.—and then loads itself into a section of memory where that antivirus product wouldn’t look; if Stuxnet assesses that security can’t be bypassed, then that instance of the worm terminates.

[56] One of these zero-days turned out to have been employed previously by another criminal malware. It is not uncommon for zero-days to be used successfully in the field long before their discovery by defenders: Leyla Bilge and Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," *Proceedings of the19th ACM Conference on Computer and Communications Security* (16-18 October 2012).

compromised password Siemens had unwisely hardcoded into SIMATIC, injects its payload into SIMATIC control systems.[57]

As a commando team radios situation reports back to base, or as a spy communicates with a handler through dead drops and cutouts, Stuxnet attempts to communicate with particular servers on the open internet. The worm was instructed to upload reports describing the machines it infected and whether or not it had located SIMATIC software. These command and control servers could also send back instructions to implement remote procedure calls on the infected hosts or software updates from home base. Stuxnet was, of course, designed to penetrate through firewalls and into machines that would not have direct connections to the internet (*i.e.*, across "air gaps"). To facilitate command and control for such cases, instances of Stuxnet can also relay commands via a peer-to-peer network.[58]

The Payload

Stuxnet's infiltration toolkit exploited generic flaws in Windows to overcome uncertainties about Iranian networks. Its infiltration techniques have precedents in other malware like Conficker, although investigators were surprised to find so many integrated so well into one package.[59] Where Stuxnet truly broke new ground was with its targeted ICS subversion payload.

[57] Falliere et al.; Matrosov et al.

[58] *Ibid*. Stuxnet might loosely be described as a botnet, which is a collection of compromised hosts under control of a command and control server (some sophisticated botnets also communicate through peer-to-peer connections like Stuxnet). However, in this case each bot or zombie was also a worm, actively infecting the network in search of its target. The known Stuxnet command and control servers were hosted at www.mypremierfutbol.com and www.todaysfutbol.com in Malaysia and Denmark. These domains were registered through a domain name registrar in Arizona using a stolen credit card and false name. This is just one way in which nefarious activity can leverage infrastructure developed for legitimate activity and techniques pioneered by cyber-criminals.

[59] Conficker exploited a vulnerability (catalogued by Microsoft as MS08-067) as well as some generic malware techniques which were also used by Stuxnet.

The details in Stuxnet's code match hand-in-glove with the details known about Natanz from IAEA inspections.[60]

Once Stuxnet infects a SIMATIC machine, it verifies the presence of a particular type of programmable logic controller (PLC) connected to a particular type of frequency converter running at 807-1,210 Hz.[61] Iran was known to have had this type of PLC since 2003, and IAEA officials note that Natanz usually ran centrifuges slightly slower than the nominal rate of 1,064 Hz due of concerns about breakage. The maximum speed the IR-1 centrifuge rotor can mechanically withstand is about 1,400 Hz.[62] Stuxnet's attack code, accordingly, instructs the PLC to speed up to 1,410 Hz (near the IR-1 maximum speed) for 15 minutes, then return to 1,064 Hz (the IR-1 nominal speed) for 27 days, then slow down to 2 Hz (too slow to enrich) for 50 minutes, and then return back to normal at 1,064 Hz for 27 days; it then repeats the whole sequence indefinitely.[63] Even stronger evidence that Natanz was the intended target can be found in code for a secondary (and apparently unfinished) payload: this code defines arrays of 164 items organized into 15 irregular groups, which exactly matches the Natanz configuration of

[60] Early reporting in Fall 2010, prior to discovery of the Natanz attack sequence by forensic investigators, suspected that the Bushehr reactor was the target: Clayton, "Stuxnet Malware".

[61] Payload details are described by Falliere et al., 38-45, and Langner, "Stuxnet Attack Code Deep Dive." Stuxnet has three different command sequences, which Symantec calls A, B, and C. A and B are essentially the same, differing only in the type of frequency converter exploited. They will only run if it verifies that the PLC is a Siemens model S7-315-2 running a Profibus communications processor model 342-5 connected to a frequency converter manufactured either by Tehran-based Fararo Paya or Finland-based Vacon. Attack sequence C looks for a model S7-417 PLC and follows a quite different logic, although it appears to have not been fully implemented.

[62] David Albright, Paul Brannan and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges At the Natanz Enrichment Plant?" Institute for Science and International Security, 22 December 2010, 3-4. Iran is known to have obtained the 315-2 PLC by 2003, but the IAEA has been unable to verify the actual types of PLCs and frequency converters installed the FEP.

[63] Stuxnet's timing works not by interrogating the system clock but by counting reporting events generated by the PLC as it controls spinning motors, which is further evidence that Stuxnet developers knew and mastered FEP technical details.

15 enrichment stages in a cascade of 164 centrifuges.[64] The fit between attack code and Natanz infrastructure cannot be coincidental.

The primary payload's two-month loop appears to be designed to introduce chronic fatigue in the cascades rather than to simply break them in one violent shock. The secondary payload periodically opens and closes valves (in contrast to the primary sequence which speeds and slows rotors), apparently also to achieve chronic fatigue rather than catastrophic failure.[65]

In order for Stuxnet to chronically degrade enrichment at Natanz, the worm had to stay hidden while it sabotaged the ICS over the course of several months. Otherwise it would have been discovered and neutralized too early. Stuxnet remains hidden via a "man in the middle" attack, inserting itself between SIMATIC software and the PLCs in order to send modified commands to the PLC as well as disguise feedback back to the SIMATIC operator. Thus Stuxnet can mask alarms of breaking centrifuges. SIMATIC operators would thus have received deceptive feedback that centrifuges were spinning normally while they were actually speeding up and slowing down and generating alarms. This devious ploy resembles a Hollywood movie heist in which a loop tape distracts the guards while the burglars make off with the loot. It takes a varsity team of burglars to pull off such a caper; likewise, it takes a top rate technical and operational team to assemble Stuxnet's impressive bag of tricks.

---

[64] Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (Corrected)," *Science and Global Security* vol. 16 (2008): 1–25, describes that the Iranian cascade of 164 centrifuges "is characterized by a total 15 stages; the feed is introduced in stage 5, which consists of 24 machines" and "the product stream feeds into the next stage and the tails stream into the previous stage" in a symmetric arrangement of decreasing numbers of machines in each stage. This configuration can be verified in a publicity photo of President Mahmoud Ahmedinejad visiting the Natanz SCADA control room where, on one of the monitor screens, there is an image of an array of 164 items grouped into a symmetric arrangement of 15 clusters (http://www.president.ir/en/9172, accessed 18 April 2012). The parameters of the array pictured on the screen exactly match those in Stuxnet's code. Furthermore, there are six such arrays described in the code. Three Siemens S7-317 PLCs could control six cascades each, and this would amount to a total of 18 cascades, which is the number known through IAEA inspections to be contained in each of the eight planned enrichment modules in one of Natanz's production halls.

[65] Albright et al., "Stuxnet Malware and Natanz."

Testing the Cyber Revolution

Stuxnet's technical wizardry has encouraged belief in a Cyber Revolution. But how well does it really support conventional wisdom about asymmetry, offense-dominance, and deterrence failure in cyberspace?

A Weapon of the Strong

According to David Sanger's reporting in the *New York Times*, the worm was part of a sustained U.S. campaign of cyber operations against the Iranian nuclear program known as Olympic Games. The program began during the Bush Administration and accelerated under Obama. It featured collaboration with Israel for both operational and strategic reasons: the U.S. needed access to Israeli clandestine intelligence networks in Iran, and the U.S. wanted to dissuade Israel from launching an airstrike against Iran. Sanger reports that the actual technical work was carried out by the U.S. National Security Agency (NSA), an Israeli military signals intelligence outfit known as Unit 8200, and the attack was rehearsed at Israel's Dimona nuclear facility.[66] Stuxnet was clearly not a weapon of the weak.

As with any complex special operation, Stuxnet required a great deal of planning and support to successfully insert malware, control its infiltration, and perform target-specific actions on the objective.[67] Planners needed expertise in computer science, ICS and nuclear engineering,

[66] Sanger, "Obama Order"; David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012): 188-225; Broad et al, "Israel Tests on Worm". There appears to be general agreement that both the U.S. and Israel were involved, but it remains unclear which country was in the lead. For instance, Holger Stark, "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War," *Der Spiegel* (8 August 2011) reports that "Israeli sources familiar with the background to the attack insist…that Stuxnet was a…purely Israeli operation." Sanger's account of U.S. leadership is persuasive, but this remains an open historical question. For the purposes of my argument here, what matters is that the U.S. and Israel, whether together or alone, are militarily superior to Iran.

[67] This attack resembles a commando raid deep into enemy territory against superior forces as contrasted with the strategic bombing imagery of wide spread devastation to economic infrastructure that is often used to describe cyber

and covert intelligence operations in order to hack into Natanz. They would have to master the ICS configuration including its network architecture, its particular peripherals, the enrichment processes it controlled, the organizational management of the plant, and the ways in which the system was likely to degrade upon malfunction. The Bush Administration had substantially stepped up investment in Iran-focused intelligence, needed for the level of detail Olympic Games planners required.[68] This renewed emphasis built on American experience with industrial sabotage against Iran, such as a CIA operation in 2006 in which a Swiss family of engineers delivered defective equipment and caused fifty centrifuges at Natanz to explode.[69] Intelligence preparation for Olympic Games in particular began years before the Stuxnet attack with cyber reconnaissance to map out Natanz's networks.[70] The same intelligence networks useful for collection would also be useful for covertly inserting the malware into Natanz. In particular, the CIA's Information Operations Center, "second only to the agency's Counterterrorism Center in size…specializes in computer penetrations that require closer contact with the target, such as using spies or unwitting contractors to spread a contagion via a thumb drive."[71] The actual

warfare. See Lukas Milevski, "Stuxnet and Strategy: A Space Operation in Cyberspace," *Joint Forces Quarterly* vol. 63, no. 4 (2011): 64-69.

[68] Joby Warrick and Greg Miller, "U.S. intelligence gains in Iran seen as boost to confidence," *Washington Post* (7 April 2012)

[69] William J. Broad and David E. Sanger, "In Nuclear Net's Undoing, a Web of Shadowy Deals," *New York Times* (25 August 2008). In another sabotage operation from 2000, a CIA-backed Russian scientist provided flawed bomb designs to Iran: James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York, NY: Free Press, 2006), 194-212. CIA experience with industrial sabotage goes well back into the Cold War, notably a counterintelligence program to insert defective equipment to the Soviet "Line X" acquisition program: Gus W. Weiss, "The Farewell Dossier: Duping the Soviets," *Studies in Intelligence* vol. 39, no. 5 (1996).

[70] Sanger, "Obama Order", describes "a beacon that could be inserted into the computers." This may have been the Flame spyware which was publically discovered after Stuxnet but which had been active before it, and almost certainly a product of the same U.S.-Israeli collaboration: Ellen Nakashima, Greg Miller and Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post* (19 June 2012). An anonymous reviewer of this paper suggests that the intelligence used in for the 2007 National Intelligence Estimate on Iranian nuclearization was consistent with the sort of intelligence collected by Flame.

[71] Nakashima *et al*, "U.S., Israel Developed Flame"

human agents used for insertion may have been affiliated with the Mossad's proxy force in Iran, Mujahedeen-e-Khalq (MEK).[72]

The engineering effort alone was non-trivial. In order to evade network defenses, NSA developers had to be willing and able to employ several valuable zero-day vulnerabilities at once.[73] By virtue of being novel discoveries, zero-days would need to be carefully tested before they could be reliably integrated. No hacker writes perfect code the first time, and cyber planners are no exception. To engineer the ICS payload, developers would need access to IR-1 centrifuges, SIMATIC software, and the peripherals installed at Natanz, all set up in a mocked-up plant in order to test and debug their code and to rehearse the attack. In 2003 the U.S. had acquired a cache of Libyan P-1 centrifuges (essentially the same as the IR-1), and in 2008 Siemens cooperated with the Idaho National Laboratory to identify ICS vulnerabilities, so the U.S. surely had adequate test equipment.[74] Israel, moreover, could offer the Dimona complex for testing. It would be imperative to find and stamp out bugs that could compromise the whole operation (as one eventually did, in fact, by causing an Iranian machine to get stuck in a reboot loop). Anonymity and effectiveness are not just natural features of cyber attacks: they take a lot of effort to generate.

---

[72] Richard Sale, "Stuxnet Loaded By Iran Double Agents," *Industrial Safety and Security Source Blog*, 11 April 2012), http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/

[73] Once zero-days are discovered, software vendors work on patches and antivirus firms work on detection. Thus zero-days are extremely valuable prior to use (vendors interested in defense and criminals interested in offense are both willing to pay), but their value rapidly drops off after they are revealed. Holding onto a valuable zero-day for too long is risky, since if someone else discovers and publicizes it first, then the value is lost. These properties make markets for zero-days highly imperfect because it is difficult to credibly signal quality without giving away the goods. See Charlie Miller, "The Legitimate Vulnerability Market: Inside the Secretive World of 0-Day Exploit Sales," Workshop on the Economics of Information Security, June 7-8, 2007. Attackers with the R&D resources to find and secretly stockpile zero-days in-house can insulate themselves from this market somewhat.

[74] Broad, et al., "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." Siemens cooperation in SCADA penetration testing was ostensibly for defensive purposes, but the same research could be leveraged for attack planning.

The operation would further need program managers, operational planners, and commanders to oversee planning, financing, and monitoring of the years-long attack. Cyber warfare combines two challenging types of managerial complexity: procurement and operations. The former requires systems integration to design and integrate complex technological projects. The latter requires competent staff work to plan and execute real-time missions with lots of moving parts. Military and intelligence operations have been steadily getting more complicated for decades; states with oft-employed militaries like Israel and the U.S. have learned a lot of hard-won lessons managing (and failing to manage) both organizational and operational complexity. Moreover, any attacker worried about domestic and international legal constraints would also need lawyers to review compliance with covert action authorities and the law of armed conflict. As Richard Clarke, cybersecurity coordinator for the Bush administration, observed, Stuxnet's code to limit its propagation and discriminate its target exhibited hallmarks of an American covert action subject to legal controls.[75]

In sum, the Stuxnet operation required substantial time and institutional infrastructure. Sanger dates the origins of Olympic Games to 2006, which is consistent with forensic evidence that Stuxnet planning was in the works up to two years prior to the infections of summer 2009.[76]

---

[75] Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian* (April 2012). On installation the worm checks the current date and halts if it is later than 24 June 2012, which suggests that its designers expected the attack to be complete by then (this might also suggest a legal requirement to limit the lifetime of a covert operation). The first version of Stuxnet limited each instance to three infections, and each instance only had a 21 day window to infect others. If Stuxnet did not find SIMATIC files with the right configuration, it did not affect the functionality of the host and might even delete itself. Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair* (April 2011), quotes Richard Clarke: "If a government were going to do something like this, a responsible government, then it would have to go through a bureaucracy, a clearance process…Somewhere along the line, lawyers would say, 'We have to prevent collateral damage,' and the programmers would go back and add features that normally you don't see in the hacks. And there are several of them in Stuxnet. It just says lawyers all over it."

[76] Recent forensics on the "Duqu" worm, which was discovered after Stuxnet and appears to target Siemens SCADA for intelligence exploitation rather than sabotage attack, reveals that both malwares share provenance in a driver compiled in January 2008. See Alexander Gostev and Igor Soumenkov, "Stuxnet/Duqu: The Evolution of Drivers," Kaspersky Lab Securelist Blog, 28 December 2011,

The Bush Administration reportedly authorized $300 million for "joint covert projects" aimed at Iran's nuclear program, and these included cyber attack as a priority.[77] While this pricetag is small by the standards of modern weapons development, it does not include the substantial infrastructure, expertise, and experience already paid for and embodied in agencies like the NSA, CIA, and Mossad.

Some would argue, however, that the advent of Stuxnet itself has lowered the barriers to ICS attack. Stuxnet is a weapon which proliferates by the very nature of its viral infiltration, making free copies of its expensive code on every machine along the way. Decoded and annotated by forensic researchers, openly-available Stuxnet code now provides a tutorial on ICS attack.[78] This argument is misleading for two reasons. First, previously existing malware like Conficker and Zeus already provide as much of an infiltration tutorial as Stuxnet, which is a difference in degree, not in kind. Second, what the unique ICS attack payload actually shows is that precision targeted effects carry formidable requirements for specific intelligence and engineering expertise. There is still no general purpose round for cyberwar after Stuxnet. Moreover, Stuxnet also provides model code for defenders to study to learn how to increase the resilience of ICS. It has indeed generated a flurry of interest in the ICS and computer security communities. Barriers to entry for targeted, destructive ICS attack will thus remain prohibitive for all but states with long-established and well-funded cyber warfare programs.

---

http://www.securelist.com/en/analysis/204792208/Stuxnet_Duqu_The_Evolution_of_Drivers . Falliere *et al*., p. 3, estimated well before Sanger's scoop that engineering the attack "may have taken six months and five to ten core developers not counting numerous other individuals, such as quality assurance and management." This estimate even at the time appeared extremely conservative.

[77] Ewen MacAskill, "Stuxnet Cyberworm Heads Off US Strike on Iran," *The Guardian* (16 January 2011). Sanger, "U.S. Rejected Aid for Israeli Raid" reports that "The covert American program, started in early 2008, includes renewed American efforts to penetrate Iran's nuclear supply chain abroad, along with new efforts, some of them experimental, to undermine electrical systems, computer systems and other networks on which Iran relies".

[78] Ralph Langner, the investigator who deciphered Stuxnet's payload, often makes this argument, e.g., Tom Gjelten, "Security Expert: U.S. 'Leading Force' Behind Stuxnet," *NPR Morning Edition* (26 September 2011)

Steep barriers to weaponization aside, strong states are also better able to manage the strategic risks of failure. Any cyber attack, no matter how sophisticated, carries nonzero probabilities that the mission will be compromised, that the attacker's identity will be attributed, or that the payload will dud or miss its intended target altogether. Stronger powers have more resources to throw at minimizing these risks. They also have more resources to throw at maximizing the risks of would-be attackers; for example, they can spend a lot on network defense and they can mount serious investigations immediately after a major attack in order to search for attribution clues. Thus a weaker power that attacks the strong and fails at best does not improve its position and at worst opens itself up to punishing retaliation. However, a stronger power that attacks the weaker and fails has an insurance policy in the form of hard military power. Israel and the U.S. could experiment with a science project like Stuxnet because both states retained the military ability to inflict considerable harm on Iran if the operation failed. I will return to this important issue in the section on deterrence failure.

Stuxnet therefore suggests that the asymmetry argument of the Cyber Revolution thesis has it backwards. Cyber warfare is not a weapon of the weak. Weaker actors face steep barriers to weaponization for causing meaningful damage, and they are vulnerable to punishing retaliation if they somehow do succeed in injuring the strong. Strong states, by contrast, have the resources and risk-tolerance to wage cyber warfare against relatively weaker targets like Iran. These barriers to entry will tend to price weaker actors out of strategic cyber warfare. The technically and organizationally sophisticated level of play required for cyber warfare is generally beyond the capacity of a lone hacker, a small group of amateurs, or even organized

criminals, some of the favorite bogeymen of cyberwar discourse.[79] There are cheaper and more reliable ways for resource-poor terrorists or states to cause damage. While the potential global reach of cyber warfare would appear attractive for limiting the exposure of terrorists, that same distance forms a formidable barrier for intelligence preparation and operational control of targeted destructive attacks, without which the risks of operational failure become a serious liability for the weak. This emphatically does *not* mean that weak actors are priced out of irritant attacks for criminal gain, espionage, or political expression; on the contrary, the desirability of maintaining ability to engage in *sub rosa* exploitation is a big reason to avoid more severe forms of cyber attack which would mobilize unwanted attention. The difference in scale between strategic cyber warfare and cheaply available cyber irritants will become more apparent in the matter of offense dominance.

Offensive Fizzle

At a technical and tactical level, Olympic Games did indeed go right through Iranian network defenses, remaining undetected to make mischief for years. Mahmoud Ahmadinejad admitted that "They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts."[80] One Iranian study of antivirus software performance found that "none of the products can detect all various versions of the Stuxnet malware,"[81] and an Iranian official said that international sanctions were delaying mitigation

[79] It's always possible to think up scenarios whereby organized criminals in the hinterlands of Siberia might have assembled a mock up of Natanz to test their weapon, but this strains credibility.
[80] Albright et al., "Did Stuxnet Take Out 1,000 Centrifuges"
[81] Morteza Rezaei, "What's the Best Defense against Stuxnet? A Comparison of Which Tools are the Best for Finding Stuxnet in a System," Control Magazine Web Exclusive (28 May 2012), http://www.controlglobal.com/articles/2012/stuxnet-iranian-view.html

efforts.[82] However, the measure of success for defense against strategic cyber warfare is not just prevention of network intrusion but the blunting of infrastructure attack. Stuxnet's effects upon uranium enrichment proved minor and temporary. As a technical study from early 2012 concluded, "The attack set back Iran's centrifuge program for about a year, after which it largely recovered."[83] The ease of offense relative to defense must be assessed with respect the full range of actual circumstances that facilitate or hinder attack.

Stuxnet is generally credited with causing the Iranians to replace 1,000 centrifuges by January 2010 based on quarterly IAEA inspection data.[84] Yet the same data also shows that the rate of LEU production at Natanz *increased* from about 80 kg/month to about 120 kg/month during Stuxnet's attack window from mid-2009 to mid-2010. At best, Stuxnet thus produced only a temporary *slowdown in the increase* of the overall enrichment rate rather than a slowdown in the enrichment rate itself. Furthermore, IAEA inspections report no change in status to the most productive cascades at Natanz (module A24), while the 1,000 centrifuges observed disconnected were from cascades under construction (modules A26 and A28), running under vacuum but not filled with uranium hexafluoride gas.[85] This means that *the breakage during the*

[82] "Iran says Stuxnet virus infected 16,000 computers," *Associated Press* (18 February 2012). Other Iranian statements contradict this report: Mark Hosenball, "Experts Say Iran Has "Neutralized" Stuxnet Virus," *Reuters* (14 February 2012).

[83] Albright et al., "Preventing Iran from Getting Nuclear Weapons"

[84] The first known Stuxnet infections date to June and July 2009. Stuxnet was discovered in June 2010 and patched by August 2010 thanks to an international effort by the global commercial information security community that benefited Iran as well. Thus the Stuxnet attack lasted at most from mid-2009 to mid-2010. From May 2009 to August 2010 there were six IAEA inspections; these reports are available at http://www.iaea.org/newscenter/focus/iaeairan/iaea_reports.shtml (as of 20 April 2012).

[85] At Natanz in 2009-2010, a single separation cascade had 164 centrifuges, and eighteen cascades were grouped into operating modules. Iran had reported plans to install a total of eight modules in the main production hall at Natanz, but by late 2009 only three were installed to some degree. IAEA inspectors were able to record, for each module, how many were filled with UF_6 and thus enriching, how many were not enriching but under vacuum and ready, how many were installed but not under vacuum, and how many were disconnected altogether. Module A24 had been enriching with all eighteen cascades since 2008, while only had a fraction of the cascades of module A26 were enriching and no cascades of module A28 were performing any enrichment. Of these three modules, IAEA inspections only record damage to A26 during the Stuxnet attack window, and this damage was largely confined to centrifuges which were not yet filled with UF_6. A26 appears to have suffered serious problems in the latter half of

attack window appears to be limited to empty centrifuges. Lastly, while the total number of enriching centrifuges did not increase during the attack window, their numbers did begin to increase again by August 2010, by which time publically-available patches for Stuxnet were available.[86] In sum, Stuxnet missed the most valuable targets at Natanz, enrichment continued or improved throughout the attack, and the Iranians repaired the damage.

One can still argue that Stuxnet degraded long term efficiency by cutting into Iranian spares and raising error rates. As we have seen, the attack appears to have been designed to chronically degrade enrichment rather than halt it altogether. The difficulty in evaluating this type of performance is that Natanz was already a very inefficient operation, and for reasons that had nothing to do with the worm. The IR-1 centrifuge is a notoriously unreliable design. Stuxnet broke 11.5% of out of a total of about 8,700 centrifuges installed, but that's just barely above the normal 10% error rate reported by the IAEA.[87] Moreover, a trend of diminishing enrichment efficiency is visible from early 2008 (measured as a declining ratio of LEU output to feed gas), which predates Stuxnet. Ironically, because Stuxnet seems to have only damaged the empty centrifuges of module A26, the attack actually seems to have *improved* overall centrifuge efficiency. As the Iranians replaced centrifuges after the attack, overall efficiency at Natanz

2009. In June, twelve cascades were enriching, but in August there were only ten, and by November only six; this implies some chronic problem with enrichment. These non-enriching cascades in A26 all remained under vacuum during this time; then suddenly in January 2010, the IAEA found eleven cascades of A26 completely disconnected. Six of these were brought back under vacuum by May 2010, and after August the numbers of cascades actually enriching began to increase again. As a result, the most productive module online (A24) continued to enrich with all eighteen cascades. The newest module (A28) had sixteen cascades under installation and two being removed in January 2010, but Stuxnet is probably not to blame for those two since they weren't even spinning yet.

[86] Albright et al., "Did Stuxnet Take Out 1,000 Centrifuges"

[87] ISIS (*Ibid*.) states that the IAEA found about a thousand centrifuges disconnected, but IAEA reports simply mention eleven cascades disconnected during the January 2010 inspection, which, if fully loaded with 164 centrifuges each, would total 1,804 disconnected, a more impressive 20.7% of the total at Natanz. Perhaps not all of these eleven cascades were fully installed, or not all of their centrifuges were affected, leaving us the more modest thousand or 11.5%. We can take confidence that Stuxnet did indeed cause the breakage even with this lower amount—it wasn't just a stochastic jump above the normal 10% rate—because the damage was concentrated in module A26. In that particular module, the IAEA found as many as 60% of the non-enriching cascades abruptly disconnected, well above the 10% baseline. Moreover, this breakage was concentrated in a span of months, whereas the 10% baseline is an annual breakage rate. Stuxnet hit A26 hard, but it was A24 that was enriching the most.

again declined, no doubt exacerbated by chronic IR-1 problems that had nothing to do with Stuxnet.[88]

Stuxnet was surely intended to exploit these prior inefficiencies at Natanz. One American planner reportedly said, "The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence….The intent was that the failures should make them feel they were stupid, which is what happened….We soon discovered they fired people."[89] IAEA inspectors reported that "the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw."[90] Perhaps Stuxnet inflicted some additional friction on an already troubled program. However, the imperative for it to remain undiscovered amidst the noise placed an upper bound on the damage Stuxnet could inflict: too much and Iranians would know they were under attack. Anonymity enabled the attack, but maintaining anonymity imposed a restraint upon the attacker.

We cannot really explain the worm's fizzle until more data emerges, but we can look for likely stories in what we know about complex organizations in general. Natanz, like any industrial facility, was not just an assemblage of technical equipment, but also a human

[88] Might overall enrichment efficiency at Natanz have been even more degraded had Stuxnet never attacked at all? The cumulative ratio (total product and feed over time) of kg LEU to kg UF_6 from 5% improves from early 2008 to a peak of 9% at the end of 2009, and then, right after the height of Stuxnet activity, gradually diminishes. At first blush this appears to be evidence for Stuxnet effectiveness. However, a more disaggregated (non-cumulative) measurement of the monthly ratio tells a quite different story. From nearly 10% (kg/month LEU per kg/month UF_6) in early 2008, efficiency declines gradually to under 8% in August 2009; but it then *jumps* suddenly to over 10% in November 2009, only to decline gradually again to 8% by September 2011. A similar story can be told with a different efficiency measure, that of average separative work per year per centrifuge. Efficiency declines from the beginning of plant operations until the beginning of Stuxnet attacks, then increases into early 2010, only to decline again after August 2010. Stuxnet in effect provided a "reset" to the inefficient drift of the non-cumulative ration and the average separative work; alternatively (as an anonymous reviewer has pointed out), Stuxnet acted as a quality control measure for Iran by removing inefficient centrifuges. Either way, in the absence of this bump in efficiency, the ultimate performance could have been even worse. Technical details are drawn from David Albright and Christina Walrond, "Performance of the IR-1 Centrifuge At Natanz," Institute for Science and International Security, 18 October 2011.

[89] Sanger, "Obama Order"

[90] *Ibid.*

organization. One sociological study of large scale corporate data systems describes "the unfinished, the untidy, the irregular, and the hack as fundamental systems practices."[91] Idiosyncratic processes are essential for coping with the "data friction" in interfaces between humans and instruments and between different parts of a large enterprise.[92] These embedded practices are often poorly understood even by the members of an organization, much less cyber planners a continent away. Given that Iran was subject to a strict sanctions regime, it surely procured some of its equipment from unorthodox sources, or jury-rigged parts of its systems with available local resources. Stuxnet looked for specific Finnish and Iranian peripherals, but there are indications Natanz may also have relied on German and Turkish parts which Stuxnet would have ignored.[93] The IAEA has never been able to inspect Iranian ICS or closely observe its operators in action, so it's unknown how well the actual plant configuration and practices matched Siemens best practices. Divergence of local idiosyncratic practices on the factory floor from documented ones could have invalidated targeting intelligence based on formal schematics. If Stuxnet's code and Iran's facts diverged at some critical decision point, then Stuxnet would have just sat inert on computers at Natanz, exactly as it did on every other machine around the world that didn't trigger its payload.

It is true that deviation from organizational standards can lead to "normal accidents" in a system that is too complex to understand.[94] Indeed, mishaps like Sayano-Shushenskaya help to

[91] Claudio Ciborra, *The Labyrinths of Information: Challenging the Wisdom of Systems* (New York, NY: Oxford University Press, 2002), 3; See also Susan Leigh Star, "The Ethnography of Infrastructure," *American Behavioral Scientist* vol. 43, no. 3 (1999): 377-391;

[92] Paul N. Edwards, Matthew S. Mayernik, Archer L. Batcheller, Geoffrey C. Bowker and Christine L. Borgman, "Science Friction: Data, Metadata, and Collaboration," *Social Studies of Science* vol. 41, no. 5 (2011): 667-690.

[93] Albright, et al., "Did Stuxnet Take Out 1,000 Centrifuges," 6

[94] The risks of complexity have spawned a vast literature, *inter alia*, Charles Perrow, *Normal Accidents: Living with High Risk Technologies* (Princeton, NJ: Princeton University Press, 1999); Scott Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq* (Princeton, NJ: Princeton University Press, 2000); Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago, IL:

inspire belief in the Cyber Revolution. Yet by the same token, if complexity makes accidents hard to foresee, then it also makes it hard for remote attackers to understand targets perfectly enough to cause predictable mishaps at will. Clauswitzian "fog" and "friction" bedevil any military attack, and cyber operations are no exception.[95] Furthermore, organization theorists have contrasted the resilience of "high reliability organizations" with the fragility of "normal accidents" to describe how social groups develop ingenious yet undocumented ways of coping with friction in order to keep things running.[96] At a national level, Germany during World War II was famously able to increase industrial output in 1943 under intense Allied bombing by dispersing factories and relying on synthetic substitutes. If the target system can absorb and compensate for strategic attacks, then the long term impact is blunted.[97] Thus complexity can not only foil the attacker's planning, but also provide the defender with resources to cope with everyday breakdowns. Counterintuitively, if Natanz had messy workplace practices, it might have had inadvertent defenses.[98] As Sanger notes of the Natanz ICS, "The connections were

---

University of Chicago Press, 1997); Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton University Press, 1993).

[95] One might argue that friction is even more problematic for cyber warfare than other operations. Unlike a human commando team which can rely upon their intuition and ingenuity to recognize and adapt to unforeseen problems, malware has only explicit rules and coded assumptions to guide it. Malware that communicates through command and control servers doesn't solve this problem because the remote operator remains deeply unaware of actual machine states, details of real time network configuration, and the activities of local users *in situ*. Even if the payload manages to reach its target, there is no guarantee that the target equipment and organization will react as attack planners expect, or on the anticipated timelines.

[96] Karl E. Weick and Karlene H. Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly* vol. 38, no. 3 (1993): 357-81; Karl E. Weick, "Organizational Culture as a Source of High Reliability," *California Management Review* vol. 29, no. 2 (1987): 112-27

[97] Lawson, "Cyber Doom," reviews studies of societies which experience natural and military disasters; scholars find that such societies, especially if they have high social capital, are likely to display altruistic tendencies and to organize themselves to restore services. Ironically, given the cyber war emphasis on the vulnerability of advanced industrial states, such societies are more likely to have the social resources to compensate for disaster.

[98] Computer security engineers usually deride "security through obscurity" in the belief that a determined hacker always finds a way through, or that lazy users who ignore security can easily be exploited. Although *cf.* Andrew Odlyzko, "Providing Security With Insecure Systems," ACM Conference on Wireless Network Security, March 2010. The argument here is that obscurity in embedded practice of the larger socio-technical system, not just the narrow computer system, can enhance security.

complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail."[99]

Another much less speculative boost to Iran's defenses was provided by open-source security researchers around the world. The existence of a global, open-source, information security community raises attacker costs and lowers defensive costs. The Belarusian discovery launched a flurry of excitement in online technical communities and soon Symantec from California, ESET from Slovakia, and Langner Communications from Germany were all reverse-engineering the worm. Virginia-based Verisign revoked the certificates Stuxnet used, Washington-based Microsoft issued patches for its zero-day vulnerabilities, the U.S. Computer Emergency Readiness Team issued advisories, and Germany's Siemens reached out to its SIMATIC customers with online advice and patches.[100] When Stuxnet was first discovered, its purpose and target was unknown; Stuxnet was just the most recent species of malware to threaten internet hygiene. Despite its propagation controls, Stuxnet still spilled out of Iran to provide the information security community with plenty of samples to investigate.[101] Computer security experts tend to be aggressive in dissecting newly discovered malware. Once vulnerabilities are understood, the malware can usually be neutralized. With antivirus analysis and vendor patches posted online for free, Iran could in effect outsource part of its

[99] Sanger, "Obama Order"
[100] Falliere, et al., 4; Zetter, "How Digital Detectives Deciphered Stuxnet"
[101] Symantec (Falliere et al., 5-7) monitored two of Stuxnet's command and control servers they had discovered and found that they were in communication with 100,000 infected hosts in over 30,000 organizations by the end of September 2010. One third of these infections were outside of Iran. Indonesia and India were a distant second and third in Stuxnet infections. Despite some panic over Stuxnet that it might have harmed an Indian satellite and a British reactor, the remaining global third of infections seems not to have caused any damage beyond the costs of investigation and clean-up. Stuxnet was looking for a SIMATIC configuration peculiar to Natanz, so it remained relatively inert as it spread elsewhere. Of course, the fact that two-thirds of the infections *were* in Iran is an important clue, along with the specifics of the payload discussed later, that Iran was the intended target. This count of 100,000 infected hosts probably severely undercounts the true number. Symantec only found and monitored two command and control servers; there could have been others. Furthermore, many infections would have been in peer-to-peer botnets without direct connections to those servers.

counterintelligence investigation at no cost.[102] Furthermore, for the attacker, compromise to the computer security community can mean the end of the operation. Covert operation, and the work it takes to maintain, is not just a luxury in such cases but a requirement.

According to offense-defense theory in international relations, "war is far more likely when conquest is easy, and…shifts in the offense-defense balance have a large effect on the risk of war."[103] One potential explanation for the relative absence of strategic cyber warfare in the historical record is that cyber offense at this level is not actually stronger than defense. Cyber warfare against critical infrastructure may face more formidable defenses than generally appreciated. Another explanation is that the causal relationship between the cyberspace offense-defense balance and strategic warfare is ambiguous. The most contentious debate over general offense-defense theory has focused on whether it is possible to measure the offense-defense balance at all, to include whether it should encompass just technology or also some combination of doctrine, manpower, resources, territory, and even diplomacy.[104] Critics have noted that the same weapons can be employed in different contexts or at different levels of war: e.g., entrenchment can provide tactical cover during operational offensives, and tanks can support

[102] Because it is almost impossible to measure computer security, anti-virus firms compete by producing free threat analysis to advertise their technical competence. I am grateful to Stefan Savage for this point.

[103] Stephen W. Van Evera, "Offense, Defense, and the Causes of War," *International Security* vol. 22, no. 4 (1998): 5-43, p. 5. Karen Ruth Adams, "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance," *International Security* vol. 28, no. 3 (2003): 45-83, attempts to assign offensive or defensive valences directly to military technology over the past two centuries and finds that states are statistically more likely to attack or be conquered in offense dominant eras. Adams' statistical result is challenged—suggesting the perils of coding technology directly for offense or defense apart from use context—by Yoav Gortzak, Yoram Z. Haftel and Kevin Sweeney, "Offense-Defense Theory: An Empirical Assessment," *Journal of Conflict Resolution* vol. 49, no. 1 (2005): 67-89. The key articles in this debate are collected in Michael E. Brown, Owen R. Coté Jr. Michael E. Brown, Sean M. Lynn-Jones and Steven E. Miller, eds., *Offense, Defense, and War* (Cambridge, MA: MIT Press, 2004).

[104]Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* vol. 22, no. 4 (1998): 44-82; James W. Davis, Jr., Bernard I. Finel, Stacie E. Goddard, Stephen W. Van Evera, Charles L. Glaser and Chaim Kaufmann, "Taking Offense at Offense-Defense Theory (Correspondence)," *International Security* vol. 23, no. 3 (1999): 179-206

counterattacks during operational defensives.[105] Moreover, defenses that can be easily defeated tactically can be reinforced by threats of strategic retaliation which make offensive aggression unwise. Technology alone does not determine the offense defense balance. An organization's ability to employ weapons in particular operational and strategic circumstances is critical.

The popular belief in the offense dominance of cyberspace should be recalibrated to the scale and ambitiousness of attack under consideration. Some weapons are costly to master. Some targeting objectives are difficult to realize. Some attacks are risky due to potential retaliation. It is notable that the vast majority of attacks by internet miscreants are individually insignificant. Cybercriminals, for instance, exploit highly standardized resources (millions of computers running identical applications, homogenous entities like credit card accounts and user credentials, billions of email transactions) to create stereotyped attacks. Most of their attacks fail most of the time, but they can still profit on the aggregate because the set of potential victims is so large. By contrast, to cause a predictable level of damage to a particular ICS target, the cyber warrior has to tailor the attack to a more heterogeneous assemblage of people and machines. Errors there are more likely to lead to irreversible mission failure. Although low-intensity cyber attacks exploiting homogenous assets do have certain advantages over technical defenses, high-intensity cyber attacks exploiting heterogeneous complexity have to overcome some serious obstacles. This distinction may help to explain why Stuxnet's infiltration phase was, in retrospect, so much more effective than its payload phase: the former targeted homogenous

[105] Richard K. Betts, "Must War Find a Way? A Review Essay," *International Security* vol. 24, no. 2 (1999): 166-198; Keir A. Lieber, *War and the Engineers: The Primacy of Politics Over Technology* (Ithaca, NY: Cornell University Press, 2005). To take just one of countless examples, detailed by Earl J. Hess, *The Rifle Musket in Civil War Combat: Reality and Myth* (University Press of Kansas, 2008), the rifled musket is often credited with significantly enhancing the lethality of defense during the American Civil War. However, because of poor training, the cluttered nature of Civil War battlefields, and its parabolic arc of fire, it caused no real improvement compared to smoothbores. Skirmishers and snipers were better able to exploit the rifled musket's potential, but they composed less than 4% of the infantry on either side.

Windows machines to move copies of code around, but the latter targeted more particular equipment to cause physical destruction.[106] Even infrastructure which appears superficially standardized and homogenous, such as cascades of centrifuges and networks of routers, is often supported by the heterogeneities of workplace practices, human interventions, and nonstandard local equipment.[107]

Weaponization in cyberspace is a complex project, and the degradation of infrastructure is rife with uncertainty. An offensive cyber planner must not only determine that an attack is possible because of internet and ICS vulnerabilities, but also be able to confidently rule out that myriad unforeseen circumstances will not defeat it. More precise specification of scope conditions of offense dominance in cyberspace is much needed in order to distinguish situations where technically undetectable cyber attacks can result in political or economic gain from situations where the complexity of the system provides holistic advantages to the defense. To put it somewhat glibly, cyberspace may be offense dominant for criminals and spies, but not for soldiers.[108] This task is necessarily left open; my goal here is simply to undermine the assumption of categorical offense dominance in cyberspace.

---

[106] Although a degree of homogenization in the centrifuge cascades did facilitate the engineering the payload in the first place, the potential uncertainties of the physical plant were much greater. Stuxnet's covert yet promiscuous propagation enabled it to burrow deep into the network without advance knowledge of the best route to the centrifuges. The homogeneity of Windows operating systems on Iranian hosts enabled the worm to use the same tricks again and again to perform a random walk through Iran's networks. If it reproduced enough copies of itself, then eventually some of them would get to the right place and Stuxnet's handlers would receive feedback of mission progress. Yet even these tricks did not deal with all the frictions Stuxnet encountered. Viral propagation enabled Stuxnet to cope with uncertainty about Iran's network configuration, but it ultimately led to the compromise of the operation.

[107] Greg Downey, "Virtual Webs, Physical Technologies, and Hidden Workers: The Spaces of Labor in Information Internetworks," *Technology and Culture* vol. 42, no. 2 (2001): 209-235

[108] Of course, there are areas where soldiers can exploit offense dominance in cyberspace, especially in those operations such as intelligence reconnaissance or psychological influence operations where soldiers behave more like spies or hacktivists. Specification of scope conditions could also help to identify a more narrow set of ICS targets and situations (e.g., surprise attack vs. protracted war) where cyber warfare might be more feasible.

The Effectiveness of Deterrence

I have so far argued that there are operational barriers to entry for strategic cyber warfare which discourage weak actors from attempting, and which frustrate strong actors from easily succeeding in, attacks on complex infrastructure. One strategic consequence of recognizing the real obstacles involved in cyber attack is the improvement of deterrence by denial, the threat of successful defense. Assume for the sake of argument that operational difficulties will eventually diminish (although, in reality, they will probably tend to increase as the sociotechnical world continues to grow more complex). Thus weak actors will be able to cheaply weaponize cyberspace, and cyber weapons will be able to easily overcome complexity. Deterrence by denial then becomes prohibitively expensive. Potential victims would then have to rely on deterrence by punishment, the threat of costly retaliation. Unfortunately, according to the Cyber Revolution thesis, retaliatory threats are not credible when cyberspace assures anonymity.[109]

At first blush, it appears that deterrence failed in this case. The U.S. launched a destructive cyber attack, and American culpability remained ambiguous for a long time, i.e., until Sanger's story broke in June 2012, a year and a half after Stuxnet was discovered. Additional Olympic Games malware like Duqu and Flame was later discovered to have been lurking anonymously in Iranian networks for many years prior. Other Iranian infrastructure such as oil terminals also appears to have suffered cyber attack from malware related to Olympic Games.[110] Furthermore, the U.S. appears to have been unable to deter Iranian cyber retaliation: allegedly

[109] On the difference between deterrence by punishment and denial (or defense) see Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Westport, CT: Greenwood Press, 1961), 14-16. I henceforth use "deterrence" to refer to the threat of retaliatory punishment.

[110] Nakashima et al., "U.S., Israel Developed Flame"; Thomas Erdbrink, "Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals from Internet," *New York Times* (23 April 2012).

Iran launched DDoS attacks against U.S. banks and sent data-wiping malware against Saudi Aramco computers.[111] Deterrence thus failed to stop a cyberwar.

An alternative interpretation of these same facts is that cyber attack can be an indication of *successful* deterrence rather than its failure. The question turns on whether deterrence is understood in terms of preventing the means or the effects of attack, *i.e.*, whether we focus on measures to prevent cyber attacks for the sake of cyber hygiene, or to prevent an unacceptable use of force that may or may not use cyber tools. A narrowly technological emphasis on preventing any sort of hacking whatsoever fails to distinguish irritant attacks from cyber warfare or to recognize the substantial potential for variation in the intensity of ICS attack. What really matters to statesmen is the political consequence of cyber attack, not the mere fact of cyber attack. Strategic actors will weigh the potential political benefits against the expected dangers of any aggressive move, eschewing those that seem too hazardous. In this interpretation, successful deterrence can lead strategic actors to choose cyber means when other options are deemed too risky, and furthermore, to restrain the intensity of their cyber attacks in order to avoid retaliation or blowback by whatever means.

The U.S. sought to halt Iran's nuclear program, but it also desired to avoid sparking a new war while already fighting two costly and unpopular wars on Iran's borders with Iraq and Afghanistan. With the intelligence failure regarding Iraqi weapons-of-mass-destruction still fresh in American minds, the domestic case for a kinetic strike was hard to make. Moreover, the prospects of Iranian mining in the Strait of Hormuz, Hezbollah terrorism, and a wider regional escalation were (and remain) distinctly unsavory. A covert option like Olympic Games to delay

[111] Ellen Nakashima, "Iran Blamed for Cyberattacks on U.S. Banks and Companies," *Washington Post* (21 September 2012); Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times* (23 October 2012)

nuclearization and buy time for diplomacy and sanctions to work would be an attractive alternative to American policymakers, but only if they believed also avoid the domestic and international audience costs of seeking public support for action against Iran. One problem, however, was that Israel was even more determined to prevent Iran from getting the bomb. Dead set against allowing a hostile nuclear power in its neighborhood, Israel had already demonstrated a willingness to use force to disrupt nuclearization in Iraq in 1981 and in Syria in 2007. In 2008 Israel reportedly asked for American assistance with aerial refueling, provision of bunker-busting munitions, and permission to overfly Iraq; the U.S. refused, and then the Israeli Air Force rehearsed strike routes over the Mediterranean that exactly matched the distance to Natanz.[112] The U.S. thus needed a way to dissuade Israel from acting rashly to spark the very war it hoped to avoid. Close collaboration between them on Olympic Games would offer the U.S. some hope of credibly conveying to Israel a reason for military restraint.[113] In sum, the U.S. was deterred from overtly striking Iran but also sought to reassure Israel, so the together they opted to experiment with cyber warfare.

In practice, however, the decision to wage cyber warfare is not so simple because the uncertainties can be debilitating. As General Hayden recalls, "I have sat in very small group meetings in Washington…unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of any decision we might make."[114] Reportedly, Obama "repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons—even under the most careful and limited circumstances—could enable other countries, terrorists or hackers to justify their own attacks….

[112] David E. Sanger, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site," *New York Times* (10 January 2009)
[113] Sanger, "Obama Order"
[114] Quoted in Nye, "Nuclear Lessons for Cyber Security?", 18

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region."[115]

The risky uncertainties of cyber warfare led Olympic Games planners to take their time, test carefully, probe cautiously, and, importantly, to limit the severity of their attack. Stuxnet's payload was designed to subtly stress centrifuge cascades for months on end, not to create catastrophic damage in a single knock-out blow. Stuxnet also had to have modest aims just to remain in place making mischief. Aggressive proliferation and breakage might have alerted Iranian operators to shut down the line, leading to early discovery of Stuxnet, collateral damage, and other unintended consequences. Deterred by the prospect of uncertain consequences, the U.S. pulled its punches with Stuxnet. The worm was never intended to be a decisive intervention to halt Iranian enrichment: "one participant said the goal was simply to 'throw a little sand in the gears' and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort."[116] Olympic Games was designed to expand the president's options, but ironically, it could not expand them too much or create too dramatic an outcome.

If an actor is deterred from taking overt action, then covert action is attractive, but only if the fiction of plausible deniability can be maintained. The "attribution problem" is thus not only a headache for the defender, but also a liability for an attacker who insists on anonymity or deniability. The cloak of anonymity is usually cast as an advantage for the attacker, but it is also a burden to bear if there are real costs associated with compromise or loss of control. As a conspiracy adds more people and more moving parts, the probability rises that someone involved

[115] Sanger, "Obama Order"
[116] Sanger, "Obama Order"

will make a mistake. For example, the Russian authors of a Facebook virus called Koobface left many traces across the internet about their cars, pets, and wives that enabled independent investigators to identify them by name and location.[117] The attribution problem is often considered to be the major obstacle to cyber deterrence, but detection and attribution are hardly impossible.

Stuxnet was compromised by a bug in a new version of its code. It spilled beyond Natanz, eventually infecting over 100,000 machines worldwide, including Chevron's corporate networks in the U.S.[118] These errant worms were not dangerous—Stuxnet was programmed to ignore all but its target ICS—but they did provide plenty of material for investigators. Network defenders contained the threat, computer security researchers tore apart the code, vendors issued patches, and antivirus firms updated their signatures. Anonymous malware can seem dangerous, but malware that is not anonymous can readily be neutralized. In the aftermath of compromise, forensic investigators searched for clues left in code artifacts and behaviors. Tehran's chief negotiator referred to an internal Iranian investigation, saying "I have witnessed some documents that show…their satisfaction in that [U.S. involvement]."[119] Not all of the clues, moreover, need be technical features of the attack itself. The broader political context and intelligence reporting

[117] Jan Drömer and Dirk Kollberg, "The Koobface Malware Gang Exposed," SophosLabs, 2012. An illustrative example outside of the cyber realm is the assassination of a Hamas official in a Dubai hotel which was captured in embarrassing detail in 648 hours of security camera footage; Emirati police reportedly discovered the names and photographs of eleven European-passport holders in the bumbling hit team, believed to be Mossad, effectively retiring them forever as covert operatives. Danna Harman, "Dubai Assassination Spotlights Top Cop Skills in a Modern-Day Casablanca," *Christian Science Monitor* (19 March 2011). Brenner, *America the Vulnerable*, narrates this same episode in a chapter entitled, "spies in a glass house." In the same book Brenner also endorses the familiar idea that offense is easy in cyberspace, which seems to contradict this argument that counterintelligence—that is, defense—is also easier in the information age.

[118] Rachael King, "Stuxnet Infected Chevron's IT Network," *Wall Street Journal* (8 November 2012). Sanger, "Obama Order", reports that Stuxnet escaped "like a zoo animal" when an ICS operator plugged an infected laptop into an external network. Sanger's depiction is somewhat at odds with Stuxnet's sophisticated methodology for infiltration in search of the ICS, as described above.

[119] Interview with Saeed Jalili on NBC News, "Iran's nuclear negotiator says U.S. involved in cyberattack," aired 17 January 2011, available at http://video.msnbc.msn.com/nightly-news/41124888#41124888. Of course, for all the reasons in this paragraph, Iran would have good reason to suspect the US, so the reliability of Iranian statements should be discounted. We don't know just what sort of evidence they may or may not have found.

also provides circumstantial evidence. Shortly after the public discovery of Stuxnet, speculation soon settled on the US and/or Israel. Once the level of technical sophistication was appreciated and publicized by the computer security community, worries about lone hackers and terrorist gangs could be ruled out for want of means. States with cyber warfare capacity such as Russia or China lacked convincing motive, although some tried to make the conspiratorial case.[120] Israel and the U.S., by contrast, were well-endowed with both means and motive.[121] The investigative journalists cited throughout this paper soon began to assemble circumstantial evidence for a persuasive case. Experts like Richard Clarke freely opined, "I think it's pretty clear that the United States government did the Stuxnet attack."[122]

Like offense dominance, the attribution problem—and thus deterrence failure—appears to be sensitive to scale. The more consequential the attack, the more effort will be invested into investigating the attacker. One reason why most cyber attacks are safely anonymous is because they are inconsequential crimes that do not mobilize the full investigative capacity of the state. For instance, we see plenty of spam for fake pharmaceuticals but no spam pushing schedule II drugs. Criminals are deterred from energizing a more aggressive law enforcement response. It is true that some cyber attacks cannot be deterred, but that is because the attacker is actively

[120] Chris Demchak, "Stuxnet: Signs Could Point to Russia," New Atlanticist Blog, 26 November 2010, http://www.acus.org/new_atlanticist/stuxnet-signs-could-point-russia; Jeffrey Carr, "Dragons, Tigers, Pearls, and Yellowcake: Four Stuxnet Targeting Scenarios," Taia Global Executive Cyber Protective Services, 16 November 2010

[121] Some early speculation of Israeli responsibility for Stuxnet turned on conspiratorial interpretations of artifacts in the code. Falliere, et al. speculate (p. 24) that a hard-coded path in the Stuxnet driver (b:\myrtus\src\objfre_w2k_x86\i386 \guava.pdb) could be a coded reference to the Book of Esther which relates the deliverance of Jewish people from destruction in the Persian Empire, and (p. 18) that a hard-coded value causing the worm to halt (19790509) could be a reference to the date the first Jew was killed by firing squad by the new Islamic government in Tehran. They caution that these provocative and dubious interpretations could also be false flags inserted to implicate Israel. Another curiosity in the code which excited conspiracy theorists was the value "0xDEADF007" in Stuxnet's PLC payload.

[122] Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian* (April 2012)

seeking that threshold in order to avoid it. Attackers who hope to do real damage cannot take anonymity for granted.[123] And that means they must also take the risk of retaliation seriously.

Reported Iranian cyber retaliation for Stuxnet, although the details are sketchy, obeys the same logic. The DDoS attacks against U.S. firms were irritants with little international political consequence or impact on corporate performance. The Shamoon virus which reportedly wiped data from over 30,000 Aramco computers and displayed anti-American propaganda appears to have been the unsophisticated work of a nationalist hacker.[124] Iranian hackers could lash out without truly injuring America as long as they calibrated their attacks to things they could get away with. Yet fear of even these sort of irritant cyber reprisals surely worried Stuxnet planners and led them to pull their punches. If we observe evidence of deliberate restraint in the severity of cyber attacks, as we do with Stuxnet as well as Iranian retaliation, then we have an indication that deterrence between two political actors is actually working. That is, modest cyber attacks may occur because more severe and consequential attacks do not.[125] The difference between the U.S./Israeli and Iranian attacks is that the greater relative power of the former pair over the latter provided the luxury to experiment with a whole different magnitude of cyber attacks: hard military power provided insurance against retaliation and a coercive fallback plan in case *sub rosa* cyber warfare failed.

[123] Keir A Lieber and Daryl G. Press, "Reading the Return Address: Assessing the Danger of Anonymous Terrorist Attack," Paper presented at the Annual Meeting of the American Political Science Association, Seattle, September 2011

[124] Michael Riley and Eric Engleman, "Code in Aramco Cyber Attack Indicates Lone Perpetrator," *Bloomberg* (25 October 2012)

[125] This dynamic recalls the stability-instability paradox of classical nuclear deterrence theory: nuclear deterrent stability can promote limited conventional instability.

Conclusion

Stuxnet is the only historical instance of strategic cyber attack and thus the only empirical opportunity to test conventional wisdom about cyber warfare. By and large, the Cyber Revolution thesis flunks the test. The worm was a technical marvel but it did not have lasting effect on Iranian enrichment. The additional friction imposed on the program was cheap and hardly a waste of effort—a marginal increase in friction in the Iranian program is surely preferable to bombing and probably better than doing nothing—but it was not a revolutionary coup. While mediocre performance degradation is better than nothing for those actors who can afford it, enthusiasm for the technical characteristics of the attack divorced from acknowledgement of its slight effects is misplaced as an argument for the strategic potency of cyber warfare.

Just because trivial attacks are easy to mount in cyberspace does not mean that consequential infrastructural attacks are also easy. Even when costs do scale up for the attacker, it does not mean costs must scale up even faster for the defender. Technical or tactical offense dominance may enable an attacker to penetrate a network, but it does not translate into strategic offense dominance against the infrastructure and social systems in which computers are embedded. In fact, the complexity, heterogeneity, and interdependence between technical and human processes can provide a degree of resilience for the defense as attacks scale up. Cyber warfare has to inflict disruption which rises beyond an organization's baseline level of considerable everyday friction and social compensation to even make a difference, yet doing so risks blowing the covert anonymity on which the attack depends. Ironically, the defender doesn't really have to work for the benefits inherent in the very complexity of the defended system (although there are certainly things a state can do to improve resiliency and redundancy). Cyber

attack to cause significant physical damage is very difficult to weaponize and execute, and so major cyberwar (whatever that looks like) may in fact be defense dominant.[126] Conversely, operations that have very modest goals—especially exploitations that aim only to steal information quietly or agitate in online forums—have a much easier intelligence and target response problem to deal with. Better identification of the conditions under which socio-technical complexity creates resilience or brittleness in a system targeted by cyber warfare is topic deserving of further research.

It is of course difficult to generalize from a single case. Perhaps Stuxnet was just an early and imperfect experiment, and the Cyber Revolution is still impending. Most historical RMAs are preceded by lackluster periods of trial and error. The first military aircraft were impressed into observation roles by the Army Signal Corps, and it took several decades for the technology and doctrine of strategic bombing to mature. When the British introduced tanks at Cambrai, they did not produce a blitzkrieg revolution; the machines were unreliable and they were not integrated via radio with aircraft and infantry into a combined arms team.[127] Likewise, future cyber attackers might one day work out the bugs, perfect the doctrine, and produce more decisive results. Even the dramatic detonation of atomic bombs in Japan did not instantly produce a revolution in doctrine and strategy, for it took several years for states to accommodate nuclear weapons as something other than just big conventional bombs.[128]

---

[126] A dangerous situation, recalling the WWI context of original debate on offense-defense theory, would be if an actor believed cyberwar was offense dominant when it was really defense dominant. Stephen W. Van Evera, "Offense, Defense, and the Causes of War," *International Security* vol. 22, no. 4 (1998): 5-43. This misperception is certainly not helped by most of the rhetoric on the topic.

[127] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca: Cornell University Press, 1991); MacGregor Knox and Williamson Murray, eds., *The Dynamics of Military Revolution, 1300-2050* (New York, NY: Cambridge University Press, 2001)

[128] Francis J. Gavin, *Nuclear Statecraft: History and Strategy in America's Atomic Age* (Ithaca: Cornell University Press, 2012) argues that even afterward the Nuclear Revolution lacked the clarity often assumed. Throughout the Cold War, there was something of gap between the strategic consequences theorists expected from the Nuclear

Yet Stuxnet is unlikely to be a harbinger of major RMA. The problems Olympic Games planners encountered—in weaponization, target complexity, and deliberate restraint—will likely become even more pronounced in the future. Increasing sociotechnical complexity in states, firms, and militaries is one of the great global trends of the last two centuries. The latest internet phase of the information revolution is only a difference in degree not in kind regarding the growing complexity of control of industrial and military operations.[129] With greater complexity there are more places to hide, but also more ways to leave clues. With greater complexity there are more things that can go wrong with a plan and foil deterministic computer code. The strongest states have the most experience managing information system complexity through their trials with combined arms force employment and large scale systems integration, and so they will be best able to integrate complex cyber operations in supporting roles. Strong states also have hard power insurance policies for when cyber operations fizzle. Deterrence will not be fundamentally changed if there will not be a credible possibility of unattributable, offense-dominant, catastrophic attacks from weak actors.

Although there is unlikely to be a Cyber Revolution, cyber operations will, nonetheless, likely become a normal component of international relations in the future. The misplaced exuberance of cyberwar rhetoric should not lead us to discount emerging developments altogether. Sloppy language that conflates war and cyber operations is not helpful, for there remain many interesting mysteries about cyber phenomena to occupy scholars and policymakers alike. Further innovation involving cyberspace will continue to fill out the low end of adversarial interaction in ever more complex ways, facilitating political and industrial espionage as well as

---

Revolution and the more pragmatic concerns of policymakers. A similar gap appears to be opening for the Cyber Revolution.

[129] James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press, 1986)

attempts to influence domestic interest groups across international borders. States will have to deal with the increased noise and friction caused by their dependence on cyberspace, and militaries will have to cope with a boggling range of options for managing the electromagnetic environment across their entire spectrum of operations. The professional militaries of strong powers will retain the advantage in integrating cyber complements into their battlefield operations. The professional intelligence services of strong powers will offer expanded options to policymakers to provide a slight marginal advantage in foreign relations. Although cyber warfare it will continue to mature as a complement to conventional military and intelligence operations, it will prove to be a temperamental and unreliable strategic instrument on its own. Even as political actors will explore new technical possibilities, the strategic uncertainties and operational complexities of the cyber instrument will encourage them to exercise restraint.