War Logs On: A Critical Approach to the Frontiers of Cyber Warfare

by

Lidia Frech

B.A. (Honours), Simon Fraser University, 2004

PROJECT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF ARTS

in the
Department of Political Science
Faculty Arts and Social Sciences

SIMON FRASER UNIVERSITY

Summer 2011

Approval

Name: **Lidia Frech**

Degree: **Master of Arts of Political Science**

Title of Thesis: ***War Logs On: A Critical Approach to Frontiers of Cyber Warfare***

Examining Committee:

Chair: David Laycock, Professor, Department of Political Science

---

Douglas Ross
Professor, Department of Political Science
Senior Supervisor

Anil (Andy) Hira
Professor, Department of Political Science
Supervisor

Patrick Smith
Professor, Department of Political Science
Internal Examiner

Date Defended/Approved: August 23, 2011

Declaration of
Partial Copyright Licence

Abstract

Militaries are developing defensive and offensive operational capabilities in cyberspace. This paper examines the unique characteristics of cyber weapons to understand the security challenges and strategic implications posed by them. A case study analysis of Stuxnet is explored to reveal the complexities associated with both deploying and defending against cyber attacks. The findings indicate that cyber attacks are well suited for covert campaigns. Secondly, cyber weapons will likely play an auxiliary or subsidiary aspect of military campaigns using traditional kinetic technologies. Alarmist discourse surrounding cyber threats is tempered by logistical and technical feasibility of carrying out attacks. However, fears of “cyber doom” and the inability to attribute the source of attacks are destabilizing factors in the context of nuclear deterrence relationships and crisis stability.

Keywords: cyber weapons; cyber war; strategic stability; covert operations; Stuxnet

Acknowledgements

I sincerely thank Dr.Doug Ross for his incredible mentorship and words of motivation throughout my years here as a graduate student. Thank you for the many discussions and suggestions on this project. I am grateful for the time and support that you provided to me on this rather winding graduate studies journey. It is with your assistance and commitment that I was able to see the project to completion. I warmly thank the remaining members of my examining committee Patrick Smith and Andy Hira for their insightful feedback that pushed me to reflect and re-consider my assumptions regarding the topic.

To my mom, for the gift of life and all that you have given in your life for me. I am thankful. To Chung, for all things good and wonderful under the stars. To my friends Anya and Jennifer for their boundless and unwavering support. To Simon, for your “peculiar” sense of humour and your friendship.

Table of Contents

Chapter 1.

Introduction

> This new form of warfare has several implications that are only now becoming apparent, and that will define the shape of what will likely become the next global arms race-albeit one measured in computer code rather than firepower.[1]

In May 2011, the Pentagon announced that it has developed a list of formally approved cyber weapons capabilities to employ against adversaries. The classified list of capabilities includes a "toolkit" of attack methods to infiltrate and map foreign networks to examine their functions and operations, the ability to deposit "beacons" for future targeting by viruses, and computer viruses that can sabotage an adversary's critical networks.[2] The development and use of cyber attack capabilities is enshrouded within classified and covert programs. This secrecy complicates conceptualization and understanding of the significance and ramifications of the operational use of cyber attacks in armed conflict.

The lack of an intellectual framework regarding the strategic uses and implications of cyber weapons is analogous to the period of uncertainty and strategic novelty of the early 1950s and the nascent debates on nuclear weapons.[3] Cyber attacks

1 Richard Falkenrath, "From Bullets to Megabytes," *New York Times*, January 26, 2011, http://www.nytimes.com/2011/01/27/opinion/27falkenrath.html (accessed July 8, 2011).

2 Ellen Nakashima, "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare," *Washington Post,* May 31, 2011.

3 Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," *The RUSI Journal* Vol. 155. no.6 (December 2010): 18. Samaan observes that the nuclear analogy is used to "emphasise the low level of existing knowledge on the strategic implications of cyber attacks."

are being actively pursed by nations and yet the policy and scholarly discourse surrounding their use has yet to take place. A military response to cyber threats frames interpretation of cyber incidents and limits and shapes the range of responses that may be marshalled to deal with them.

To date, the literature on cyber warfare has not addressed the strategic implications of the use of cyber attacks in armed conflict and the potentially destabilizing effects they may have on nuclear deterrence relationships. The purpose of this project is to examine the unique characteristics of cyber attack capabilities to understand the security challenges and strategic implications posed by them.

In Chapter Two I establish that governments are pursuing cyber attack capabilities and that cyberspace is emerging as a realm of military contestation. I focus on the embryonic contours of U.S. Cyber Posture and examine the roles, missions and capabilities that U.S. armed forces are developing in cyberspace. Working within the boundaries of publicly available unclassified information I examine the tangible steps the U.S. has taken to institutionalize and develop offensive and defensive capabilities in cyberspace. The U.S. military discourse on cyberspace is worth examining at length as the approach the U.S. adopts to operating in cyberspace has ramifications for the way other governments develop their own cyberspace policies. Deibert notes that other countries, namely those closely allied with the U.S. "have to fall in step as a function of being closely engaged on an operational level with the U.S. military."[4] Indeed this development is confirmed by General Keith Alexander, Commander of United States Cyber Command and Director of the National Security Agency, who observes that the recent creation of Cyber Command has garnered a great deal of attention from foreign

[4] Ronald Deibert,"Tracking the Emerging Race in Cyberspace," *Bulletin of the Atomic Scientists* Vol. 67, no.12. (Jan/Feb 2011): 2. Further, Deibert and Rohozinski argue: "the leading superpower provides a model for similar developments in other states' armed forces, who feel the need to adapt or risk being left behind." Ronald Deibert and Rafal Rohozinski, "Liberation Vs. Control," *Journal of Democracy* Vol. 21, no.4 (October 2010): 49.

militaries and many governments are contemplating the creation of their own cyber commands.[5]

In chapter three I examine the cyber threat debate surrounding the disruptive and destructive potential of cyber attacks. Visions of "cyber doom" roused by the lightning "click of a mouse" have remained within the realm of the hypothetical yet continue to surface in security debates in the U.S. The analytical discord that marks the cyber threat literature produces a disjointed picture surrounding the nature, scope and gravity of cyber threats. I explore the alarmist discourse surrounding cyber attacks and demonstrate that cyber doom scenarios are largely exaggerated and implausible based on an assessment of cyber threats grounded within technical and logistical considerations. While visions of "cyber doom" are unlikely to materialize the alarmist cyber narrative plays a decisive role in prescribing and justifying an encroaching military role for "securing" cyberspace. In the context of stable nuclear deterrent relationships, the prospect of "cyber doom" may induce panicked responses and risks of escalation in a crisis scenario.

In chapter four I examine the unique characteristics of cyber attacks in a case study analysis of Stuxnet to illuminate some of the complexities of both using and defending against cyber attacks. Stuxnet demonstrates that cyberspace is a medium in which it is difficult to ascertain not only who an attacker is but also whether it is an attack at all. Cyber attack effects are marked by many uncertainties including potential for collateral damage. The ability to develop such attacks in secret, plausible deniability surrounding attack attribution and the ability to conduct such attacks without "boots on the ground"[6] make them suitable instruments for use in covert campaigns. When viewed

[5] Gen. Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* (Summer 2011): 7., http://www.au.af.mil/au/ssq/2011/summer/alexander.pdf (accessed June 7, 2011). Alexander maintains that this does not entail a militarization of cyberspace but rather concern over "current problems" and development of defensive improvements to counter threats.

[6] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities* (Washington D.C.: The National Academic Press, 2009), 2.

in the context of nuclear and WMD deterrent relationships the use of secret cyber attack capabilities and the inability to attribute the source of a cyber attack has potentially destabilizing and corrosive implications for the maintenance of stable mutual deterrent relationships.

In chapter five I explore the strategic ambiguities and implications surrounding cyber attacks and demonstrate that stable nuclear deterrence is put at risk by the development of offensive cyber capabilities. A comparison of cyber attacks to nuclear and biological weapons of mass destruction (WMD) is undertaken to highlight the unique characteristics of cyber attacks in order to understand the security challenges posed by them. I conclude that cyber attacks share many parallels with biological weapons that render traditional arms control and deterrence strategies largely ineffective in containing cyber threats. The use of nuclear analogies to explain cyber weapons capabilities complicate rather than explain the strategic implications of cyber attacks. In part two I argue that cyber war is not likely to be an independent form of warfare. I establish that cyber attacks will likely be a subsidiary or auxiliary aspect of military campaigns using kinetic technologies. However, the development and diffusion of offensive cyber attack capabilities may have potentially disintegrative effects on strategic stability between nuclear-armed nations. The auxiliary use of cyber attacks to degrade and confuse command and control will “densify” the fog of war and may provoke panicked escalation across the nuclear threshold. Cyber attacks are secretly deployed, they may be difficult to detect and their effects are not certain. Fears surrounding “secret cyber capabilities” may inject panic and confusion into a crisis between nuclear powers and provoke pre-emptive or preventive war. The potentially destabilizing effects of cyber attacks on strategic stability reaffirm that sustained nuclear disarmament initiatives must be pursued with greater resolve.

Parameters of Inquiry

In this section I discuss the definitional and methodological parameters that inform this paper. Attempting to assess threats emanating to and from cyberspace requires a definition of this concept. Many definitions of cyberspace abound and there is no agreed upon consensus in media and scholarly discourse regarding how to define

cyberspace. Kuehl identifies several threads that link proposed definitions of cyber space including: "the role of electronics, telecommunications, infrastructures, and information systems."[7] Considering the focus of this discussion is on U.S. Cyber Posture, I employ the definition of cyberspace put forth by the US Department of Defense. According to the National Military Strategy for Cyberspace Operations (2006) cyberspace is defined as: "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures."[8] This definition acknowledges that cyberspace is a broader realm than the Internet.

In this discussion I employ the definition of cyber attack developed by the U.S. National Research Council: "Cyber attack refers to the use of deliberate actions-perhaps over an extended period of time-to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[9] This definition conceptually separates cyber attacks from cyber espionage although the two are closely related. Both require the successful exploitation of system or network vulnerability the only difference is that cyber attacks leave a disruptive or destructive payload. Cyber espionage obtains information "resident on or transiting through an adversary's computer systems or networks" but does not seek to "disturb the normal functioning of a computer system or network from the user's point of view."[10] Cyber espionage may be used to reconnaissance and map a system for cyber attacks to follow.

7 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds. Franklin D.Kramer, Stuart H.Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 25.

8 Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 27.

9 National Research Council, *Technology, Policy, Law and Ethics Regarding the U.S. Acquisition and Use of Cyber Attack Capabilities*, 10.

10 National Research Council, *Technology, Policy, Law and Ethics Regarding the U.S. Acquisition and Use of Cyber Attack Capabilities*, 10-11 and 20.

Chapter 2.

The Contours of American Cyber Posture

Cyberspace is emerging as a sphere of political and military contestation. States are developing and refining capabilities and doctrines for fighting wars in cyberspace.[11] Rohozinski and Deibert observe: "most of the world's armed forces have established, or are in the process of establishing, cyber commands or cyber warfare units."[12] According to the Center for Strategic and International Studies, a number of nations, including the U.S., U.K, Russia, China and Israel have the capability to wage cyber war and will use such capabilities in the event of a conflict; at least another 30 militaries intend to acquire advanced cyber-attack capabilities.[13] Deibert and Rohozinski note that while the securitization of cyberspace has been driven by a "defensive agenda" to protect critical infrastructure and fight cyber crime alternative perspectives emphasize the pursuit of offensive posture and capabilities.[14] Sommer and Brown assert that the deployment of

[11] Deibert, "Tracking the Emerging Arms Race in Cyberspace," 2. According to Deibert the militarization of cyberspace refers to "the growing pressures on governments and their armed forces to develop the capacity to fight and win wars in this domain." Cyberspace is becoming militarized and weaponized as governments develop and refine Cyberwar capabilities. Deibert is the Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs at the University of Toronto. He is a principal investigator with the OpenNet Initiative and the Information Warfare Monitor. Deibert has published extensively on Internet censorship, surveillance and information warfare.

[12] Deibert and Rohozinski, "Liberation vs. Control in Cyberspace,"49.

[13] James Lewis, "The Cyber War has not Begun," *Center for Strategic and International Studies* (March 2010), http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf (accessed June 25, 2011) and James Lewis, "Cyber Attacks, Real or Imagined, and Cyber War," *Center for Strategic and International Studies* (July 11, 2010), http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war(accessed June 25, 2011).

[14] Deibert and Rohozinski, "Liberation vs. Control in Cyberspace,"49.

cyber weapons is “already widespread” and used individually, or in combination with conventional kinetic weapons as a force multiplier, in an extensive range of circumstances. They predict that the use of cyber weaponry will become “ubiquitous.”[15]

These developments represent a marked shift in the way nation states approach cyberspace; a largely “laissez faire” approach to the regulation and operation of the Internet has shifted to the pursuit of strategic and foreign policy interests in cyberspace.[16] The evolution of cyberspace as a domain within which to wage war is linked in the literature reviewed to the inherent vulnerabilities and opportunities for subversion that accompany the inexorable emergence and ubiquity of information technology as an indispensable component of modern life.

Historically information technology in the military domain was treated as a force enabler. During the Cold War American strategic planners envisioned that the numerical might of Soviet conventional forces would be offset by superior American technology that multiplied combat effectiveness.[17] Information technology enables almost everything that modern militaries do including logistical support, command and control of forces, provision of intelligence and remote operations capabilities.”[18] The military dimension of the cyber threat debate recognizes that the technological superiority, central to the Revolution in Military Affairs (RMA)[19,] and the bulwark of American conventional and nuclear military superiority, is now a perceived source of vulnerability.

15 OECD, *Reducing Systemic Cybersecurity Risk*, prepared by Peter Sommer and Ian Brown (14 January, 2011), 6, http://www.oecd.org/dataoecd/3/42/46894657.pdf (accessed March 12, 2011).

16 Ronald Deibert, “Cyber Security: Canada is Failing the World,” *Huffington Post Canada,* May 26, 2011, http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html (accessed August 23, 2011).

17 Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge: New York, 2008): 43.

18 International Institute of Strategic Studies, *The Military Balance 2011*, Vol. 111, Issue 1(2011): 5

19 The term originated in Soviet discourse in the early 1980s when they realized they were suffering an emerging and calamitous IT gap vis a vis the Americans.

The core theme in cyber "warfare" literature emphasizes that enmeshing the operations of infrastructure, commerce, and national defense and military operations within cyberspace engenders vulnerabilities and risks that will inevitably be exploited by a range of state and non-state actors. The responses to rising concerns over the vulnerability of national information and communication technology systems have gradually become entrenched within the military domain; it is militaries that are "developing capabilities for assessing, countering and, presumably, prosecuting operation in cyberspace."[20]

Cyber "weapons" remain unknown until used and offensive military postures and capabilities remain largely classified. This presents a complex challenge to analyzing the "cyber "weapons" capabilities that states are developing. In their assessment of the military dimensions of cyberspace, the International Institute for Strategic Studies recommends tracking organizational development as a useful starting point for looking at the resources nations are mobilizing to prosecute offensive and defensive operations in cyberspace.[21] The U.S. has taken tangible steps to institutionalize military operations in cyberspace through the creation of a Cyber Command and the inclusion of "manoeuvrability" in cyberspace, articulated in armed forces doctrines, to ensure and bolster force projection of kinetic military capabilities. Working within the parameters of publicly available information, this discussion provides only a partial picture of U.S. cyber "weapons" capabilities. It does establish that operations conducted in cyberspace are indispensable components of U.S. military capabilities and missions.

[20] International Institute for Strategic Studies, *The Military Balance 2011*, 5.
[21] International Institute for Strategic Studies, *The Military Balance 2011*, 27.

In May of 2010, the U.S. Department of Defense established U.S. Cyber Command (USCYBERCOM or CYBERCOM)[22] with the express mission to plan, coordinate, integrate, synchronize and conduct activities to:

> Direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[23]

U.S. Deputy Secretary of Defense William Lynn III describes the creation of Cyber Command as a logical organizational development to consolidate a "loose confederation of joint task forces dispersed both geographically and institutionally" to effectively address the gravity and scale of the cyber war threat to U.S. national security and the U.S. economy.[24] The stated focus of Cyber Command is to assist troops in the field in limiting their vulnerabilities in and from cyberspace.

Hughes argues that the creation of a formal command and control infrastructure signifies intention to acquire and employ offensive cyber attack capabilities.[25] Full spectrum operations include defensive, offensive, stability and support operations. It is not further elaborated what type of denial strategies or tactics, noted in the mission statement, will be utilized apart from affirmation that such activities will be executed within applicable juridical boundaries.

22 US Department of Defense, "*U.S Cyber Command Fact Sheet,"* (May 25, 2010), http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf (accessed December 28,2010). Cyber Command is a joint organization that includes components from all services namely the Army Forces Cyber Command, the US Navy Fleet Cyber Command, the 24th Air Force and the Marine Corps Forces Cyberspace Command.

23 U.S. Department of Defense, "*U.S. Cyber Command Factsheet."*

24 William J. Lynn III, "Defending a New Domain*," Foreign Affairs* (Sep/Oct2010), http://web.ebscohost.com.proxy.lib.sfu.ca/ehost/detail?vid=3&hid=18&sid=c1d46fd6-6440-42ae-9a55-b5c9ed99568b%40sessionmgr4&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=aph&AN=52957873 (accessed August 23, 2011).

25 Rex Hughes, "A Treaty For Cyberspace," *International Affairs* 86:2 (2010): 530.

Jackson speculates that the creation of USCYBERCOM may indeed be a response to Russian and Chinese activities in the cyber domain.[26] In both Russia and China there is concern that "the US is seeking to achieve in cyberspace the same dominance it is perceived to have in the realms of conventional and nuclear weapons, and space."[27] The perception of Russian and Chinese analysts is that the mission goal of cyber dominance "narrows the diplomatic leverage of the United States, reduces the ability to foster partnerships in other cyber security areas" and contributes to the radicalization of responses from China and Russia to the perceived technological superiority.[28]

Further, the U.S Department of Defense identifies cyberspace as a new domain of warfare that is as critical to military operations as land, sea, air and space. The Deputy Secretary of Defense stresses the ubiquitous use of information technology to enable almost everything the U.S. military does.[29] While the digital infrastructure gives the U.S. "critical advantages" over its adversaries, the reliance on computer networks allows adversaries to gain intelligence about U.S. capabilities and operations, to impede U.S. conventional military forces, and to disrupt the U.S. economy.[30] The Pentagon's cyber strategy underscores that cyber threats are not limited to military targets but endanger critical infrastructure. Software and hardware are at risk of being tampered with at point of manufacture and industrial espionage and theft of commercial

26 Patrick Jackson, "Meet US Cybercom: Why the U.S. is fielding a Cyber Army," BBC News, 15 March 2010, http://news.bbc.co.uk/2/hi/8511711.stm (accessed September 14, 2010).

27 Jackson, "Meet US Cybercom: Why the U.S. is fielding a Cyber Army."

28 Franz Stefan Gady, "Lost in Translation: Doctrines and Diplomatic Efforts in Cyberspace," *Huffington Post*, May 11, 2011,http://www.huffingtonpost.com/franzstefan-gady/lost-in-translation-doctr_b_864760.html (accessed June 4, 2011). Gady further notes that the U.S. doctrine of cyber dominance only applies in military situations and in times of war. It is comparable to the NATO doctrine of air supremacy defined as "that degree of air superiority wherein the opposing air force is incapable of effective interference."

29 Lynn III, "Defending a New Domain." The list of information technology enabled functions include logistical support and global command and control of forces, real-time provision of intelligence, and remote operations. According to Lynn the military's "global communication backbone" consists of 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries.

30 Lynn III, "Defending A New Domain."

information could erode U.S. military effectiveness and competiveness in the global economy. The mention of "sustained intellectual property loss" from private sector corporate entities is significant as it establishes cyber attacks against such entities as threats to national security and within the scope and purview of the military domain. It is unclear how the Pentagon intends to deal with "sustained intellectual property loss" and what type of Department of Defense policies will emerge to counter industrial and commercial espionage. The movement of "industrial espionage" from the private sector to a national defense concern may elevate the importance of such activity into the murky realm of "cyber warfare" and consequently define the range of feasible options that determine how to counter such threats.

The Pentagon emphasizes three characteristics of cyber war including asymmetric advantage for adversaries,[31] offense dominance of cyber weapons and the futility of Cold War deterrence models to counter cyber threats. The strategy is replete with reference to robust defenses around military networks but silent in regard to any offensive operations the U.S. is developing and pursuing in cyberspace. This is a curious omission considering the strategy identifies cyberspace as an offense dominant environment in which the structural features of the Internet make highly probable that the U.S. government's ability to defend its networks always lags behinds its adversaries' ability to exploit weaknesses.

A number of US military service groups function under the auspices of USCYBERCOMMAND and each is developing capacity to operate in cyberspace. The most recent US Air Force Cyberspace Operations doctrine emphasizes the importance of cyberspace to operations in all other domains and freedom of action in cyberspace to enable command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities. The Air Force doctrine notes that control of

[31] Lynn III, "Defending a New Domain." The Pentagon's cyber strategy notes that many militaries are developing offensive capabilities in cyberspace to take advantage of the relatively low costs of developing cyber weapons, vis a vis the cost of conventional military capabilities.

cyberspace is integral to its mission and the ability to gain and maintain superiority in cyberspace is essential to "deliver global reach, power, and vigilance."[32] US military strategic superiority in the domain is assured using an integration of skilful personnel and the "integration of offensive and defensive cyberspace operations."[33] The doctrine notes that code writing can be a form of logical manoeuvre in cyberspace akin to the manoeuvring of forces to gain positions of advantage in air, land, space and maritime domains. The challenge in cyberspace is that attacks that are delivered at cyber speed "give little or no time for human reaction, especially if such reactions involve several layers of decision making."[34] Attacks can be masked so that it is difficult to determine who is doing what to whom and it is difficult to determine what has been damaged considering services may remain functional while information content is changed.[35]

The mission assurance prerogatives of the doctrine are to ensure "the availability of a secured network to support military operations by assuring and defending the portion of the network directly supporting the operation." The strategy recognizes that operating in cyberspace is linked to other operational domains that facilitate interdependent defensive, exploitative, and offensive operations to achieve situational advantage.[36]

The U.S. Army's Cyberspace Operations Concept Capability Plan 2016-2028 strikes a similar chord to goals espoused by the Air Force doctrine with the addition of seeking to retain freedom and to deny the same to its adversaries in both cyberspace and the electromagnetic spectrum. Cyber operations are emphasized as an integral part of full spectrum operations and include activities "prevalent in peacetime military

[32] United States Air Force, *Cyberspace Operations, Air Force Doctrine Document 3-12*(15 July 2010), *Forward,* http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf (accessed September 15, 2010).

[33] United States Air Force, *Cyberspace Operations, Air Force Doctrine Document 3-12*, 7.

[34] Robert Miller, Daniel Kuehl and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Forces Quarterly* Issue 61, Second Quarter (2011): 21.

[35] Miller et al., "Cyber War: Issues in Attack and Defense," 21.

[36] United States Air Force, *Cyberspace Operations, Air Force Doctrine Document 3-12*,10.

engagement."[37] The doctrine emphasizes "unprecedented levels of adverse activity in and through cyberspace threaten the integrity of the United States critical infrastructure, financial systems, and elements of national power."[38] The doctrine identifies several operational challenges including the inability to "identify, attack exploit, and defeat the expanding cyber-electromagnetic threats or mitigate the increasing vulnerability of its own networks."[39] The army doctrine makes specific reference to the component of cyber operations that extends "cyber power" beyond the defensive boundaries of the Global Information Grid (GIG) to detect, deter, deny and defeat adversaries.[40] The Air Force and the Army's doctrinal visions emphasize that military outcomes can be determined by cyber operations alone although generally they are not an end to themselves but an integral part of full spectrum operations.[41]

At time of writing, the US Navy is yet to publish a formal cyber strategy. However, its Naval 2010 concept notes that naval forces achieve sea control by "neutralizing or destroying threats in the maritime, space and cyberspace domains that constrain our freedom to manoeuvre, conduct follow-on missions, or restore maritime security."[42] The strategy predicts that adversaries will conduct space and cyberspace attacks to negate U.S. abilities to command and control forces. To counter such threats, the US naval forces will "deploy and employ redundant systems to maintain command and control of

37 United States Army, *Cyberspace Operations Concept Capability Plan 2016-2028* (22 February 2010), v, http://www.fas.org/irp/doddir/army/pam525-7-8.pdf (accessed September 15, 2010).

38 United States Army, *Cyberspace Operations Concept Capability Plan 2016-2028*,6.

39 Ibid.

40 United States Army, *Cyberspace Operations and Concept Capability Plan 2016-2018*, 69. The Global Information Grid refers to the "globally interconnected, end to end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to war fighters, policy makers, and support personnel."

41 United States Army, *Cyberspace Operations Concept Capability Plan 2016-2028*, 7.The Army's Cyber doctrine stresses that commanders conduct cyber operations to retain freedom of action in cyberspace and thereby enable other operational activities.

42 United States Navy, *Naval Operations Concept 2010: Implementing the Maritime Strategy: US Navy Operations Concept,* 2010, 53, http://www.navy.mil/maritime/noc/NOC2010.pdf (accessed September 15, 2010).

dispersed forces in the face of such threats, and will maintain proficiency in retaining the operational and tactical initiative when communications and information systems are degraded or denied."[43]

In July 2011, the Department of Defense (DoD) published its first strategy for operating in cyberspace. The strategy is worth examining at length to discern how the U.S. will enable and exploit the capabilities of cyberspace while protecting and defending against vulnerabilities. The strategy outlines DoD's reliance on, and continued growth and expansion of, cyberspace-enabled capabilities to operate and fulfill mission objectives.[44] The global scope of DoD networks and systems provides opportunity for exploitation and attack.

Secondly, the document emphasizes that the private and civilian sector, specifically integrated critical infrastructure, may be vulnerable to disruption and exploitation by hackers and foreign governments that may cause damage to U.S. national and economic security. DoD links the security of civilian infrastructure to its functions by noting that its operations are dependent on this critical infrastructure.[45]

Thirdly, the strategy emphasizes the asymmetric nature of the cyber threat characterized by low barriers to entry for malicious activities that can potentially cause significant damage. The strategy is focused on external threat actors, insider threats, supply chain vulnerabilities and threats to DoD's operational capabilities. The Department of Defense identifies foreign nations are working to exploit DoD unclassified and classified networks; it is unclear whether exploit in this context means probe,

[43] United States Navy, *Naval Operations Concept 2010: Implementing the Maritime Strategy: US Navy Operations Concept,* 54.

[44] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (July 2011),1, http://www.defense.gov/news/d20110714cyber.pdf (accessed July 16, 2011). The Department of Defense uses cyberspace "to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations."

[45] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* 1.

espionage, or attack.[46] Conflating a range of diverse phenomena under a catch-all banner can elevate the importance and significance of events along with the requisite responses that such a label may imply.

The strategy is largely based on preparation for hypothetical future threats emanating from suppositional capabilities that have not yet materialized.[47] Importantly, the document lacks a declaratory policy regarding offensive cyber attack capabilities save for the statement that the Department of Defense "oppose(s) those who would seek to disrupt networks and systems, dissuade and deter malicious actors and reserve the right to defend these vital national assets as necessary and appropriate." [48]

An examination of these doctrines and policies reveals that cyberspace is an integral part of broad-spectrum military operations however the development and use of offensive cyber capabilities remains classified and unexplained. Importantly basic information regarding what constitutes an attack and what the range of "appropriate" responses is to such attacks is left undefined. Ambiguity and speculation in regard to intentions, motivations and perceived capabilities may lead down the path of inadvertent and unintended escalation in a crisis scenario.

[46] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* 1.

[47] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* 2-4. The strategy outlines that: some foreign intelligence organizations have already *acquired the capacity* to disrupt elements of DoD's information infrastructure and that non state actors *increasingly threaten* to penetrate and disrupt DoD networks and systems. There may be malicious activity that DoD has *not yet detected* and "evidence grows of adversaries *focusing on the development* of increasingly sophisticated and potentially dangers capabilities." In addition DoD outlines that software and hardware are "at risk" of malicious tampering at point of design, manufacturing and service and "potential adversaries may seek to exploit, disrupt, deny, and degrade the networks and systems that DoD depends on for its operations."

[48] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*,10.

Chapter 3.

The Cyber Threat Debate

> The best-laid defenses on military networks will matter little unless our civilian infrastructure is also able to withstand attacks.[49]-William Lynn III, Deputy U.S. Defense Secretary

The policy and scholarly literature reviewed resounds with concern that cyber attacks will be unleashed on critical infrastructure by a medley of both state and non-state actors. However, in the absence of major destructive events to draw experience from, debates surrounding cyber threats are shaped by narratives about future events and potential cyber warfare capabilities.[50] Consequently, there is much analytical discord in regard to the nature, scope and gravity of cyber threats.

In part one of this chapter I establish that the ubiquitous use of and inextricable dependence on information technology in modern society, to power its economic, political and military organs, will be exploited as both a tool and target of attacks. Secondly, I provide a basic outline of the contours of the "cyber doom" narrative that informs policy and scholarly assessments of the destructive potential of cyber attacks. I conclude with analysis of arguments provided by "cyber-skeptics" who bemoan the

[49] Jim Wolf, "The Pentagon's New Cyber Warriors," *Reuters*, October 5th, 2010, http://www.reuters.com/article/2010/10/05/us-usa-cyberwar-idUSTRE69433120101005 (accessed January 12, 2011).

[50] Ralf Bendrath, "The American Cyber-Angst and the Real World-Any Link?" in *Bombs and Bandwidth*, ed. Robert Latham (New York: The New Press, 2003): 51.

"selling of cyber doom"[51] and elucidate technical and logistical considerations that underlie and temper cyber attack capabilities.

The "pervasiveness" and "importance" of infrastructure to the function of states make it a key target in warfare as demonstrated in World War II strategic bombing and U.S. Cold War nuclear planning.[52] According to Lewis, cyber attacks are merely a new addition to the "portfolio" of instruments and methods of attack used in military campaigns against established high priority civilian targets such as electrical grids.[53] As information technology has become the "brains and nervous system" of critical infrastructure operations it is susceptible to attack as "an infrastructure in its own right."[54] U.S. Deputy Defense Secretary William Lynn III predicts that any major conflict "inevitably will involve cyber warfare that could knock out power, transport and banks, causing massive economic disruption."[55]

Eriksson and Giacomello note that the "common view" inherent in policy and scholarly literature is that as societies become more reliant on information technology they also become more vulnerable to cyber threats.[56] As critical infrastructure is dependent on software based control systems that function in interdependent networks it is both an "invaluable asset" and a "lucrative target."[57] Dunn reviews the critical infrastructure protection debate and concludes that vulnerabilities in critical infrastructure

[51] I thank Dr. Doug Ross for suggesting this term to characterize the sceptics who see the publicly invoked threat as largely unwarranted.

[52] Robert Latham, "Introduction," in *Bombs and Bandwidth,* ed. Robert Latham (New York: The New Press, 2003): 14.

[53] OECD, *Reducing Systemic Cybersecurity Risk*, 6. Sommer and Brown note that cyber weapons include: "unauthorized access to systems(hacking), viruses, worms, Trojans, denial of service, distributed denial of service using botnets, root-kits, and the use of social engineering", 6.

[54] Latham, "Introduction," 14.

[55] Wolf, "The Pentagon's New Cyber Warriors."

[56] Johan Eriksson and Giampiero Giacomello eds. *International Relations and Security in the Digital Age* (New York: Routledge, 2007): 7.

[57] Myriam Dunn, "Securing the Digital Age: The Challenge of Complexity for Critical Infrastructure Protection and IR Theory," in *International Relations and Security in the Digital Age*, eds. Johan Eriksson and Giampiero Giacomello (New York: Routledge, 2007): 94.

are "believed to be on the rise;" interdependence between information technology and infrastructure entails that critical infrastructure may be attacked through virtual means.[58] Patel et al, Sommer and Brown, and Lewis all reiterate a variation of the following observation: new Supervisory Control and Data Acquisition (SCADA)[59] networks have moved away from proprietary systems and have become integrated into corporate networks and the Internet, these systems use commercial software and can be remotely accessed and controlled, therefore they are less complex to infiltrate and exploit using unauthorized cyber attacks.[60]

Cyber doom scenarios constitute a central "metaphor" of the larger debate surrounding the strategic vulnerabilities of networked societies. In these alarming accounts "overall infrastructure would be disrupted to the point that society and government would lose the ability to function normally."[61] Richard Clarke provides the following archetypal account of dread wrought by a cyber attack on the U.S.: A nation wide blackout has thrown the continental U.S. into disarray. The financial system is crippled. Poisonous gas clouds bellow from burning oil refineries. Airplanes collide in mid air and fall from the sky. Subways crash and trains derail. The U.S. military sits isolated, powerless and unable to communicate and respond to the instantaneous and mass

58 Dunn, "Securing the Digital Age: The Challenge of Complexity for Critical Infrastructure Protection and IR Theory," 94.

59 Ronald Kurtz, *Securing SCADA Systems,* (Indianapolis: Indiana: Wiley Publishing Inc, 2006) http://www.scribd.com/doc/60046847/3/SCADA- (accessed August 15, 2011). Supervisory Control and Data Acquisition Systems (SCADA) are defined as the "technology that enables a user to collect data from one or more distant facilities and/or send limited control instructions to those facilities." SCADA systems are used in transportation systems, pipeline controls, refineries, electricity generation plants, and water treatment facilities.

60 Sandip Patel, Ganesh Bhatt, and James Graham, "Improving the Cyber Security of SCADA Communication Networks, "*Communications of the ACM* Vol. 52 No.7 (July 2009): 139.

61 Eriksson and Giacomello, *International Relations and Security in the Digital Age,* 8.

devastation.[62] Such visions of paralysis and devastation aptly labeled as cyber doom, "Cybergeddon" and cyber Pearl Harbor have permeated media and policy discourse since the early 1990s and continue to resonate in U.S. defense policy debates; the threat is potentially perilous and it cannot be ignored.

The Center for Strategic and International Studies Commission on cyber security for the 44th Presidency argues that: "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. It is, like Ultra and Enigma, a battle fought mainly in the shadows. It is a battle we are losing."[63] The 2009 White House Cyber Security Policy Review assesses the gravity of the cyber threat risk as follows: "threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies."[64] Newly minted U.S. Secretary of Defense, Leon Panetta, articulates the most recent U.S. defense establishment pronouncement regarding the possibility of a "cyber Pearl Harbor":

> "There is no question that the whole arena of cyber attacks, developing technologies in the information area represent potential battlefronts for the future. I have often said that there is a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber attack that

62 Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: Harper Collins, 2010):65-67. Clarke's "Cyber War" appears to accept the technical and logistical adeptness and resources to carry out such attacks as a given. There is a paucity of technical analysis and referenced source material in the book that complicates verification of the scenarios and cyber attack capabilities described by the said authors.

63 Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (December 2008): 17, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed January 17, 2011). The report notes that Enigma refers to the German military encryption machine in World War II and Ultra is the British program that cracked it; this gave the British "immense advantage,"11.

64 The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 2009): 12, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed June 10, 2011).

> cripples our power systems, our grid, our security systems, our financial system, our governmental systems."[65]

Beneath the veneer of dramatic rhetoric, the underlying premise of the "electronic Pearl Harbor" scenario reveals that "information operations are seen not merely as a means of improving or complementing physical attack, but as a means of replacing physical destruction with electronic."[66] This is exacerbated by the dynamics of complex interdependent systems whereby "independent failures will interact in ways that can neither be foreseen by designers nor comprehended by operators" and will produce cascading effects that are not well understood and proceed at a pace which precludes mitigating intervention.[67] The appeal of launching cyber attacks is based on perceived low costs to developing such attacks and the ease of using computer technologies to inflict damage.[68] The problem of attack attribution ensures attackers may function with relative impunity in the cyber realm: "the enemy becomes a faceless and remote entity, a great unknown that is almost impossible to track and that opposes security institutions and legal systems that are ill-suited to counter or retaliate against such a threat."[69] All of these factors create varying degrees of ambiguity surrounding cyber attacks that make risk assessment and mitigation difficult. As Samaan observes, the inability of decision makers to accurately articulate degrees of risk associated with cyber warfare is manifest

[65] Senate Committee on Armed Services, "*Hearing to Consider the Nomination of Hon. Leon E Panetta to be Secretary of Defense*," June 9, 2011, http://armed-services.senate.gov/Transcripts/2011/06%20June/11-47%20-%206-9-11.pdf (July 14, 2011).

[66] Eriksson and Giacomello, *International Relations and Security in the Digital Age*, 8.

[67] Dunn, "Securing the Digital Age: The Challenge of Complexity for Critical Infrastructure Protection and IR Theory," 96.

[68] Dunn, "Securing the Digital Age: The Challenge of Complexity for Critical Infrastructure Protection and IR Theory," 93. Dunn further notes that research conducted in the 1960s by Forrester showed that "complex systems behave contra-intuitively due to parallel occurrences happening at different speeds, irregularities and non-linear cause/effect relationships with the result that the human brain is unable to 'read' these systems correctly."

[69] Dunn, "Securing the Digital Age: The Challenge of Complexity for Critical Infrastructure Protection and IR Theory," 95.

in “menacing labels” and “evocative imagery” that provide a simplistic portrayal of cyber conflict.[70]

Cyber doom: A critical assessment

Scepticism abounds regarding the technical and logistical feasibility of carrying out cyber attacks that could produce long-term destructive effects that pose an existential strategic threat to the U.S. According to Sommer and Brown, in order for the type of attack described by Clarke to succeed there “needs to be a succession of different, persistent attacks on several targets the consequences of which is that each individual attack has a magnifying effect.”[71] The vulnerabilities that enable the cyber attack may be “easily” fixed by the defender or nullified as security configurations of the target operating environment change.[72] Sommer, Brown and Libicki[73] note that once the cyber attacks are detected there would be attempts to neutralize them by eliminating the vulnerability and thus reducing the system’s susceptibility to further attacks; once detected and “disarmed” the same attack exploit could not be used again. [74]

Once a hacker has gained access to a system, to execute such “perfect storm conditions” would require a “great deal of accurate research and preparation”[75] involving heavy insider knowledge from a saboteur who is able to physically manoeuvre within

70 Jean-Loup Samaan, “Cyber Command: The Rift in US Military Cyber-Strategy,”16.

71 OECD, *Reducing Systemic Cybersecurity Risk*, 47.

72 National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberatttack Capabilities,* 134. According to this report “a system administrator can close down unused access point with a few keystrokes. A patch can repair a security flaw only a few seconds after it is installed. A new security scan can discover and eliminate malicious software agents in a few minutes.”

73 Martin Libicki, “Cyberwar as a Confidence Game,” *Strategic Studies Quarterly* (Spring 2011): 133.

74 OECD, *Reducing Systemic Cyber Security Risk*, 5. This type of attack scenario would involve using a “successive series of never before used DDOS attacks each with a command and control system as well as a subservient botnet as each individual attack loses its effectiveness.” The authors note that Distributed Denial of Service attacks usually last only 1-2 days thereafter, which a specific attack signature is identified and blocking technology is quickly developed and implemented, 47.

75 OECD, *Reducing Systemic Cyber Security Risk,* 47.

proprietary air gapped computer facilities to retrieve in-depth knowledge regarding the target facilities, in order to design the attack, and to infect the target system. This analysis is echoed and expanded upon by Dunn who observes that tailoring each weapon to the system denotes an intimate knowledge of the enemy's weaknesses and possible system entry points; such exigencies deflate the argument that cyber attacks are cheap, could be readily developed and that an "arsenal" of such weapons could be stockpiled for use.[76] Libicki makes parallel conclusions in his discussion of the cyber battlefield. Cyber warfare is "soaked in intelligence" and requires knowledge of network architecture and the relationships between various defense systems. The search for vulnerabilities "is usually a search for specific vulnerabilities in specific systems that can be exploited in specific ways."[77]

As observed by Sommer and Brown, to stage these types of attacks on several targets would require a confluence of conditions including the IP addresses of the computer systems or targets, their operating systems and applications, and forms of protection and back up in place.[78] The latter point is important, as somehow the attack would have to subvert safety systems in place that detect various idiosyncratic failures and operational abnormalities. As Libicki notes, systems attacked may have a "crisis reserve mode," a failsafe device or procedure, that may "not be observable in normal times"[79] but which may detect and override errant operations or alert human operators that something is amiss.[80] As will be explored in chapter three, the Stuxnet worm was developed using a precisely mirrored target environment that included industrial

76 Myriam Dunn Cavelty, "As Likely as a Visit from E.T," *The European*, January 7, 2011, http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear (accessed March 4, 2011).

77 Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009): 155. Libicki asserts that the preparation of the cyber battlefield requires more money, time, and people than operating on the conventional battlefield.

78 OECD, *Reducing Systemic Cyber Security Risk*, 47.

79 Martin Libicki, "Cyber-Security and Cyber-Deterrence,"(Presentation, John Hopkins University, February 16, 2011), https://outerdnn.outer.jhuapl.edu/videos/021611/Libicki.pdf (accessed July 12, 2011).

80 Libicki, *Cyberdeterrence and Cyberwar*, xvii

equipment, computing software and hardware, calibration parameters and safety systems and settings, to test the attack vector. Once discovered the software and hardware vendors developed patch remedies and the attacks were neutralized; launching another variant of Stuxnet would entail developing new attack methods to exploit yet previously unknown vulnerabilities. A cyber doom scenario on the scale envisioned by Clarke would require surmounting logistical hurdles including: insider infiltration of target systems and likely expansive testing of mirrored target systems, which could be several hundred or several thousand systems, across a vast number and array of government, military and civilian organizations.

Lewis illustrates this conundrum by looking at the water supply infrastructure in the U.S. which he reports has 54, 064 separate water systems; this type of diversity creates resilience and makes large scale cyber attacks against multiple operators highly unlikely.[81] Berinato evaluates the cyber threat to water utilities by reviewing the organizational framework, operations and safety and security protocols of the air-gapped SCADA systems at the Massachusetts Water Resource Authority. Even if the attacker were to gain physical access to the facility, gain or subvert control of command and control equipment or programmable logic controllers and make changes undetected, water samples are tested systematically for abnormalities and crews regularly check the integrity of the equipment, facilities and electronics. Even if a hacker were to subvert all such controls, data is relayed back to the SCADA operators from sensor points in the pipes that would report any abnormalities in chlorine or other chemical levels.[82] The aftermath of natural disaster precedents such as floods indicates that temporary unavailability of service has produced "neither terror nor paralysis."[83]

81 James A Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *Center for Strategic and International Studies* (December 2002), 4. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (accessed July 12, 2011).

82 Scott Berinato, "Debunking the Threat to Water Utilities," http://www.cio.com/article/30935/Debunking_the_Threat_to_Water_Utilities (accessed June 3, 2011).

83 Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," 4.

The U.S. electrical grid has over 3,000 public and private utilities that operate their own lines using a variety of separate and different information technologies and security arrangements.[84] Lewis notes attackers would need to "find vulnerabilities in multiple systems to significantly disrupt the power supply and even then an attack might only disrupt service for a few hours."[85] According to Hersh the formation of regional grids entails that "an electrical supplier that found itself under cyber attack would be able to avail itself of power from nearby systems."[86] Clarke, among other commentators, has suggested that critical infrastructure has been laced with logic bombs that will be used later upon activation by adversaries. However, according to Libicki, no system will "stand still"[87] and there is simply no guarantee that a specific vulnerability will be there when the time comes to exploit it. Further, while information systems may be mapped and data extracted from them, there are important factors that may not be ascertained from such clandestine online reconnaissance including: the level of redundancy of the system; the level of human control, monitoring, and intervention in critical operations;[88] and responses and protocol to normal system failures.

Sommer and Brown analyze typical feasible cyber-related events for likelihood of occurrence, duration and propagation that would have varying degrees of impact on the affected nation state and business and individuals; they conclude most would be "relatively localized and short-term in impact."[89] The authors base their analytical

84 Seymour Hersh, "The Online Threat: Should We Be Worried About a Cyber War?" *The New Yorker*, November 1, 2010, http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh (accessed November 5, 2010).

85 Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," 5.

86 Hersh, "The Online Threat: Should We Be Worried About a Cyber War?"

87 Libicki, *Cyberdeterrence and Cyberwar*, 55.

88 Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," 10.

89 OECD, *Reducing Systemic Cyber Security Risk, 5,* 89-108. From their findings, Sommer and Brown conclude that large-scale global effects would be limited to scenarios where there was a fundamental compromise of Internet infrastructure or a large-scale solar flare. The authors admit that damage in the scenarios they analyzed would be likely and individuals and businesses may suffer. The authors' analysis looked at whether such attacks could result in a "global shock."

conclusion on the following: the Internet is designed to be robust and to provide for route around; most cyber events do not involve the loss of physical resources; "solutions to discovered flaws in software and operating systems/or the emergence of new forms of malware have been found and made available within a few days;" few single distributed denial of service attacks last more than a day; many governments and businesses have back-up and contingency plans; many networks are not connected to the Internet and use specialized protocols and equipment and any successful compromise would require heavy insider knowledge.[90]

Secondly, cyber security risk scenarios with long term physical effects are "dwarfed" by conventional catastrophes, such as natural disasters, in which disruptions to the cyber infrastructure may "propagate and magnify" the original event and inhibit recovery and mitigation. The authors recommend that contingency plans are in place to ensure alternate means of essential service delivery to "withstand and recover" from both accidental and deliberate cyber events.[91]

The analytical discord manifest in varying assessments of the nature, scope and gravity of cyber threats shapes the potential range of institutional and policy frameworks for addressing such threats. The act of "securing" against perceived digital threats within a particular framing of the event dictates the actors, politics and policies that constitute the framework for providing security against the threat.[92]Stark assessments of cyber threats prescribe an expanded military role to protect public and private sector organizations from what is perceived to be potentially devastating phenomena. As noted by Eriksson and Giacomello, framing an incident as a cyber crime implies that criminals are the culprits and that the proper authority responsible for investigating and prosecuting such incidents are domestic law enforcement bodies. Conversely, framing

90 OECD*, Reducing Systemic Cyber Security Risk*, 82.

91 OECD, *Reducing Systemic Cyber Security Risk*, 6.

92 Dunn, "Securing the Digital Age: The Challenge of Complexity for Critical Infrastructure Protection and IR Theory," 87.

an incident as “information warfare” implies that the perpetrators are nation state actors and that the military has a responsibility to respond to the threat.[93]

States have varied approaches in regard to how to define cyber attacks and whether the incident is considered an attack at all; this frames their assessment of the intentions and capabilities of peer competitors. It is quite possible that one state may decipher a cyber attack as a matter for domestic law enforcement to address while another state may diagnose the same incident as an existential military threat to national security and survival. In the largely anecdotal media publications reviewed cyber espionage is conflated with the chimeric term “cyber war”.

The lack of lexicon, norms and rules, and policy framework for state interaction in the digital domain, complicated by the interface of state strategic goals and criminal privateering, is embodied in the analytically ambiguous term “cyber war”. It is unclear what cyber war is and who the protagonists in this cyber war are albeit according to some commentators the U.S. is thick in the midst of one: “The United States is fighting a cyber-war today and we are losing it. It’s that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking.” [94]Former NSA Director, Mike McConnell indicates that the cyber-war mirrors the potential economic and psychological effects of the nuclear challenge and thus a doctrine of both deterrence and pre-emption must be adopted to counter the threat. McConnell provides the example of hacking incidents against private U.S. corporations, including against Google in 2009 as the basis of both the threat analysis and his recommendations for increased NSA involvement in locating and eliminating cyber-attacks.[95] According to Lewis espionage in cyberspace is a routine occurrence and “talking in terms of war, terror, attack, weapon constrains the range of action that the

[93] Eriksson and Giacomello, *International Relations and Security in the Digital Age*, 20.

[94] Mike McConnell, “Mike McConnell on How to Win the Cyber-War We’re Losing,” *The Washington Post,* February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (accessed May 16, 2010).

[95] Ibid.

United States can take in response."[96] The semantic imprecision and confusion regarding cyber warfare, and the trend towards using this term as a catch-all phrase involving all incidents with a cyber pre-fix, elevates the importance and significance of these incidents along with the requisite responses that such a label may imply.

[96] James Lewis, "The Cyber War has Not Begun."

Chapter 4.

Stuxnet and the Future of Cyber War

In July 2010, a spyware attack was discovered targeting industrial control systems in several countries including "Iran, Indonesia, India, Ecuador, the United States, Pakistan, and Taiwan."[97] Initial reports indicated that the attacks might be an advanced cyber espionage ploy designed to steal proprietary information, via collecting and transmitting data, from a history database within Siemens SCADA control software.[98] The picture that emerged after several months of reverse engineering and binary code analysis is that the attacks were anything but the machinations of a quotidian spyware program. According Liam O Murchu of Symantec, Stuxnet is the first publicly known worm to target industrial control systems with an ability to control physical machinery; this sets it apart from other cyber threats.[99] Since its discovery in July 2010, computer security firms as well as accompanying media commentary have analyzed and highlighted the technical prowess, level of ingenuity, and complexity of the Stuxnet worm.

[97] Mark Clayton, "Stuxnet Spyware Targets Industrial Facilities, via USB Memory Stick," *The Christian Science Monitor*, July 23, 2010, http://www.csmonitor.com/USA/2010/0723/Stuxnet-spyware-targets-industrial-facilities-via-USB-memory-stick (accessed September 9, 2010).

[98] Ibid, At the time it was not known what the close to 5,000 functions of the "spyware" could do and thus what the attackers intentions could be.

[99] Liam O Murchu, "Last Minute Paper: An Indepth Look into Stuxnet," http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml (accessed June 12, 2011). O'Murchu is the supervisor of security response operations at Stuxnet and principal investigator and co-author of Symantec's Stuxnet Dossier.

It has taken several months for researchers to reverse engineer Stuxnet in order to determine what attack vectors Stuxnet used to gain access to industrial control systems, what type of equipment or process the attack was intended to sabotage, what functions Stuxnet used to achieve this and what organizations or entities were attacked. In the realm of cyber war, the time necessary to unearth and decipher the schematic details regarding the targets, capabilities and level of damage caused by a cyber-attack complicates the political and strategic context for identifying who or what is attacked and what responses may be marshalled. In fact, the intended victims of the "cyber missile" may not be aware they are under attack if at all; Stuxnet was discovered in July 2010 and yet it has been confirmed that it existed undetected at least one year prior to this date.

A number of security firms and government agencies, as well as accompanying media commentary, have analyzed and highlighted the technical prowess, level of ingenuity, and "ground-breaking" complexity that is the Stuxnet worm.[100]

For the purposes of this discussion, the anatomical composition of Stuxnet is worth examining in some detail insofar as to provide an understanding of the interface between digital software operations and the functional integrity of physical hardware such as industrial control systems. Many theories abound regarding the origins of Stuxnet and its intended purpose and targets; one of the prevailing theories is that it may be a pre-emptive attack on Iran's budding nuclear program by either or both Israel and the United States.

[100] In depth technical analysis of Stuxnet has been compiled by experts at Symantec and is published as W32.Stuxnet Dossier, Version 1.4(February 2011), accessed at http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf ESET has produced a report on the nature of targeted cyber attacks, SCADA and the distribution of the Stuxnet worm in a publication entitled Stuxnet Under the Microscope accessed at http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf Langner, an independent cyber security firm in Germany specializing in control systems, obtained a copy of Stuxnet and reverse engineered and analyzed the worm code in depth over the course of several months; this analysis has been chronicled on Langner's blog in full and may be accessed at http://www.langner.com/en/blog/

In this chapter, I examine the Stuxnet attacks to explore the evolution of offensive cyber weaponry and the embryonic contours of cyber warfare. This chapter reviews the published data on the Stuxnet attacks to illuminate the complexities surrounding cyber-attack attribution; ambiguity regarding appropriate responses to such events; and the political and strategic implications that arise with the use of pre-emptive cyber-attacks.

Dissecting the Stuxnet Worm: Clues in the Code

> **"**The whole attack is not at all about stealing data but about manipulation of a specific industrial process at a specific moment in time. This is not generic. It is about destroying the process"[101]

Stuxnet surreptitiously infiltrates and establishes control over industrial control systems with the aim to sabotage normal operations. The worm is introduced into an "air gapped" industrial control system via a removable device such as a USB memory stick.[102] Stuxnet employs four zero day exploits[103] and Siemens' default passwords to access Windows operating systems that run WinCC and PC7 programs.[104] [105] The

[101] Mark Clayton, "Stuxnet Malware is Weapon out to Destroy…Iran's Bushehr Nuclear Plant?" *The Christian Science Monitor,* September 21, 2010, http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant (accessed November 8, 2010).

[102] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53:1 (Spring 2011): 24. The term air gapped entails that these devices were not connected to the internet.

[103] Kim Zetter, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target," *Wired Threat Level Weblog,* entry posted September 23, 2010, http://www.wired.com/threatlevel/2010/09/stuxnet/ (accessed November 8, 2010). According to Zetter: "One zero-day is used to spread the worm to a machine by a USB stick. A Windows printer-spooler vulnerability is used to propagate the malware from one infected machine to other on a network. The last two help the malware gain administrative privileges on infected machines to feed the system commands."

[104] Farwell and Rohozinski, 24.

[105] According to Byres, Ginter and Langill, "SIMATIC Win CC is a process visualization system that comprises the core SCADA system. It works with Siemens branded control equipment, such as the S7 line of programmable logic controllers(PLC) or it acts independently with control products from other vendors." The SIMATIC PCS7 is composed of S7 Programmable logic controllers, Win CC visualization software and STEP 7 configuration software. Accessed at: http://www.isssource.com/stuxnet-report-a-system-attack/ (accessed June 3, 2011).

attack engages in a complex process of "finger printing" the infected system to establish it has reached the intended target including "checking model numbers, configuration details, and even downloading program code from the controller to check it if was the right program."[106] Stuxnet looks for Siemens 315 and 417 PLC's; once it locates one of these two models it verifies the PLC for certain process configurations and injects "rogue code" into the controllers, where it resides alongside legitimate code, until activation by "complex timer and process conditions."[107] Stuxnet inventories the infected system to check that it has 33 frequency converter drives, made by either, or both, Fararo Paya in Tehran or Finland Based Vacon. The worm then monitors and verifies that the installed frequency converter drives run between 807 Hz and 1210 HZ for a period of several days before it modifies their behaviour by activating an attack sequence.

According to Ralph Langner, Stuxnet contains two different "digital warheads" that were deployed in combination as an "all-out cyber strike against the Iranian nuclear program."[108] The first digital warhead runs on Siemens S7-315 controllers and takes control temporarily away from the legitimate program.[109] The "warhead" code manipulates up to 186 high-speed drives by cycling drive speeds between low values and high values.[110] The second digital warhead, the Siemens 417 attack code, intercepts physical input and output and "provides the legitimate program running on the controller

[106] Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *Security & Privacy, IEEE,* Vol. 9 Issue 3(May/June 2011): 49-51.

[107] Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," 49-50.

[108] Ralph Langner. "The Big Picture," *Langner Blog*, entry posted 19 November, 2010, http://www.langner.com/en/2010/11/19/the-big-picture/ (accessed April 17, 2011).

[109] Ibid. According to Langner "war head one" manipulates an array of 186 high-speed drives attached up to six Profibus segments. The manipulation cycles drive speeds between low values and high values. The 315 code would only control the rotors of single modules in the cascade; it cannot control the centrifuges alone as there must be additional controllers that take care of pumps and valves. See Langner's post at: http://www.langner.com/en/2010/11/13/potential-417-target-k-1000-603000-3/

[110] Langner, "The Big Picture."

with normal input patterns that are actually pre-recorded by Stuxnet."[111] Langner likens the process to a form of subterfuge typically portrayed by Hollywood films; real time surveillance during a heist operation is replaced by pre-recorded security camera footage that deceives authorities into thinking nothing is amiss.[112]

The infected programmable logic controllers deploy the "warheads" to sabotage the system process by slowing down or speeding frequency converter drives outputs to different rates at different times; Stuxnet changes the output frequency for short intervals, to 1410 Hz and then to 2 Hz and then 1064HZ, over a period of several months. Following each attack sequence the system returns to normal operations for a period of 27 days before the next attack sequence commences.[113] If a nuclear centrifuge is indeed the target, centrifuges need to spin at a precise speed for long periods of time in order to extract uranium; cessation of this process at high speeds can disrupt the process of isolating the heavier isotopes in the centrifuges. The manipulation of cycling drives in a gas centrifuge would crack the rotor and thereby destroy this component.

Target: Iran

Iran has emerged as the likely target of the Stuxnet worm based on the prevalence of infections, which suggests it is the epicenter of the attacks, and technical analysis that reveals Stuxnet could at least theoretically "disrupt or destroy" Iranian

[111] Ralph Langner, "How to Hijack a Controller," *Control Global,* January 13, 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html (accessed April 17, 2011). Langner notes that during the 417 attack Stuxnet changes the controller program by disabling automatic updates of input process and output process images. According to Langner, "the fake input data is really recorded by Stuxnet on the PLC from the original process."

[112] Langner, "How to Hijack a Controller."

[113] Eric Chien, "Stuxnet: A Breakthrough," *Symantec Official Blog*, entry posted 16 November, 2010, http://www.symantec.com/connect/blogs/stuxnet-breakthrough (accessed May 2, 2011). According to Symantec, converter drives that output over 600HZ are regulated for export by the US Nuclear Regulatory Commission. If a nuclear centrifuge is indeed the target, centrifuges need to spin at a precise speed for long periods of time in order to extract uranium; cessation of this process at high speeds can disrupt the process of isolating the heavier isotopes in the centrifuges." The manipulation of cycling drives in a gas centrifuge would crack the rotor and thereby destroy this component.

centrifuges.[114] This has led to a cacophony of analysis that contends the worm is a cyber attack on Iran's nuclear facilities, specifically its alleged clandestine nuclear arms programme.[115]

In November 2010 researchers at Symantec speculated that the concentration of infections in Iran "likely indicates that this was the initial target for infections and was where infections were initially seeded."[116] By the end of September 2010, Stuxnet infected over 35,000 Iranian organizations; this represented over 60,000 hosts or 58.31% of infections worldwide.[117] Further analysis of the infection data from Symantec provides compelling evidence that indeed Iran was the target of the Stuxnet attacks. Every time Stuxnet infects a new host, a time stamp, along with other system information

[114] William Broad and David Sanger, "Worm was Perfect for Sabotaging Centrifuges," *New York Times*, November 18, 2010, http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html (accessed December 28, 2010).The article notes that Stuxnet was calibrated in a way that could send nuclear centrifuges spinning out of control. The worm's target appears to be frequency converter drives that changes the output frequency to control the speed of a motor; changing the speed sabotages the operation of the industrial control process.

[115] Although this is not an exhaustive list, the author notes the following publications reviewed herein have carried analysis linking the Stuxnet attacks to Iran's nuclear facilities. Several of these news organizations and publications have included extensive coverage of Stuxnet from its initial discovery onward. The following is a sample of this analysis: BBC http://www.bbc.co.uk/news/world-middle-east-11414483, *The Guardian* http://www.guardian.co.uk/world/2010/sep/25/iran-cyber-hacking-nuclear-plants, the Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2010/11/15/AR2010111506768.html, *The Christian Science Monitor* http://www.csmonitor.com/USA/2010/0924/Stuxnet-worm-mystery-What-s-the-cyber-weapon-afterr , *Aviation Week and Space Technology* http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awst/2010/10/04/AW_10_04_2010_p29-258117.xml&headline=Cyberattack%20Becomes%20More%20Sophisticated

[116] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W.32 Stuxnet Dossier,* Symantec Security Response, September 2010, quoted in CRS Report for Congress, "*The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*," by Paul Kerr, John Rollins, and Catherine Theohary," Congressional Research Service, December 9th, 2010.

[117] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier Version 1.3*, Symantec Security Response Centre (November 2010), http://www.symantec.com/index.jsp (accessed May 2, 2011). In July 2010, Symantec set up a system to monitor traffic to the Stuxnet command and control server. According to Symantec, this allowed the researchers to "observe the rates of infection and identify the locations of infected computers, ultimately working with CERT and other organizations to help inform infected parties."

is recorded within the Stuxnet code for that attack sample. Symantec used this data to determine that over 12,000 infections can be directly traced back to an initial 10 infections at five different organizations in Iran;[118]the organizations were targeted in June 2009, July 2009, March 2010, April 2010, and May 2010. Symantec notes that since Stuxnet's propagation mechanisms are LAN based, "the final target must be assumed in close network proximity to the initial seeded targets."[119] It also appears that the attackers likely knew whom they wanted to infect prior to completing the code. For the June 2009 attack, the timeframe between compilation of the source code and launch of infection was just 12 hours; this suggests that "the attackers had immediate access to the computer they attacked-either working with an insider or using an unwitting insider to introduce the infection."[120]

Siemens, the manufacturer of the targeted systems, has refrained from commenting as to the target of the virus albeit they affirmed that Siemen's was not

[118] Nicholas Falliere, Liam O Murchu and Eric Chien, *W.32 2011Stuxnet Dosser Version 1.4*, Symantec Security Response, February 2011, 7. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed May 2, 2011). As Stuxnet records a timestamp within itself every time a new infection occurs this entails that each sample of Stuxnet studied by Symantec "has a history of every computer that was infected, including the first infection."

[119] Ibid,10.

[120] Kim Zetter, "Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant," *Wired: Threat Level Blog,* entry posted February 11, 2011, http://www.wired.com/threatlevel/2011/02/stuxnet-five-main-target/ (accessed March 5, 2011).

involved in any plant construction, delivery of software or control systems to Iran.[121] The company's products are "widely used in Iranian electricity plants, communication systems and in the country's first nuclear power plant, near the city of Bushehr.[122] The worm was likely spread via contractors or LAN networks to its speculated target destination: Natanz.

Navigating the Labyrinth of Attribution: The case of Stuxnet

The fact that there are several actors with potential motivation, interest, capabilities and resources to carry out cyber attacks, against the Iranian nuclear programme or other targets hit by Stuxnet, indicates that attribution in the cyber realm remains a vexing challenge and offers no easy or obvious answers.

Israel and the U.S. have emerged as the likely suspects behind the Stuxnet attacks based on their documented pursuit of diplomatic inducements, and consideration of pre-emptive military strikes to halt Iran's alleged nuclear weapons program, buttressed by companion covert campaigns to infiltrate and sabotage Iranian nuclear supply chains, equipment and facilities. Neither Israel nor the U.S. has to date acknowledged or denied what, if any, involvement their intelligence agencies or military

[121] Jonathan Fildes, "Stuxnet Worm Targeted High-value Iranian Assets," *BBC News*, 23 September, 2010. http://www.bbc.co.uk/news/technology-11388018http://www.bbc.co.uk/news/technology-11388018 (accessed November 5, 2010). Analysis provided by Benjamin Weinthal provided in the *Wall Street Journal* indicates that in 2008 Siemens conducted 438milllion Euro worth of trade in Iran and had 290 Iran based employees that remain active in the gas, oil, and infrastructure and communications sectors despite the company's affirmation in the above cited BBC article that "Siemens left the country nearly 30 years ago." Weinthal's analysis may be accessed at http://online.wsj.com/article/SB123379548035950207.html Effective July, 2010 Siemens has stopped accepting orders from Iran. However, an investigation by Der Spiegel indicates that Siemens had shipped high technology components to a subsidiary of Atomsroyexport(the company handling the Bushehr contract) The said parts were then allegedly shipped to Iran but were intercepted by German customs officials: http://www.spiegel.de/international/business/0,1518,710810,00.html

[122] Thomas Erdbrink and Ellen Nakashima, "Iran Struggling to Contain Foreign-made Stuxnet Computer Virus," *Washington Post,* September 27, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706229.html (accessed November 5, 2010).

units may have played in developing and orchestrating the Stuxnet attacks. It is unlikely that such public admission will be forthcoming, even if the allegations are correct, as it would substantiate speculation regarding American and Israeli cyber offensive capabilities and confirm that a cyber variant of a pre-emptive military strike did indeed hit Iran.

Jeffrey Carr proposes alternative scenarios to "commonly held assumptions" that Israel or the U.S. targeted Iran's Bushehr or Natanz facilities. Carr suggests that China may want to support its third largest oil supplier whilst concurrently seeking ways to get Iran to stop enriching uranium by using Stuxnet to achieve these dual goals. Carr's analysis is based on the following compendium of information: Chinese designs for centrifuges, smuggled by the A.Q Khan network, were allegedly discovered in Iran; Chinese firms manufacture Vacon frequency converter drives; Real Tek , whose digital signatures were stolen and used by Stuxnet, has a subsidiary based in China and China has direct access to Windows source code.[123] As Swaine notes, Iran forms part of China's calculations to strengthen its political and economic goals in the Middle East and it serves as an opportune counterweight to American influence in the region; importantly Iran is a source of critical energy exports. In its relations with Iran, the Chinese

[123] Jeffrey Carr, "Stuxnet's Finnish-Chinese Connection," *The Firewall Blog Forbes,* entry posted December 14, 2010, http://blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/ (accessed December 28, 2010). Carr is the founder and CEO of Taia Global Inc. computer security company, principal investigator of Project Grey Goose into cyber conflicts and he writes a security blog for Forbes magazine.

leadership attempts to tread carefully to avoid any direct challenge to U.S. policies in the region.[124]

While China remains a strong supporter of the "global counter-proliferation regime" it makes a distinction between Iran's "as a possible violator of the non-proliferation regime-and the NPT in particular-and its right under the NPT to develop non military, civilian nuclear capabilities". However, China concomitantly recognizes that Iranian acquisition of nuclear weapons will likely destabilize the Middle East, by triggering an arms race or an Israeli and/or U.S. attack, thus jeopardizing critical energy exports."[125] As noted in this discussion, China also appears to have developed cyber attack capabilities that are regularly exercised and highlighted through espionage exploits on various companies and government organizations.

A second theory contends that China could have used Stuxnet to target nations that mine rare earth exports in order to thwart peer competitors in this industry;[126] it is unclear why China would pursue sabotage in this area considering it currently produces

[124] Michael D. Swaine, "Beijing's Tightrope Walk on Iran," *China Leadership Monitor*, No.33, June 28, 2010, Carnegie Endowment for International Peace, http://www.carnegieendowment.org/2010/06/28/beijing-s-tightrope-walk-on-iran/5on (accessed June 3, 2011). According to Swaine, Iranian crude accounts for 10-15 percent of its crude oil imports and this figure is likely to grow. China also appears to have benefited from U.S. sanctions that allow Chinese companies to face less competition in Iran. A more nuanced assessment of Chinese interests and policies, than the scope of this discussion allows, is taken up by Swaine in his piece. Swaine is a Senior Associate at the Asia Program at the Carnegie Endowment for International Peace specializing in Chinese security and foreign policy and U.S.-China relations.

[125] Ibid. Swaine further notes that: "Chinese opposition to efforts to prevent Iran from acquiring nuclear weapons could damage China's international reputation as a strong supporter of the global counter-proliferation regime."

[126] Jeffrey Carr, "Dragons, Tigers, Pearls, and Yellowcake: Four Stuxnet Targeting Scenarios," Taia Global Executive Cyber Protective Services, November 2010, http://nanojv.files.wordpress.com/2011/03/dragons_whitepaper_updated1.pdf (accessed May 2, 2011).

95% of the global supply of such materials. Cyber attack to consolidate market dominance in this context appears rather futile.[127]

Carr's third theory contends that Stuxnet may be a form of escalation from protests, by anti-nuclear power groups such as Green Peace, to full-fledged rogue sabotage of uranium producing states.[128] Apart from the fact that such operations may run counter to the scope and mandate of such organizations, it is unclear how such groups could muster the financial and technical resources to stage such attacks.[129]

Industrial subversion against competitors is also a potential explanation. Carr considers the possibility that Stuxnet could be deliberate corporate sabotage against Siemens by industry competitor Areva in order to create an "aura of uncertainty or lack of trust in Siemens products."[130] The Siemens and Areva corporate venture came to a rather abrupt end in 2009 when Siemens divested itself of a 34% stake in ArevaNP and embarked on securing a business partnership with Russia's Rosatom.[131] While Carr acknowledges that the prospect of Areva launching Stuxnet is low, the analysis does draw attention to the burgeoning underground global criminal economy within which

[127] Keith Bradsher, "China to Tighten Limits on Rare Earth Exports," *New York Times*, December 28, 2010, http://www.nytimes.com/2010/12/29/business/global/29rare.html (accessed May 4, 2011).

[128] Carr, "Dragons, Tigers, Pearls and Yellowcake: Four Stuxnet Targeting Scenarios."

[129] Falliere, O Murchu and Chien, *W32. Stuxnet Dossier Version 1.4* , 3. Symantec suggests that the attackers would "need to setup a mirrored environment that would include the necessary ICS hardware, such as PLC's, modules, and peripherals in order to test their code. The full cycle may have taken six months and five to ten developers not counting other individuals such as quality assurance and management." In other words, the attacks required resources, an intelligence capacity and testing facility.

[130] Carr, "Dragons, Tigers, Pearls, and Yellowcake: Four Stuxnet Targeting Scenarios," A fourth scenario not discussed herein involves China attempting to compete with India over energy shipping lanes in the Malacca straits. The reader is referred to pages 10-12 of Carr's paper for further elaboration of said argument.

[131] For full details see "Siemens and Areva: Nuclear Fission-Franco-German Industrial Relations Take Sharp Turn for the Worse, *The Economist,* January 29, 2009: http://www.economist.com/node/13022201 (accessed May 14, 2011).

crime ware kits and resources are "bought, sold and traded, and typically used for corporate warfare to knock political and business competitors off line."[132]

A sparsely explored theory is that Stuxnet may have been an attack on India's INSAT-4B satellite and is part of an escalating Chinese and Indian strategic rivalry that is extending into space-based assets.[133] This speculation was quickly dispelled when the Indian Space Research Organization confirmed that the satellites do not use Siemens software but an indigenously designed program. According to the Indian Space Research Organization a power supply glitch on July 7, 2010 resulted in the shutdown of 50% of the transponder capacity.[134] It may be difficult to readily distinguish whether a software or hardware malfunction is the result of a cyber attack or a defect or glitch; the effects on system operation may be identical considering the aim of cyber attacks is to disrupt normal system operations. Herein lies the danger: rather benign malfunctions may be condemned as cyber attacks and lead to increased suspicion and hostilities between rivals.

The list of potential creators and developers, and accompanying exploration of motives and capabilities is a glimpse into the advent of cyber war; an uncertain and untraveled strategic environment in which "the effort to pinpoint a perpetrator is bound to confound; "the detection systems are not likely to deliver as much data as fast or as clearly as the policymakers want" and it may be "difficult to tell if an incident is an act of war, the deed of a small terrorist group, a simple crime, or a natural occurrence."[135]

[132] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 26.

[133] Carr, "Did the Stuxnet Worm Kill India's INSAT-4B Satellite?" *The Firewall Blog Forbes*, entry posted September 29, 2010, http://blogs.forbes.com/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/ (accessed May 4, 2011).

[134] Srinivas Laxman, "Cyber Threat: ISRO Rules out Stuxnet Attack on Insat-4 B," *The Economic Times*, 12 October, 2010 http://articles.economictimes.indiatimes.com/2010-10-12/news/28435956_1_insat-internet-worm-stuxnet-worm (accessed May 4, 2011).

[135] David Hoffman, "The New Virology: From Stuxnet to Bio-bombs, the Future of War by Other Means," *Foreign Policy* (March/April 2011), http://www.foreignpolicy.com/articles/2011/02/22/the_new_virology?page=full (accessed April 9, 2011).

Clues in the Code and Design?

Stuxnet's origins are debated in what appear to be varying degrees of analytical conjecture; at time of writing, there is no indication that the Stuxnet code itself contains verifiable or definitive information regarding its developers or the design process. A review of publicly available information reveals that hypothetical speculation, for lack of conclusive evidence, largely defines the parameters of the Stuxnet debate.[136] If this is the future of cyber war it is one that is frightening indeed. The kinetic effects of such attacks may be far more benign than the speculation, fear and conspiracies that may exacerbate strategic rivalries, indulge temptations to engage in pre-emptive cyber strikes and lead to crisis escalation as paranoia sets in regarding an adversary's capabilities. Almost a year after the attacks were discovered, a great degree of uncertainty and ambiguity regarding how these attacks could have been developed and staged remains unresolved and perhaps precludes a denouement that will provide complete and authoritative answers regarding Stuxnet's creators and targets.

Some accounts posit that Stuxnet is coded with biblical and historical references that implicate Israel as the worm's developer. One of the Stuxnet project files is named "Myrtus" which according to research and media speculation may allude to the plant myrtle. The plant corresponds to the Hebrew name for Queen Esther in the Old Testament; in the Book of Esther the Jews pre-empt a Persian plot to destroy them.[137] The second alleged clue is the "do not infect code" "19790509" that could be a date marker. According to Symantec on May 9th, 1979 Habib Elghanian was the first Jew executed by the new Islamic government in Iran, which prompted a mass exodus of the

[136] It is important to note that this analysis has been pieced together from available commentary in the public domain regarding potential "clues" in the code and theories surrounding how the attackers may have acquired information regarding Iranian nuclear industrial control processes in order to successfully implant and carry out the attack.

[137] Arthur Bright, "Clues Emerge about the Genesis of Stuxnet Worm," *The Christian Science Monitor*, October 1, 2010, http://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm (accessed November 14, 2011).

Jewish community.[138] It is questionable why Stuxnet's developers would leave any clues regarding its origins considering the attack was elaborately designed for stealthy sabotage. Stuxnet's code reveals the execution of the attack sequence took several months and was programmed to lead to the disruption and gradual degradation of targeted industrial control equipment; successful sabotage was contingent on the attacks remaining undetected. It is plausible that the "clues" in the code are simply arbitrary code sequences or they could be reference to something utterly mundane; the "do not infect code" could be any date personally significant to the developer while "myRTU" can simply mean my Remote Terminal Unit.[139]

The clues could also be red herrings that were deliberately placed there to deflect attention and blame for the attacks. As Bruce Schneier observes: "Stuxnet's authors were uncommonly thorough about not leaving clues in their code; the markers could have been deliberately planted by someone who wanted to frame Israel. Or they could have been deliberately planted by Israel, who wanted us to think they were planted by someone who wanted to frame Israel. Once you start walking down this road, it's impossible to know when to stop."[140]

Stuxnet's genesis lies within a complex and exhaustive development process requiring vast resources, espionage, an existing foreign intelligence capability in order to gain access to and knowledge of foreign systems, likely co-operation of "insiders", and the ability to test the weapon in a precisely mirrored environment that exactly replicates the computing and control systems, including all software, equipment, calibration settings and safety mechanisms of the target domain.

[138] Falliere, O Murchu, Chien, "W32. Stuxnet Dossier Version 1.4," 18.

[139] Ibid. According to the researchers at Symantec RTU stands for remote terminal unit and are similar to a PLC; in some environments they are used as synonyms for PLCs.

[140] Bruce Schneier, "Stuxnet," *Schneier on Security Blog*, entry posted October 7, 2010, http://www.schneier.com/blog/archives/2010/10/stuxnet.html (November 14, 2010). Schneier is an American cryptographer and computer security specialist. He has published several books on cryptographic algorithms and is credited with designing "blowfish" encryption in 1993. Schneier writes a regular blog on security technology.

The attackers likely obtained the design documents for the targeted industrial control system schematics, as "each PLC is configured in a unique manner", through an insider saboteur or perhaps through some yet unknown digital retrieval precursor to Stuxnet. The digital weapon was then tested in a mirrored environment, for several months, that included the necessary industrial controls hardware, programmable logic controllers, modules and peripherals.

Secondly, the attackers used two stolen authentic digital certificates, from Realtek and JMicron in Taiwan.[141] Symantec notes that someone may have stolen such information that had physical access to the two companies both located in the Hsinchu Science Park in Taiwan.[142]

There is speculation that suggests the Dimona complex in the Negev desert may have functioned as a joint Israeli-U.S. test facility for the effectiveness of Stuxnet worm where Israel is alleged to have spun nuclear centrifuges identical to Iran's at Natanz.[143] The U.S. also appears to have a "cache " of P1 centrifuges that were intercepted[144] and

[141] Randy Abrams, "Why Steal Digital Certificates," *The ESET Threat Blog*, posted July 22, 2010, http://blog.eset.com/2010/07/22/why-steal-digital-certificatesnotes (accessed August 23, 2011). Abrams notes that when the creators of Stuxnet signed their driver files with stolen certificates this ensured that Windows would install the driver without warning and that if someone did look at the certificate they would not be suspicious. Randy Abrams of the ESET Threat Blog notes that: "When you install certain types of software on Windows Vista or Windows 7 it needs to be digitally signed with a trusted certificate. By stealing the certificate of a trusted vendor they decrease the chance of their malicious software being detected as quickly. In theory the digital signature tells you who signed the file, and who issued the digital certificate so you can decide if you trust the person or company who signed the file in practice if a digital certificate is stolen then you don't know who signed the file".

[142] Falliere, O Murchu, and Chien, *W32.Stuxnet Dossier Version 1.4*, 3.

[143] William Broad, John Markoff, David Sanger Broad, Markoff, Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all (accessed January 15, 2011). Although, if this is indeed true it remains unclear how Israel would procure such centrifuges, perhaps through the AQ Khan network as the article's authors suggest.

[144] "Libyan Nuclear Weapons," GlobalSecurity.Org, http://www.globalsecurity.org/wmd/world/libya/nuclear.htm (accessed May 25, 2011). In 2004 the U.S. airlifted 25 metric tons of Libyan weapons program components including centrifuge parts, uranium and sensitive documentation to Tennessee.

sent to the Oak Ridge National Laboratory after Libya gave up its nuclear program in 2003; these appear to have been assembled and tested in the U.S. “in order to gain insight” into other countries nuclear weapons programs. [145]

In 2008, Siemens provided assistance to U.S. agencies to defend against cyber attacks on critical infrastructure and according to some accounts by doing so the company may have inadvertently provided Washington with the requisite information necessary to infiltrate and sabotage Iranian nuclear facilities; “The expertise needed to defend against a cyber attack is essentially indistinguishable from that needed to make such an attack.”[146]

Amidst ongoing concerns in the U.S. regarding vulnerabilities of critical infrastructure to cyber attacks, the Idaho National Laboratory formed partnerships with industrial control system manufacturers to identify cyber vulnerabilities. Siemens co-operated with the Idaho National laboratory to identify vulnerabilities in its computer controllers in an effort to secure its global product chain against cyber attacks. Specifically, the Department of Homeland Security and the Idaho National Laboratory studied the widely used Siemens controller known as PCS-7 for Process Control Systems; this is the Siemens controller targeted in the Stuxnet attacks. It remains unclear whether Idaho National Laboratory may have passed information regarding the Siemens systems to “other parts of the nation’s intelligence apparatus.” The diagnosis of such vulnerabilities revealed information that could be exploited in a cyber attack, including against Siemens manufactured equipment identified by American intelligence agencies as being used at Iran’s nuclear enrichment facilities.[147] Stuxnet does appear to demonstrate “inside” knowledge of Siemens Win CC/Step 7 software that is reflected in

[145] Jeffrey Lewis, “On Spinning Libyan Centrifuges,” Arms Control Wonk Blog, entry posted 15 February, 2011, http://lewis.armscontrolwonk.com/archive/3551/on-spinning-libyan-centrifuges (accessed May 14, 2011). Lewis notes that “the U.S. is operating centrifuges from Libya in order to gain insight” into other countries nuclear weapons programs.” Lewis is the director of the East Asia Non-proliferation Program at the James Martin Center for Non-proliferation Studies at the Monterey Institute of International Studies.

[146] Falkenrath, “From Bullets to Megabytes.”

[147] Broad, Markoff and Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay.”

its capability to detect specific conditions and made code modifications in organizational Block 35; a part of the software that monitors critical factory operations that need a response within 100ms.[148]

Counter-proliferation through Cyber Pre-emption?

A number of strategies have been utilized in an attempt to decelerate and stop Iran's nuclear program. It is beyond the purview of this analysis to engage in a comprehensive survey of the approaches both contemplated and employed to effectuate such outcomes. In summary, such efforts have included:

> "Technology denial through export controls, sanctions and probable sabotage; the threat of force to destroy Iran's nuclear facilities and/or remove its regime, use of disincentives such as financial and economic sanctions and political pressure(including through four successive rounds of U.N. Security Council resolutions), and finally offers of economic and political incentives made through negotiations like the EU3 and later theP5+1"[149]

American and Israeli positions have ebbed and flowed towards and away from consideration, and planning, for military attacks against Iran's nuclear enrichment programme.

The American plans under the Bush doctrine envisioned regime change in Iraq as the first step towards "total transformation of the Middle East"; the quip 'Real Men Want to go to Tehran' eulogizes the desire of the neoconservative Bush administration to effect regime change in Iran.[150] Seymour Hersh's analysis of the Bush administration's "Iran Plans" indicates that a nuclear confrontation with Iran, in the form of a "sustained

[148] Thomas Chen, "Stuxnet, The Real Start of Cyber Warfare?" *IEEE Network* Vol. 24 Issue 6 (November/December 2010): 3. This type of information is proprietary and is not made publicly available by Siemens.

[149] Simon Zukowski, "The Nuclear Nonproliferation Regime: Its Status and Prospects"(unpublished Master's Thesis, Simon Fraser University, 2010), 55-56.

[150] David Hastings Dunn, "Real Men Want to go to Tehran: Bush, Pre-Emption and the Iranian Nuclear Challenge," *International Affairs* 83:1(2007):19-22.

bombing campaign" against nuclear targets, was envisioned as a triggering mechanism for a revolt against the religious leadership leading to the ultimate goal: regime change.[151] While attack scenarios were contemplated, Sanger argues that they did not progress beyond contingency planning at the Pentagon.[152] However, a good deal of preparatory work appears to have taken place: Turkey was approached for the use of air bases to attack Iranian nuclear targets, vessels equipped to counter mines were deployed to the Persian Gulf; and a second U.S. battle carrier group was moved into the area in early 2007 as an apparent demonstration of force in support of sanctions.[153]

A number of assessments reiterate the sentiment that the gravity of risks and sobering repercussions surrounding pre-emptive military air strikes on Iranian nuclear installations has arguably, to date, kept the specter of such attacks at bay. Military strikes on Iran would likely provide a national rallying cry for the Iranian population around the regime; "reinforce the belief inside Iran that the only way to defend the country is to have a nuclear capability"[154] and end any internal Iranian political debates regarding whether to build a bomb.[155] Rather than inspire an anti-regime revolution, Farwell and Rohozinski suggest that air strikes may actually work "to unite a currently divided Iran and enable Ahmadinejad and his allies to consolidate power."[156]

[151] Seymour Hersh, "The Iran Plans: Would President Bush Go to War to Stop Tehran from Getting the Bomb?" *The New Yorker,* April 17, 2006, http://www.newyorker.com/archive/2006/04/17/060417fa_fact (accessed June 4, 2011).

[152] David E. Sanger, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site," *New York Times*, January 10, 2009, http://www.nytimes.com/2009/01/11/washington/11iran.html (accessed March 22, 2011).

[153] Dunn, "Real Men Want to Go to Tehran," 21.

[154] Hersh, "The Iran Plans."

[155] Joseph Cirincione, "Five Myths about Iran's Nuclear Program," *Washington Post*, October 18, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/10/15/AR2009101503476.html (accessed May 14, 2011). Cirincione is the president of the Ploughshares Fund. He is the former director for non-proliferation at the Carnegie Endowment for International Peace.

[156] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 29. The prospect of such developments appears quite plausible. The characterization of Iran as the "axis of evil" appeared to strengthen the position of the conservative nationalists in Iran and culminated in the election of a new and hardline president, Ahmadinejad in 2005. See Dunn supra note 9.

As Perkovich notes, the ability to physically destroy all of Iran's capacity to make centrifuges and enrich uranium is unlikely considering that many such facilities are deep underground complexes and there is a lack of information regarding how many and where all such facilities are located.[157] Any military strikes on Iran may result in the disruption of the flow of oil from the Gulf; Iran could potentially block 40 percent of global oil exports by sinking tankers coming from Iraq, Saudia Arabia and other Gulf States. Iran could also respond to such attacks with a regional retort by arming the Taliban in Afghanistan with surface to air missiles or supplying Hezbollah in Lebanon with missiles to use on Israel.[158]

According to Zukowski, "invasion and occupation, the only sure way of neutralizing Iran's nuclear program for any extended period of time, is out of the question considering America's bloody, humbling, expensive and recent experience in Iraq."[159] A ground invasion is an ill-advised prospect considering Iran's geographic size, mountainous terrain, and 450,000 strong military.[160] It is unlikely that the U.S. could field sufficient ground forces to ensure a "stable" regime change and possible occupation should this be necessary.[161]

Air strikes could destroy some facilities but the survival of the Iranian nuclear regime is ensured by the retention of knowledge and experience and the ability to replace equipment and reconstitute efforts at smaller clandestine sites; Iran may already

[157] George Perkovich, "Sanctions on Iran-The Least Bad Option," Carnegie Endowment for International Peace,June 28, 2010, http://carnegieendowment.org/2010/06/28/sanctions-on-iran-least-bad-option/4ug (accessed May 2, 2011). Perkovich is the vice president for studies and director of the Nuclear Policy Program at the Carnegie Endowment for International Peace.

[158] Gwynne Dyer, "There's No Way for the U.S. to Win a Non-Nuclear War with Iran," *The Georgia Straight,* August 3, 2010, http://www.straight.com/article-336907/vancouver/gwynne-dyer-theres-no-way-us-win-nonnuclear-war-iran (accessed August 5, 2010).

[159] Zukowski, "The Nuclear Non-Proliferation Regime: Its Status and Prospects," 57.

[160] Dyer, "There's No Way for the U.S. to Win a Non-Nuclear War with Iran."

[161] James Devine and Julian Schofield, "Coercive Counter-Proliferation and Escalation: Assessing the Iran Military Option," *Defense and Security Analysis* Vol. 22. No 2 (June 2006): 141.

maintain “redundant capabilities for key centrifuge components” in anticipation of attacks.[162] Dyer concludes that considering these factors, short of a nuclear war on Iran, the prospect of a U.S victory is unlikely and this realization has kept such plans from materializing.[163]

Considering the political and strategic fallout that would accompany air strikes, the use of cyber attacks, with an assemblage of other covert initiatives, emerged as a viable alternative to impede Iranian nuclear development.[164] Early in 2008, the Israeli government made a “secret” request to the Bush administration to provide them with bunker-busting bombs capable of destroying underground facilities; refuelling equipment to allow them to fly to Iran and return to Israel; and permission to fly over Iraqi airspace.[165] According to Sanger, the Israeli resolve to attack may have been influenced by a 2007 National Intelligence Estimate that indicated Iranian engineers had been ordered to halt the development of nuclear warheads in 2003; such findings would preclude the possibility of “decisive” action against Iran before the Bush administration left office.[166] The Bush administration “deflected” Israeli requests for bombs and refuelling equipment and denied use of Iraqi airspace over concerns that it would lead to a “political uproar” in Iraq that may result in “the expulsion of American forces”. Should

[162] David Albright and Jacqueline Shire, “A Witches’ Brew? Evaluating Iran’s Uranium Enrichment Progress,” *Arms Control Today* 37 (November 2007) http://www.armscontrol.org/act/2007_11/Albright (accessed May 18, 2011).

[163] Dyer, “There’s No Way for the U.S. to Win a Non-Nuclear War with Iran.” Dyer observes that “The U.S. could ‘win’ by dropping hundreds of nuclear weapons on Iran’s military bases, nuclear facilities and industrial centres(ie cities) and killing five to 10 million people, but short of that, nothing works.”

[164] Farwell and Rohozinski, “Stuxnet and the Future of Cyber War,” 28-29. The authors briefly explore the political and strategic implications regarding why the Stuxnet approach was pursued versus a more direct approach such as pre-emptive air strikes.

[165] Sanger, “U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site.” the Israelis conducted exercises over the Mediterranean Sea that appeared to be “dry runs” for an attack on Natanz,

[166] Ibid. Of note is that the National Intelligence Estimate was based on “a trove of Iranian reports obtained by penetrating Iran’s computer networks.” The 2007 Intelligence Estimate was contrary to findings and evidence the Israelis purported to have and was viewed with equal suspicion by the Bush administration. Israeli intelligence believes that there are two parallel nuclear programs in Iran; “the program declared to the IAEA and a separate operation, run by the military and the Revolutionary Guards.”

the Israelis proceed with the Iraq fly-overs without American consent it was unclear if the American military would be ordered to shoot them down or if failure to do so would constitute a tacit blessing for the attack.[167]

One of the military pre-emptive strike options for Iran called for the use of bunker buster tactical nuclear weapons to penetrate underground Iranian nuclear facilities; however, serious misgiving arose from the Joint Chiefs of Staff and senior Pentagon officers regarding crossing the nuclear threshold.[168] Secretary of Defense Robert Gates and a number of other unnamed administration officials stated that: "any overt attack on Iran would probably prove ineffective, lead to the expulsion of international inspectors and drive Iran's nuclear effort further out of view."[169] There was also the prospect that American troops stationed in Iraq could become embroiled in a broader Middle East War[170]. Hertzberg echoes this assessment and notes that the bombing of Iran's fortified nuclear facilities would be the start of a war of "unknown duration and immense human, material, and political cost."[171] The assessments reviewed echo the sentiment that such air strikes may postpone Iran's acquisition of nuclear weapons for two to three years at an unacceptable cost.

A new covert push was pursed by the Bush administration as a result of the perceived failure of sanctions to decidedly curb Iranian uranium enrichment and in light of the fact that military strike options appeared "untenable." In an effort to "create leverage" against Iran, the Bush administration turned to the CIA to assist in slowing progress at Natanz and other "known and suspected nuclear facilities."[172] Despite hints

[167] Ibid.

[168] Hersh, "The Iran Plans."

[169] Sanger, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site."

[170] Ibid.

[171] Hendrik Hertzberg, "Iran and the Bomb," *The New Yorker*, December 13, 2010. http://www.newyorker.com/talk/comment/2010/12/13/101213taco_talk_hertzberg (accessed May 3, 2011).

[172] Sanger, "U.S. Rejected Air for Israeli Raid on Iranian Nuclear Site."

of potential Israeli military action in the fall of 2010,[173] other analysis suggests that the Israelis have been seeking ways to "cripple Iran's capability without triggering the opprobrium, or the war, that might follow an overt military strike of the kind they conducted against nuclear facilities in Iraq in 1981 and Syria in 2007."[174]

The expanded covert program to delay Iran's ability to produce nuclear weapons-grade fuel is broadly aimed at the "entire industrial infrastructure that supports the Iranian nuclear program" including efforts to "destabilize" centrifuges. The program 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."[175] Prior to leaving office in 2009, the Bush administration committed $300 million dollars toward such joint cover projects against Iran.[176] The clandestine program appears to have been "accelerated" under the Obama administration albeit what this entails remains shrouded in secrecy.[177] Importantly, the acknowledgment of clandestine efforts to engage in cyber attacks on Iranian computer systems provides some indication that indeed the U.S. is incorporating offensive cyber attack capabilities into its modus operandi. As Falkenrath aptly describes: Whether it's true or not, as far as the rest of the world is concerned the United

[173] Jeffrey Goldberg, "The Point of No Return," *The Atlantic,* September 2010, http://www.theatlantic.com/magazine/archive/2010/09/the-point-of-no-return/8186/ (accessed May 5, 2011). According Goldberg, Israel adopted a wait and see approach to the West's "non-military methods" to stop Iran and this "forbearance" was to expire in December, 2010. Goldberg explains in detail the existential threat that Israel perceives as emanating from Iran's nuclear goals.

[174] Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[175] Sanger, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site."

[176] Ewen MacAskill, "Stuxnet Cyberworm Heads Off U.S. Strike on Iran," *The Guardian,* September 25, 2010, http://www.guardian.co.uk/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran

[177] David Sanger, "Iran Fights Malware Attacking Computers," *New York Times,* 25 September, 2010, http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html (accessed May 8, 2011).

States is now in the business of offensive information warfare, along with China, Israel and Russia, among others."[178]

The Covert Battlefield: Pre-emption Incognito?

Stuxnet provides a "road map" for evolution of the cyber battlefield; one of the defining characteristics of this battlefield appears to be the obfuscation and invisibility of attacks. According to Langner, Stuxnet is a stealth control system that resides on target controllers alongside legitimate code; the attack code resides in the system and "monitors the hijacked process for extended periods of time before executing the strike" that neither legitimate program code or SCADA system notices.[179] Stuxnet's technical features allow for it to both infect and to reside on the target system undetected for long periods of time.

This suggests that the attack was not a pre-emptive strike designed to destroy the target in one decisive blow but a more nuanced form of incremental sabotage in which the gradual degradation of the targeted industrial equipment acted to deflect suspicion that something was askew. If indeed the target of the Stuxnet attacks was Iran's nuclear enrichment programme the equipment failures may not have signalled anything particularly abnormal was occurring; Iran regularly experiences periodic centrifuge failures emanating from faulty equipment design.[180] The ability to infiltrate a system and operate sub rosa whilst surely but steadily progressing towards the sabotage objective may indeed be an alluring prospect to those developing and employing offensive cyber weaponry. Depending on the strategic and political goals of such attacks, one does not need to "blow up generators", as in operation Aurora, to

[178] Falkenrath, "From Bullets to Megabytes."

[179] Langner, "How to Hijack a Controller: Why Stuxnet Isn't Just about Siemens' According to Langner, control is taken away from the legitimate control program by calling a conditional block end directive instead of passing control flow on to legitimate code.

[180] David Albright and Christina Walrond, "Iran's Gas Centrifuge Program: Taking Stock," *Institute for Science and International Security* (February 11, 2010), http://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock/8 (accessed Jun 5, 2011).

effectively strike at one's adversary; a slower methodical approach may achieve the same objectives by stealth.

Arguably, the success of such pre-emptive cyber attacks is contingent on covert subversion of the intended target. The failure of the Stuxnet attack appears to be the adoption of more zealous propagation methods that allowed the worm to spread vastly beyond its intended targets and hence increased the chance of its discovery. Once Stuxnet was detected, the worm's technical characteristics were analyzed and it was rather quickly neutralized. As Farwell and Rohozinski suggest, "Iran was able to quickly harness the intellectual capital of the global security community through effective crowdsourcing solutions to the worm, casting some doubt on the conventional wisdom and hype surrounding the efficacy of computer network attacks."[181]

Assessing the Effects of the Attacks on Iran's Nuclear Program:

> "A sophisticated half-megabyte of computer code apparently accomplished what a half-decade of United Nations Security Council resolutions could not."[182]

Following the Stuxnet attacks Iran's nuclear program did not grind to a halt. There appear to be conflicting assessments regarding the extent of damage to Iranian nuclear enrichment capacity, or other industrial installations, and whether the attack did substantially set back Tehran's nuclear enrichment program. Iran has acknowledged that facilities at Natanz were infected with the worm albeit public statements issued by Iranian authorities rebuff any speculation that Stuxnet was able to inflict any degree of damage at Natanz or other nuclear facilities. One account from an official at the Iranian Ministry of Communications and Information Technology indicates "the effect and damage of this spy worm in government systems is not serious and that it had been more or less halted."[183] This sanguine assessment is in contrast to a statement issued

[181] Farwell and Rohozinski, 27.
[182] Falkenrath, "From Bullets to Megabytes."
[183] Sanger, "Iran Fights Malware Attacking Computers."

by the deputy head of Iran's Information Technology who reveals that Iran anticipated to root out the "virus" within a one to two month timeframe but instead three new versions were spreading.[184] In November 2010, Iranian President Ahmadinejad conceded that the Stuxnet virus did "create problems for a limited number of our centrifuges with the software they had installed in electronic parts" but concluded: "the problem has been resolved." Iranian authorities have not elaborated further upon what the nature or extent of such problems may be."[185]

Stuxnet's impact on the Iranian nuclear enrichment programme cannot be evaluated and separated from the conjoined effects of economic and political sanctions and covert activities such as targeted assassinations.[186] It is beyond the parameters of this report to engage in a detailed history of the technical setbacks that have plagued the Iranian nuclear enrichment program. It is important to acknowledge that Iran routinely experiences technical difficulties, including with operating the archaic IR-1 centrifuges, and this is an important factor in continued delays and low-productivity levels associated

[184] Erdbrink and Nakashima, "Iran Struggling to Contain Foreign-made Stuxnet Computer Virus."

[185] Parisa Hafezi, "Iran Admits Cyber Attack on Nuclear Plants," *Reuters,* November 29, 2010, http://www.reuters.com/article/2010/11/29/us-iran-idUSTRE6AS4MU20101129 (accessed April 18, 2011).

[186] Leonard S. Spector, "Direct Action: The New Attacks on Iran's Nuclear Program," WMD Junction, James Martin Center for Non-proliferation Studies (March 26, 2011), http://cns.miis.edu/wmdjunction/110121_iran_direct_action.htm (accessed May 7, 2011). Spector is the deputy director of the Monterey Institute of International Studies at the James Martin Center for Non-proliferation Studies. Spector also serves as editor for the Non-Proliferation Review. According to Spector "direct action" refers to characterize destructive, often violent acts by anonymous individuals, groups, or governments to achieve political objectives, and refers to the range of activities beyond traditional diplomatic and political processes but short of overt armed conflict. Spector, "Direct Action," Spector notes that two direct actions have emerged so far against the Iranian program: the Stuxnet computer worm and attempts to assassinate two key scientists in the country's nuclear program(likely part of a wider assassination campaign stretching back several years).

with Iran's enrichment endeavours.[187][188] The compounding effects of sanctions, assassinations and inherent technical flaws with equipment and materials make it difficult to establish that cyber attacks alone have produced substantive effects to curtail Iran's nuclear aspirations.

In late 2009 and early 2010 Iran decommissioned and replaced about 1,000 centrifuges, out of 9,000 installed, at the Natanz. According to David Albright, this level of breakage "exceeded expectations and occurred during an extended period of relatively poor centrifuge performance."[189] In addition, the IAEA reported that in November 2010, Iran had stopped feeding uranium into centrifuges for a period of six days before again restarting the process.

[187] Albright and Walrond, "Iran's Gas Centrifuge Program: Taking Stock." According to the in 2008 fuel enrichment at Natanz experienced a drop in performance and evidently did not recover until early 2010. More information regarding this may be found at: http://www.isis-online.org/uploads/isis-reports/documents/IAEA_Iran_Report_Analysis_18Feb2010.pdf According to Albright, P-1 centrifuges are prone to excessive vibration problems which interfere with normal operations leading to shut downs and breakage. This is one of the reasons Urenco in the Netherlands stopped using these centrifuges. See http://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock/8 Jeffrey Lewis also suggests that Iranian UFC6 contains high concentrations of molybdenum and heavy metals which collect on centrifuge walls and cause them to unbalance as well as plug valves and pipes leading to malfunctions. See http://lewis.armscontrolwonk.com/archive/945/iran-focus-part-1-how-close-is-iran-to-the-bomb

[188] Albright and Walrond, "Iran's Gas Centrifuge Program: Taking Stock." According to the authors P-1 centrifuges are prone to excessive vibration problems which interfere with normal operations leading to shut downs and breakage. This is one of the reasons Urenco in the Netherlands stopped using these centrifuges. Jeffrey Lewis observes that Iranian UFC6 contains high concentrations of molybdenum and heavy metals which collect on centrifuge walls and cause them to unbalance as well as plug valves and pipes leading to malfunctions. See http://lewis.armscontrolwonk.com/archive/945/iran-focus-part-1-how-close-is-iran-to-the-bomb

[189] David Albright, Paul Brennan and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," International Institute for Science and International Security, December 22, 2010, http://www.isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed June,5 2011).

Despite these equipment failures, Iran has been able to maintain a "constant, stable out-put" of low enriched uranium by replacing and adding centrifuge capacity.[190] The cyber attacks may have worked in tandem with sanctions to impede Iranian enrichment activities. While Iran appears to have been able to replace the damaged centrifuges the shortage of embargoed specialized materials such as maraging steel and carbon fiber may affect its ability to both replace centrifuges and develop and adopt more advanced centrifuge models.[191] Albright notes "if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the Fuel Enrichment Plant (FEP), while making detection difficult, it may have succeeded, at least temporarily. If the goal was to quickly destroy all the centrifuges in the FEP, Stuxnet failed."[192]

In distilling the ambiguous information regarding the level of damage that Stuxnet inflicted it remains unclear why damage was limited to 1,000 centrifuges; there may be other control systems that inhibited Stuxnet from destroying the centrifuges and it is unclear whether Stuxnet seized control of the entire control system. In the event of a malfunction, the safety systems are designed to quickly empty the centrifuge of uranium hexafluoride; there is no code located in Stuxnet that appears to block this process from happening. It is plausible that safety systems independent of the control system targeted

[190] Joby Warrick, "Iran's Natanz Nuclear Facility Recovered quickly from Stuxnet Cyberattack," *Washington Post,* February 16, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html (accessed May 9, 2011). This point is also reiterated by Albright et all in "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report,". Albright notes that while Stuxnet delayed the Iranian centrifuge program at Natanz and contributed to slowing its expansion, it did not stop or even delay the continued buildup of low enriched uranium LEU.

[191] Editorial, "The Iranian Slowdown," *Washington Post,* January 13, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/12/AR2011011205566.html (accessed May 9, 2011). Albright reiterates this point in his analysis by noting that Iran may only have enough material to build 12,000 to 15,000 IR-1 centrifuges; thus the loss of 1,000 centrifuges to sabotage should not be underestimated even with continuing LEU enrichment levels. See Albright, supra note190.

[192] Albright, David, Paul Brennan and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," International Institute for Science and International Security, 15 February, 2011, http://www.isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/ (accessed May 9, 2011).

by Stuxnet did "intervene" to mitigate damage.[193] This point is critical, as while building fortified systems that are impenetrable to any form of cyber attack may be futile, it may be possible to ensure that redundant safety systems that can detect system changes or fluctuations may be able to mitigate both failures that occur due to emergency breakdowns, in events such as natural disasters, and cyber attacks. A key factor to mitigate against cyber attacks or other calamities is system resilience and the ability to "ride out" an attack, or other emergency, by being able to detect and isolate the problem from spreading into a system wide malfunction and having protocols to restore at least vital operations.

Collateral Damage:

The sequence of initial Stuxnet attacks commenced as early as June 2009. Since then, the worm has undergone several evolutionary mutations to arrive at its current form.[194] The first variant of the worm included measures to limit its spread and to remain close to the original infection point; this version remained undetected.[195] A second variant was introduced in March 2010 and included more advanced propagation mechanisms[196] that allowed it to spread and diffuse more widely on networks[197].[198]

[193] Ibid.

[194] For a technical discussion of Stuxnet variants refer to: Liam O Murchu, "W32. Stuxnet Variants," entry posted 04 August 2010, http://www.symantec.com/connect/blogs/w32stuxnet-variants

[195] Gregg Keizer, "Why did Stuxnet Worm Spread," *Computer World*, October 1, 2010,http://www.computerworld.com/s/article/9189140/Why_did_Stuxnet_worm_spread_ (accessed, November 18, 2010). The original infection method, which relied on infected USB drives, included a counter that limited the spread to three PC's. There was also a three week propagation window within which the worm could migrate to other machines before "calling it quits."

[196] The advanced propagation mechanisms included the addition of multiple Windows zero day vulnerabilities and the ability to spread, and update itself to the most recent version, via peer to peer networking. See references cited in Notes 11 and 12.

[197] This is the version of Stuxnet that was discovered by Belarusian security firm Virus Blokada in July 2010. This is also the version that has received extensive media coverage and has been the subject of technical analysis since July, 2010.

The aggressive propagation techniques used in the more advanced variant of Stuxnet are self-replicating which entails that "it's difficult to exercise complete control over where it goes, what it does, and how far it spread."[199] By adopting a more aggressive dissemination functionality the worm could disperse further to increase the likelihood of reaching designated targets however this approach sacrificed stealth and ensured that the this particular cyber weapon could not be used again upon discovery. Markoff speculates that perhaps a government "may have been so eager to stop the Iranian nuclear program that the urgency of the attack trumped the tradecraft techniques that traditionally do leave fingerprints, digital or otherwise."[200] The adoption of such an approach sacrificed attack stealth and increased the potential for collateral damage including the prospect of infection spreading to the nation or nations that developed and unleashed the attacks.[201]

The difficulties in limiting the spread of such attacks may conceivably result in a range of repercussions including death by digital friendly fire, inadvertent fratricide, and collateral damage; this undermines the notion that cyber attacks are akin to precision-guided cyber munitions. Unintended, and potentially large scale, collateral damage is a very real possibility considering the global diffusion of software and hardware technology

198 Keizer, "Why did Stuxnet Worm Spread." The code itself does not provide clues as to why more advanced propagation methods were introduced by the developers, however researchers suggest it is plausible the first variant did not reach its intended targets and hence failed to gain control of industrial systems

199 Aleksandr Matrosov et al., "Stuxnet Under the Microscope: Revision 1.31," *ESET*, http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf (accessed May 23, 2011).

200 John Markoff, "A Silent Attack but Not a Subtle One," *New York Times*, September 26th, 2010, http://www.nytimes.com/2010/09/27/technology/27virus.html (accessed November 19, 2011).

201 Keizer, "Why did the Stuxnet Worm Spread." Keizer quotes Kaspersky security expert Schouwenberg who notes that perhaps the developers knew their own critical infrastructure would not be impacted because they don't run the same hardware or software as the intended target.

and equipment used in both commercial and civilian and military government sectors. At time of writing, research findings indicate that Stuxnet successfully infected over 100,000 hosts spanning the globe albeit it is unclear as to how many of these systems were affected by the attack payload described in the above. There is a lack of publicly available information on the degree of disruption and damage caused by the attacks in affected countries.[202] It is unlikely that such information will be disclosed considering it may provide confirmation of success to the attack's perpetrators and may reveal critical information to adversaries, and would be attackers, regarding which sectors, agencies and systems are vulnerable to these types of cyber strikes. Silence and secrecy regarding system vulnerabilities may indeed constitute a form of passive cyber defense as would be attackers are denied purview to information they can then seek to exploit. However, formulating strategies and policy, at both the national and international levels, surrounding safeguards against and mitigation mechanisms for cyber attacks may require some degree of transparency, disclosure and debate, regarding discrepancies, deficiencies and failure, or lack of, appropriate and effective policy and security protocols.

The Strategic and Political Ramifications of the Stuxnet Attacks

Enter Stuxnet: the attack is able to manoeuvre within Iran's nuclear programme in ways that bomber squadrons and even nuclear weapons cannot. According to Langer, the chance of success in destroying targets using cyber attacks; "is as good as using explosives" and the attacks are relatively cheap and bloodless when considering the enumerated repercussions associated with pursuing military invasion and/or air strikes. The victim of the attack "has no idea how to retaliate" and may not be able to confirm that there was an attack, if at all. Importantly, the propitious advantage of Stuxnet is the ability to reach deeply submersed facilities and its apparent ability to target and sabotage clandestine ones. Langner argues that it can be assumed that the control

[202] CRS Report for Congress, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," by Paul Kerr, John Rollins, and Catherine Theohary." Congressional Research Service, December 9th, 2010, 3.

systems for any hidden centrifuge plants "are equipped with the same industrial control products and logic as the known plants."[203] Hence Stuxnet was able to hit both Natanz and Bushehr even if the latter poses only a negligible proliferation risk.

Spector identifies a number of advantages, for the perpetrators, in "directly damaging critical components of Iran's nuclear program without the open use of military force". Chiefly, to date, Tehran has been unable to conclusively determine who is behind the cyber attacks limiting its ability to make diplomatic appeals for support from the international community and few viable options to respond to and condemn those responsible. An overt Iranian military response, using means such as conventionally armed missile strikes on Israel is not feasible:

> "any such response could credibly be portrayed as an unprovoked attack and hand Israel and the United States a diplomatic free pass to retaliate decisively. Were Iran to intensify anti-US attacks in Iraq or orchestrate a resurgence of Hezbollah rocket launches on Israel, these too, might be treated as provocations that could trigger a powerful response."[204]

Stuxnet expands the toolkit of covert "direct action" employed vis a vis the Iranian nuclear program.[205] Stuxnet appears to pave the "new way forward" for future attacks that will use more sophisticated cyber sabotage and "may inflict more serious, longer-lasting damage." The covert program conveys determination to stop Iran's nuclear program, coupled with the ability to thwart Iranian nuclear efforts through physical interference, without the risk of military or diplomatic retaliation that "the overt use of armed force would entail."[206]

In assessing the utility of cyber attacks prudent consideration should be given to the political and strategic goals and conditions that such covert attacks achieve and

[203] Ralph Langner, "Better than Bunker Busters: The Virtual Chinese Water Torture," *Langner Blog*, entry posted 15 November 2010, http://www.langner.com/en/2010/11/15/better-than-bunker-busters-the-virtual-chinese-water-torture/ (accessed May 4, 2011).

[204] Spector, "Direct Action."

[205] Spector, "Direct Action."

[206] Spector, "Direct Action."

create or exacerbate. Indeed, the drums of war appear to be temporarily muted as both Israel and the U.S. have revised their estimates for Iran acquiring a nuclear weapons capacity. Mossad's former chief of intelligence, Meir Dagan, indicated to the Knesset Foreign Affairs and Defense Committee that Iran could not acquire a nuclear weapon before 2015 due to "unspecified technical problems."[207] The cyber attacks and a series of assassinations appeared to have "taken the pressure off" to pursue military actions at least in the short term.[208]

The strategic picture that is emerging in the aftermath of Stuxnet is that the cyber attacks have not vanquished or altered Iranian political resolve to continue enrichment suggesting that such tactics do not provide a panacea solution to induce Iran to change course. Spector credits the current intensification of sanctions and covert intervention for "bringing Iran to the negotiating table in December 2010 and again in January 2011."[209] A closer look at what occurred at these meetings indicates that progress towards getting Iran to suspend uranium enrichment remains elusive; the P5+1 offered a set of economic and technical aid programs if Iran agreed to stop enrichment. This was countered with Iran's continued assertion that they are in compliance with IAEA inspectors and their program is dedicated solely towards producing civilian energy. The Iranian position at the negotiations is summarized by Iran's ambassador to the IAEA: "Resolutions, sanctions, threats, computer virus nor even a military attack will stop uranium enrichment in Iran."[210]

Iran's motivation and reasons for pursuing nuclear enrichment remain including the tenuous and complex domestic political situation in which the splintered elites jockey to consolidate power. Indeed Iran's resolve appears to have intensified as most recent

[207] Editorial, "Iran's Nuclear Slowdown."

[208] Ewen MacAskill, "Stuxnet Cyberworm Heads off US Strike on Iran."

[209] Spector, "Direct Action."

[210] Steven Erlanger, "Little Progress is Seen in Iran Talks," *New York Times,* January 21, 2011, http://www.nytimes.com/2011/01/22/world/middleeast/22nuke.html (accessed May 5, 2011).

developments indicate that Iran is proceeding with tripling the production of 20 percent enriched uranium, transferring such enrichment processes to its Fordow plant.[211]

Secondly, the Stuxnet attacks have revealed, but more likely confirmed, the inconsistencies and contradictions of pursuing sabotage against Iran whilst engaging in seemingly "good faith" diplomatic negotiations. Cirincione argues that the Obama administration's Iran strategy can be dubbed "Engage, Sanction and Sabotage" however such measures alone cannot compel Iran "into either compliance or collapse."[212] Arguably, keeping a negotiations channel open and encouraging Iran to increase transparency regarding its activities to the IAEA while concurrently pursuing a continuation of the Bush era covert sabotage program against the Iranian regime and nuclear programme appears to be counter-productive. Cirincione notes that the Iranian regime should be given a "face-saving way out" of the current nuclear conundrum that provides a "negotiated solution that can guarantee its security and allow a resumption of normal diplomatic and economic relations."[213] A recent study by the Stimson Centre recommends a re-balancing of the dual track approach to Iran a policy of strategic engagement based on comprehensive set of incentives for Iran, including the conditional acceptance of enrichment, for a mutually acceptable agreement on the nuclear issue, including conditional acceptance of enrichment.[214] The current sanctions regime needs to be matched with "equal readiness" by the U.S. and its allies to offer Iran incentives

[211] Peter Crail, "Iran to Boost 20% Enriched Uranium Output," *Arms Control Today*, July/August 2011, http://www.armscontrol.org/act/2011_%2007-08/%20Iran_to_Boost_Enriched_Uranium_Output (accessed August 3, 2011).

[212] Joseph Cirincione, "U.S. Strategy on Iran is Working," Ploughshares Fund, posted January 18, 2011, http://www.ploughshares.org/news-analysis/blog/us-strategy-iran-working (accessed May 5, 2011).

[213] Cirincione, "U.S. Strategy on Iran is Working."

[214] Barry, Blechman, Daniel Brumber and Steven Heydemann, *Engagement, Coercion and Iran's Nuclear Challenge: A Report of a Joint Study Group on US-Iran Policy,* Stimson Centre, November 16, 2010, http://www.usip.org/files/resources/Engagement_Coercion_and_Irans_Nuclear_Challenge.pdf (accessed May 18, 2011).

that are aimed at a broad spectrum of Iran's ruling elite.[215] The recommendations for strategic engagement include readiness to reduce and eliminate sanctions concomitant with progress on the nuclear issue and provision of assistance to Iran in modernization and rebuilding of its oil and gas industry. The normalization of relations could also include bilateral or multilateral dialogue on regional non-nuclear subjects of mutual concern including Afghanistan, regional energy co-ordination, and drug trafficking and regional security. Importantly, the U.S. "should be prepared to accept Iranian uranium enrichment within tightly controlled and verifiable limits on level and volume, as part of a package of arrangements that include clarification of outstanding questions concerning Iran's nuclear program and weapons-related activities."[216] The U.S. could then proceed with a more ambitious plan of advocating for internationalized global fuel services to replace nationally controlled enrichment as a solution to long-term energy issues in the region. This could be linked to a wider initiative to build conventional national gas and electricity grids in the region in lieu of nuclear options.[217]

While the cyber attacks may provide marginal intervals of time for diplomatic interaction to unfold, they also serve to derail any such process by ensuring that diplomatic overtures are viewed as duplicitous tactics. Cyber attacks may be "bloodless and cheap" but they serve to exacerbate existing tensions and may drive Iran's nuclear program further underground. The alluring appeal of being able to destroy physical targets via cyber attacks with relative impunity is not lost on other nations that may be contemplating such "direct action" adversaries. The difficulties in being able to detect an attack, determine attribution, and devise an appropriate response are equally confounding whether it is the Iranian nuclear program that is struck by Stuxnet or a component of the U.S. electricity grid that fails due to cyber assault.

[215] Blechman et al caution against pandering to any one economic, political or strategic interest within Iran's ruling elite. "Engagement, Coercion and Iran's Nuclear Challenge: A Report of a Joint Study Group on US-Iran Policy,",8.

[216] Blechman et al, "Engagement, Coercion and Iran's Nuclear Challenge: A Report of a Joint Study Group on US-Iran Policy," 21.

[217] Blechman et al, "Engagement, Coercion and Iran's Nuclear Challenge: A Report of a Joint Study Group on US-Iran Policy," 8.

Chapter 5-Unraveling the Strategic Ambiguities and Implications of Cyber "War"

Analysis of the strategic implications surrounding the deployment and use of cyber "weapons" is still very much embryonic and evolving. The lack of an intellectual framework regarding the strategic use and implications of cyber weapons is analogous to the period of uncertainty and strategic novelty of the early 1950s and the nascent debates on nuclear weapons.[218] Libicki cautions that "cyberspace must be understood in its own terms, and policy decisions being made for these and other new commands must reflect such understanding. Attempts to transfer policy constructs from other forms of warfare will not only fail but also hinder policy and planning."[219]

This discussion asserts that it is by exploring the parallels of cyber attacks to nuclear and biological weapons that the unique characteristics of cyber attacks may be discovered and highlighted. In this analysis, I examine the challenges and complexities that cyber attacks pose to traditional arms control approaches. I then establish that cyber attacks will likely serve as subsidiary or auxiliary aspects of military campaigns using traditional kinetic technologies. I conclude the project with exploring the ramifications surrounding the development and use of cyber attacks on nuclear deterrence relationships and crisis stability.

[218] James A. Lewis, "The Korean Cyber Attacks and their Implications for Cyber Conflict," *Center for Strategic and International Studies* (October 2009), 2 http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict (accessed July 5, 2011) and Jean-Loup Samaan, "Cyber Command," 18.

[219] Martin Libicki, *Cyberdeterrence and Cyberwar,* xiii

Parallels to Nuclear Weapons

While acknowledging the low level of knowledge and dearth of analysis surrounding cyber "weapons," Samaan cautions that this is where the similarities between cyber warfare and the dawn of the nuclear age may start and end.[220] The application of the nuclear strategy paradigm, and the attendant concepts of first strike capability, second strike capability, and deterrence, may not be an appropriate conceptual or doctrinal framework for analyzing the strategic implications of cyber warfare. The use of analogies may aid in understanding and explanation of phenomena but it may also box issues into a rigid conceptual frameworks that precludes relevant assessment of cyber attack attributes, capabilities and attendant strategic implications.

Morgan observes that like the early Cold War, "discussion about how a conflict would go and what it will take to deter it is largely hypothetical." Morgan elaborates "there is considerable secrecy now about American cyber attack capabilities and their survivability for purposes of retaliation. The U.S. is widely believed to have the best capabilities in the world, but little is available about how robust they would be after a major attack."[221]There are a number of reasons why such comparisons warrant careful reflection. It is unclear how survivability could apply to cyber attacks considering such attacks are not a force or fleet but techniques and methods, rather than tangible and quantifiable armament entities, located in silos or launchers that can be detected and destroyed. Upon detection, plugging system vulnerabilities may neutralize cyber attacks; in this sense targeted systems survive following an attack as functions can be restored however Morgan refers to the survivability of cyber attack "capabilities." According to Libicki, counterforce and pre-emption does not apply in cyberspace as "command and control can be simultaneously hosted in redundant servers, killing any one server may be pointless."[222] Striking back would confer little protection[223] as it would not prevent or

[220] Samaan, "Cyber Command," 19.

[221] Patrick Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm" in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council, 2010.

[222] Libicki, "Cyber Security and Cyber Deterrence."

eliminate the system vulnerability exploited with the attack; rather the focus should be on utilizing back up processes, and redundant systems, to restore function. Even if the U.S. were to suffer a hypothetical cyber attack with a destructive payload, to civilian or military infrastructure, it is unclear why or how this would degrade its own capacity to exploit vulnerabilities in an adversary's systems. The notion of second-strike capabilities in cyberspace is of questionable merit considering the victim is not limited to retaliation in the cyber realm and could employ its conventional, and perhaps nuclear arsenals in retaliation.

A "second strike capability" is contingent on knowing whom the attacker is to ensure the possibility and plausibility of retaliatory action against it; retaliation against cyber attacks is complicated by the fact that attribution in cyberspace is difficult it at all possible. One cannot fire back if it is unknown and unclear who is attacking you, and what damage has occurred, irrespective of the toolkit of "survivable" weapons available to the victim to retaliate with.

Colonel Charles W. Williamson III argues that the U.S. currently lacks a credible deterrent strategy in cyberspace and should replace an antiquated fortified firewall defense approach to cyberspace with a flexible deterrent strategy emphasizing the ability to strike the enemy while "he is still on the move." To this effect Williamson recommends developing a power projection capability in the form of a af.mil robot network (botnet) that can direct massive amounts of traffic to target computers and render them ineffective.[224] Williamson postulates that the strategy would be akin to air base defense, which involves the necessity of finding the enemy and destroying his planes on the ground before they launch (strategic bombing). The recommendations put

[223] Libicki, "Cyber Security and Cyber Deterrence."

[224] Col. Charles W. Williamson III, "Carpet Bombing in Cyberspace: Why America Needs a Military Botnet," *Armed Forces Journal,* May 2008, http://www.armedforcesjournal.com/2008/05/3375884 (accessed May 3, 2011).

forth by Williamson acknowledge that the U.S. may find itself defending against an attack from a computer that was "co-opted" by an attacker and that this may result in a defensive denial of service attack on a neutral country. Williamson contemplates that the political ramifications of said actions may be "difficult to manage" and the U.S. may need to consider claims for compensation if warranted.[225] The suggestions amount to the equivalent of retaliatory cyber shots in the dark; it is unclear how adversaries will be deterred if they cannot be properly identified and retribution vis a vis the real culprit is unlikely. Arguably unleashing cyber "bolts from the blue" on unsuspecting neutral countries may unleash diplomatic crises that will indeed be rather difficult to manage considering such attacks may engender new hostilities and start new crisis.

According to Miller et al, the use of analogies and comparison of the cyber battle space to previous periods and conflict can be misleading. In comparison to the development and maintenance cost of conventional and nuclear strategic forces, the relative low costs of developing and deploying cyber attack capabilities creates asymmetric advantages. Missions capable units can be created quickly, under stealth, and capabilities remain masked or hidden before use. As effective use, rather than physical control are key to functioning in the cyber battle space, any rhetoric regarding the domination or control of the cyber sphere is unrealistic.[226]

One of the escalatory dangers of analyzing cyber attacks within the nuclear strategy paradigm is that this framework distorts and imbues such attacks with strategic effects endogenous to nuclear weapons rather than a realistic examination of the features, properties and limitations of cyber attacks.

Parallels to Biological Weapons

Cyber attacks share many of the characteristics of biological weapons namely they are developed and deployed in secret, suited for covert delivery, and difficult to

[225] Williamson, "Carpet Bombing in Cyberspace."
[226] Miller et al., "Cyber War: Issues in Attack and Defense," 20.

attribute to an attack source. The speed and spread of both biological weapons and cyber attacks is difficult to control and may produce collateral damage with the possibility of blowback against the attacker and neutral third parties. Biological weapons and cyber attacks utilize multi-use technology making it difficult to ascertain the capabilities, intentions and motives of the developers. Consequently it is problematic to determine misuse of technology for hostile purposes and to obtain an accurate assessment of a state's capabilities and intentions.[227] The parallels drawn between cyber attacks and biological weapons illuminate the destabilizing effects of cyber weapons on international security, the difficulties with devising deterrence strategies against such threats and the obstacles to developing and implementing effective arms control measures to proscribe their use.

A confounding dilemma surrounding the proliferation of biological weapons is that the multi-use nature of skills, abilities, materials and technology "to produce biological weapons are also necessary to develop defenses against them and to conduct civilian activities such as biomedical research and pharmaceutical production."[228] The obstacles to verifying biological arms control are rooted in the fact that nations can disguise biological weapons research and development in civilian institutes tasked with legitimate pharmaceutical and medical research.[229] Secondly, research that is undertaken for defensive purposes against natural biological agents and their weaponized variants cannot be differentiated from research undertaken to develop such agents as weapons. This is because at the research and development stage "the same equipment, materials, technologies, and techniques are used for both types of research."[230] Indeed both civilian defensive and biological weapons programs would involve testing the infectious agents to vaccine effectiveness and decontamination procedures.[231] This overlap

[227] Gregory Koblentz, *Living Weapons: Biological Warfare and International Security* (Ithaca, NY: Cornell University Press, 2009), 6.

[228] Koblentz, *Living Weapons: Biological Warfare and International Security*, 5.

[229] Koblentz, *Living Weapons: Biological Warfare and International Security*, 66.

[230] Koblentz, *Living Weapons: Biological Warfare and International Security*, 67.

[231] Koblentz, *Living Weapons: Biological Warfare and International Security*, 68.

between defensive and offensive capabilities can mask an offensive biological weapons program.

The lines between offensive and defensive capabilities in cyber space are indistinguishable; the information used to build both defensive and offensive capabilities involves an identical process of finding and exploiting information system vulnerabilities. Fulghum describes that in 2007 Idaho National Laboratory created a 21-line piece of software code dubbed the "Aurora test" that introduced destructive instructions into a closed computer network and caused the generator to blow up.[232] For defensive purposes, such vulnerabilities are sought out and patched while offensive attacks would exploit such vulnerabilities to deliver the intended payload.

Biological weapons have several advantages for being used in surprise attacks namely they are "relatively easy to develop in secret, are well suited for covert delivery, and do not provide signatures that can be used to easily identify the attacker."[233] As evidenced in the Stuxnet case study, cyber attacks were used as part of a covert plan likely designed to sabotage the Iranian nuclear enrichment programme albeit who orchestrated such attacks is debatable. There is nothing that reverse engineering the Stuxnet code has produced that suggests attribution to a definitive party is possible.

According to Koblentz, biological weapons depend on the element of surprise for their success because "the ability to conceal the identity of an agent, the timing of an attack, the means of delivery, and the planned target is crucial for an effective BW attack."[234] The existence of a cyber attack capability is contingent on being able to surreptitiously survey and infiltrate information systems to exploit a vulnerability that the target does not know about and to deliver a payload that disrupts or degrades the

[232] David Fulghum, "Cyber Attack Turns Physical," *Aviation Week and Space Technology*, September 28th, 2010, http://www.aviationweek.com/aw/generic/ (accessed May 15, 2011).

[233] Koblentz, *Living Weapons: Biological Warfare and International Security*, 26.

[234] Koblentz, *Living Weapons: Biological Warfare and International Security*, 27.

intended target system without detection; upon detection of intrusion or attack the target system operator may employ counter measures to resolve the vulnerability.[235]

Both biological weapons and cyber attacks are not suitable as strategic deterrents as this requires "the capability of the target of a surprise attack to reliably inflict unacceptable damage in retaliation against its attacker."[236] Koblentz notes that the effects of biological weapons are delayed, variable and difficult to predict; a number of countermeasures may be mustered either before or following a biological attack; and the secret nature of biological weapons programs negates the ability to issue credible threats of unacceptable damage vis a vis an adversary. [237] Similarly, the secrecy required to carry out cyber attacks negates a state's ability to make credible deterrent threats that an unacceptable level of damage will be inflicted vis a vis adversaries. While there is no effective defense against nuclear weapons, vaccines and antibiotics may be marshalled against biological attacks. Cyber attacks generate temporary effects as countermeasures may be readily employed upon attack detection.[238] Cyber weapons remain unknown until used and "weapon effects cannot be considered independent of the adversary's vulnerabilities and its ability to recover."[239] In summary, a potential adversary cannot be deterred "if the intention and capabilities to implement the strategy are unknown." [240]

There is some nascent indication that the U.S. military wants to transition from defending against cyber attacks to deterring assaults by threatening retaliation with both cyber weapons and kinetic weapons.[241] However, deterrence against cyber attacks

[235] Libicki, *Cyberdeterrence and Cyberwar*, xv.

[236] Koblentz, *Living Weapons: Biological Warfare and International Security,* 40.

[237] Koblentz, *Living Weapons: Biological Warfare and International Security*, 40-42.

[238] Libicki, *Cyberdeterrence and Cyber War*, xv.

[239] Libicki, *Cyberdeterrence and Cyberwar*, 126.

[240] Koblentz, *Living Weapons: Biological Warfare and International Security*, 42.

[241] Julian Barnes and Siobhan Gorman, "Cyberwar Plan has New Focus on Deterrence," *The Wall Street Journal*, July 15, 2011. http://online.wsj.com/article/SB10001424052702304521304576446191468181966.html (accessed August 7, 2011).

remains an elusive prospect namely due to the difficulties of attributing cyber attacks to a specific party. In its basic form deterrence is manifest in a psychological relationship in which "the goal is to shape an opponent's perceptions, expectations, and ultimately its decisions about launching an attack."[242] As Libicki notes, deterrence has to "work in the mind of the attacker" and is a function of "whether the attacker believes the threat to retaliate will be carried out and the potential damage that will result if and when the retaliation occurs." [243] In cyberspace such considerations are complicated by a number of factors. Revealing an access path back to the source of the attack may be possible but it does not confirm attribution to the actual party responsible for such attacks.[244] Cyber attacks may be launched from and routed through compromised computers that function as botnets. Locating a specific computer that launched the attack does not entail this activity was orchestrated by or for a government entity. Unlike other weapons systems, cyber attacks may be developed and deployed by a medley of state and non-state actors whose activities are not "functionally distinguishable;" "one cannot readily tell whether a cyber-attack originated from a civilian hacker, a cyber-criminal, or a military or intelligence agency." [245]

A deterrence posture premised on retaliation and increasing military capabilities is not effective in cyberspace; "If you cannot tell who did it or even communicate what the damage was, you also cannot tell who did not do it or what the damage could have been."[246] Libicki and Lewis conclude that deterrence is a problematic strategy against cyber threats and recommend increased attention to defense and system resiliency in the face of attacks.[247] Libicki concludes that before contemplating deterrence as a

[242] Patrick Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,"56.

[243] Libicki, *Cyberdeterrence and Cyberwar*, 8.

[244] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, 138-139.

[245] Paul Meyer, "Cyber Security Through Arms Control," *The RUSI Journal,* 156:2, 22.

[246] Libicki, *Cyberdeterrence and Cyberwar,* 51.

[247] James Lewis, "Cross-Domain Deterrence and Credible Threats," *Center for Strategic and International Studies,* July 2010, http://csis.org/publication/cross-domain-deterrence-and-credible-threats (accessed July 5, 2011).

primary response to the threat of state-sponsored cyber attacks "the United States may first want to exhaust other approaches, such as diplomatic, economic, and prosecutorial means." [248]

There are a number of reasons why biological weapons have rarely been used including normative barriers to the use of disease as a weapon, the logistical difficulties involved in storage and handling of such weapons and fear of retaliation or escalation of a conflict.[249] These types of normative constraints associated with a normative taboo or opprobrium against use do not influence conduct in cyberspace considering the ongoing background noise of cyber espionage. Governments and non-state actors regularly penetrate and exploit networks and systems to exfiltrate information. The initial phases of cyber espionage and cyber attack both require exploitation of system vulnerability; "an implant designed to purloin information may be indistinguishable from an implant designed to disrupt systems or corrupt information."[250] The only technical difference between cyber espionage and cyber attacks is the former exploits the vulnerability to obtain information whilst leaving the operational integrity of the system intact while cyber attacks would use a payload to disrupt or degrade computer systems or networks. [251]

With biological weapons it is difficult to ascertain whether a program is used for peaceful vaccine or nefarious weapons purposes. In the cyber realm, it would be difficult to discern that there is an active offensive program short of admission of such capabilities by the relevant protagonists. In fact the only publicly available information surrounding the sophistication of the American cyber offensive capabilities is recent disclosure by the Pentagon that they have developed a classified list of capabilities,

[248] Libicki, *Cyberdeterrence and Cyberwar*, 177.

[249] Koblentz, *Living Weapons: Biological Warfare and International Security,* 49.

[250] Libicki, *Cyberdeterrence and Cyberwar*, 24.

[251] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, 10-11.

including “viruses that can sabotage an adversary’s critical networks,” along with the requisite executive approvals for their use.[252]

While the Biological Weapons Convention prohibits the development, production, stockpiling, acquisition and retention of biological weapons, the difficulties in determining whether a program is used for peaceful civilian or military weapons purposes renders the Biological Weapons Convention a ‘toothless’ arms control treaty’[253] and serves as a cautionary tale for advocates of cyber arms control.[254] Cyber attacks are computer code that can be infinitely replicated and stored in encrypted form in multiple locations and may be launched from any number of multiple unknown locations. Lewis elaborates that the technologies used in cyber attacks are commercially sourced and easy to attain thus nullifying the notion that “precursors” to weapons can be controlled. Secondly, the close links between cyber attack and cyber espionage “makes countries reluctant to discuss or even admit they possess cyber attack capabilities.”[255] This renders that strategic arms agreement precedents based on calculable definitions of the development, production and stockpiling of weapons are not applicable in cyberspace.[256] Chyba adds that preventing the spread and proliferation of cyber weapons is “insurmountably difficult” and “renders traditional inspection approaches absurd.” [257]

252 Ellen Nakashima, “List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare.”

253 Koblentz, *Living Weapons: Biological Warfare and International Security*, 54.

254 Koblentz, *Living Weapons: Biological Warfare and International Security*, 61. The parties to the convention Biological Weapons Convention have been unable to agree on mandatory transparency measures, as compromise has not been reached pertaining to “the scope of required declarations, the extent and intrusiveness of inspections, the degree of protection afforded to proprietary information, and restrictions on trade in biotechnology.”

255 James Lewis, “Multilateral Agreements to Constrain Cyberconflict,” *Arms Control Today*, June 2010, http://www.armscontrol.org/act/2010_06/Lewis (accessed July 5, 2011).

256 James Lewis, “Multilateral Agreements to Constrain Cyberconflict.”

257 Christopher Chyba, “Toward Biological Security,” *Foreign Affairs*, Vol.81 No.3 (May/June 2002), 125.

Understanding Cyber Attacks

There are some unique attributes of cyberspace that complicate the application of historical analogies. Libicki notes that there is no forced attack entry into cyberspace. Unlike, other domains of warfare, organizations are vulnerable to cyber attack insofar as their networks and pathways into the system are exposed and this can be controlled and corrected for.[258] Therefore the vulnerabilities of systems and targets are not static but shift and change according to the ability to secure systems and to identify and employ countermeasures against attacks. It is not possible to ascertain what cyber weapons an adversary may possess in its "arsenal" until such weapons are used. The attacker's capabilities are contingent on the existence and extent of system and organizational weaknesses and failures; they cannot be quantified according to type and destructive payload yields a priori. While a toolkit of potential cyber weapons methods exists in the form of various virus and malware applications, their efficacy against an adversary is contingent upon being able to exploit and manoeuvre within their networks and systems and to do so undetected.

Many uncertainties exist surrounding the employment of cyber attacks to fulfill mission objectives. As Libicki notes, permanent effects are hard to produce with cyber attacks as they are "enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities;" the ambiguities of launching cyber attacks entail that the attacker cannot be certain of what they achieved and whether they can do it again.[259] According to the National Research Council, understanding the effects of cyber weapons remains a challenge considering that:

> "the smallest change in the configuration and interconnection of an IT system can result in completely different system behavior, and the and the direct effects of a cyber attack on a given system may be driven by the behavior and actions of the human system operator and the specific

[258] Libicki, Cyberdeterrence and Cyberwar, xiv.

[259] Libicki*, Cyberdeterrence and Cyberwar*, Preface.

> nature of the system as well as the intrinsic characteristics of the cyber weapon involved."[260]

Paradoxically, the unknown and unintended effects arising from the complexity of planning and executing cyber attacks mean that the attack may both fail to deliver the intended payload, or may be discovered and neutralized by the target operators, whilst concurrently producing cascading tertiary and secondary effects, that cannot be reliably predicted.[261] Unlike kinetic weapons there is no weapons yield calculation that could provide a modicum of certainty regarding how far such attacks can spread; they "may operate at time scales ranging from tenths of a second to years" at spatial scales which are difficult to predict and they can be used with "high degrees of anonymity and with plausible deniability."[262] Importantly, even after the attack "neither the attacker nor even the target may know for sure what the damage was."[263]

Prudent reflection regarding the strategic objectives and effects of launching such attacks is warranted as the probability of digital blowback against one's own systems and that of neutral third parties is a possibility.[264] According to Lewis, the prospect of attack damage spreading beyond the intended target may be unavoidable in an intertwined, interdependent and crowded cyber environment of combatants, non-combatants, allies, friends and neutral third parties.[265] This vein of analysis is expanded upon by Sommer and Brown who note that the levels of mutual dependence and interconnectedness appear to be limiting factors for those contemplating the use of cyber attacks as "outcomes from the deployment of a succession of large numbers of

[260] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, 122.

[261] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, 20.

[262] National Research Council, *Technology, Policy, Law and Ethics Regarding the U.S. Acquisition and Use of Cyber Attack Capabilities*, 2.

[263] Libicki, *Cyberdetterence and Cyberwar,* 52.

[264] OECD, *Reducing Systemic Cyber Security Risk*, 47.

[265] Lewis, "The Korean Cyber Attacks and Their Implications for Cyber Conflict,"2.

powerful attacks are very uncertain; self damage is a real possibility."[266] Considering the uncertainties surrounding the consequences of a "counter strike" against innocent third parties, this makes it difficult to authorize cyber attacks. It is worth noting that the cyber attacks described below, both hypothetical and realized, were used as force multipliers in conjunction with electronic jamming and conventional firepower.

During the 1999 NATO Kosovo intervention, American military used cyber attacks against Serbian telecommunications network that apparently "hampered" the Intelsat satellite communications system.[267] In the lead up to the 2003 Iraq invasion, the risk of unpredictable collateral damage appears to have informed the Bush administration's restraint in fulfilling Pentagon and American intelligence agencies' cyber attack plans to freeze Saddam Hussein's bank accounts. There was fear that the repercussions of doing so would spread beyond Iraq's borders and result in "worldwide financial havoc."[268] More than a decade earlier, during Gulf War I, similar concerns, surrounding the effects on banking, communications and financial systems, appear to have foiled plans to pursue cyber attacks vis a vis Iraq. According to Fulghum, the integrated KARI air defense system was designed and installed in Iraq by the French; the system was integrated with the Iraqi national computer system and perhaps had links to French domestic networks.[269] However, the risk of collateral damage appears to inform and limit, but not prohibit cyber attacks. The Bush administration did authorize electronic jamming and digital attacks against Iraq's telephone networks in 2003 that did produce collateral damage as they temporarily disrupted telephone service in

[266] OECD, *Reducing Systemic Cyber Security Risk,* 82.

[267] John Markoff and Thom Shanker, "Halted 03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times,* August 2, 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html (accessed April 18, 2011).

[268] Markoff and Shanker, "Halted 03 Iraq Plan Illustrates U.S. Fear of Cyber War Risk."

[269] David Fulghum, "What is a Weapon?" *Aviation Week and Space Technology*, Vol. 171 No.12 (September 28, 2009), 60-61.The article does not explain how Iraqi and French networks could be linked apart from the use of similar hardware. However, this consideration did foil cyber attack plans on Iraq. According to a U.S. Air Force General quoted in the article: "We were afraid we were going to take down all the automated banking machines in Pairs."

neighbouring nations that shared Iraq's cell-phone and satellite telephone systems.[270] Balancing mission objectives against difficult to predict collateral damage effects will remain as vexing concern as states develop and incorporate cyber weapons into their military arsenals.

Measured Approaches: Cyber Attacks as Auxiliary Components of Military Campaigns

Measured approaches to the cyber strategic debate attempt to carve out an analytical middle ground that recognizes considerable damage may be inflicted through cyber attacks while engaging in a critical appraisal of cyber capabilities, doctrine and case study evidence to establish that cyber attacks are "valuable" but not decisive tools of military action.[271] Samaan notes that the belief cyber attacks could defeat a country, or that they present an existential threat to it, are both flawed and dangerous and the notion that *cyber warriors* could fight in a cyber frontier without physical implications is quixotic.[272] A Chatham House report chastises the notion that cyber warfare can be a "painless and bloodless" form of conflict that delivers "decisive outcomes." The authors caution "victory and defeat are far from recognizable in cyberspace."[273]

Samaan's critique forms part of a body of emerging analysis, discussed below, that deflates the notion that war can be fought strictly in cyberspace but rather sees cyber attacks as force multipliers, enablers, means of denial, or as tools of psychological intimidation. Importantly such attacks constitute part of broader military campaigns involving kinetic weapons. Samaan argues that there are no "autonomous" cyber wars but rather cyber attacks are "subsidiary additions" to conventional kinetic military

[270] Markoff and Shanker, "Halted 03 Iraq Plan Illustrates U.S. Fear of Cyber War Risk."

[271] Jean-Loup Samaan, "Beyond the Rift in Cyber Strategy," *Strategic Insights* Vol. 10 Issue 1 (Spring 2011): 4

[272] Samaan, "Beyond the Rift in Cyber Strategy,"4 and 10.

[273] Paul Cornish et al., *On Cyber Warfare,* Chatham House Report, November 2010, 3, http://www.chathamhouse.org/publications/papers/view/109508 (accessed March 25, 2011).

operations and are part of larger military campaigns.[274] Sommer and Brown concur with this assessment as they note cyber attacks may be used in combination with or "blended simultaneously with conventional kinetic weapons as force multipliers;" they do however acknowledge that stand-alone cyber attacks may be pursed.[275] Cornish et al concur that cyber attacks function as force multipliers as part of broader "strategic ways and means" employed by states to achieve objectives; as such, they are more likely to occur in conjunction with other methods. The authors doubt the prospect of "cyberwarfare" as an independent occurrence.[276]

The likelihood of a "true cyber war" is questionable considering that "there is no strategic reason any aggressor would limit themselves to only one class of weaponry."[277] Lewis echoes these sentiments by noting that a "pure cyber war" that is limited to cyber volleys is unlikely as such attacks do not produce decisive compelling effects that "damage an opponent's will and capacity to resist. Consequently, no one would plant to fight using only cyber weapons."[278] Libicki buttresses these conclusions by noting that cyber weapons can only be used as support functions for other elements of warfare considering that they do not directly harm individuals or equipment and their use "at best" would temporarily confuse operators of military systems. Libicki concludes: "attempting a cyberattack in the hopes that success will facilitate a combat operation may be prudent; betting the operation's success on a particular set of results may not be"[279] as "strategic cyberwar by itself would annoy but not disarm an adversary."[280]

Inevitably, as warfare in cyberspace "must be accompanied by warfare in one of these domain to lead to physical effects,"[281] the designation of cyberspace as an

[274] Samaan, "Beyond the Rift in Cyber Strategy,"9- 10.
[275] OECD, *Reducing Systemic Cybersecurity Risk*, 6.
[276] Cornish et al.,11.
[277] OECD, "*Reducing Systemic Cyber Security Risk,"* 6.
[278] James Andrew Lewis, "Cyber Attacks, Real or Imagined, and Cyber War."
[279] Libicki, *Cyberdeterrence and Cyberwar,* xv.
[280] Libicki, *Cyberdeterrence and Cyberwar,* xix
[281] Samaan, "Beyond the Rift in Cyber Strategy," 4.

individual domain, akin to land, sea, or air has come under fire. Samaan argues that cyber attacks should be analyzed and incorporated into a "joint" analysis of military campaigns within which cyber attacks are part of defense or offensive engagements "in the process of a larger naval, air or land campaigns."[282] An exploration of the mysterious Israeli air raids on Syria in 2007 illuminates some of the ways in which cyber attacks are incorporated into military missions. In September 2007, non-stealth Israel aircraft[283] slipped past Syrian air defense undetected and carried out an aerial bombing mission on a suspected clandestine Syrian nuclear complex.[284] En route to the target at Dayr as Zawr, the Israelis engaged a single Syrian radar site near the Turkish border using electronic attack jamming techniques and cyber attack; this caused the Syrian radar system to "go off air" during the aerial bombing raid that ensued.[285] Israel employed a "network invasion capability" similar to the U.S. "Suter"[286] system that shoots data streams laced with algorithms into enemy antennas; a surveillance aircraft was concurrently employed to monitor "enemy signals to ensure the data streams were

[282] Samaan, "Beyond the Rift in Cyber Strategy,"4. According to Samaan, cyber attacks have dubious utility in coercing an opponent let alone posing an existential threat to their survival.

[283] David Fulghum, Robert Wall and Douglas Barrie, "All Arms Attack," *Aviation Week and Space Technology*, Vol 167 Issue 18 (November 5, 2007): 32-33. The authors note that Israel used two person Lockheed Martin F-16I aircraft in which one operator focuses on targeting and electronic warfare and the pilots focuses on flying and evading air defenses.

[284] Seymour Hersh's article examines the mysterious circumstances surrounding what was bombed in Syria and why; it may not have been a nuclear facility but a show of deterrent force by the Israelis to Syria or potentially a warning shot to Iran. Hersh's full arguments are found in "A Strike in the Dark," *The New Yorker,* February 11, 2008. The IAEA has referred Syria to the UN Security Council following a three-year investigation that determined that the sight was very likely a nuclear reactor. See Peter Crail, "IAEA Sends Syria Nuclear Case to UN," *Arms Control Today(*July/August 2011), http://www.armscontrol.org/act/2011_%2007-08/%20IAEA_Sends_Syria_Nuclear_Case_to_UN (accessed August 3, 2011).

[285] David Fulghum, "Cyber-Combat's First Shot," *Aviation Week and Space Technology*, Vol 167, Issue 21(November 26, 2007): 28-31. According to Fulghum, "network raiders can conduct their invasion from an aircraft into a network and then jump from network to network until they are into the target's communication loop." It does not matter if the network is wired or wireless.

[286] The Suter system is an airborne network attack system developed by BAE systems and integrated into U.S unmanned aerial vehicle operations by L-3 Communications. The U.S. system has been tested operationally in Iraq and Afghanistan against insurgent communication networks. See David Fulghum and Douglas Barrie, "Off the Radar," *Aviation Week and Space Technology* Vol.167 Issue 14 (October 8, 2007): 28-29.

having the intended effect on the target sensors."[287] According to Fulghum and Barrie, "the technology allows users to invade communications networks, see what the enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions where approaching aircraft can't be seen."[288] Syrian air defense infrastructure is largely comprised of antiquated Russian surface to air missiles and radar[289] that are dependent on HF and VHF communications;[290] however Syria has procured the RussianTOR-M1(Sa-15 Gauntlet) short range mobile surface to air missile system. It is unclear whether the use of Suter, or Suter like clones used by the Israelis, could in fact temporarily blind newer generation Russian SAM's as it remains unknown what type of system was deployed at the Syrian radar site.[291] The ability to temporarily blind radar systems would be a rather unsettling prospect for Russian armaments customers such as Iran considering the oft discussed contemplation of American and Israeli pre-emptive strikes to dampen Iranian nuclear ambitions; Iran recently purchased 29 TOR launchers at a price tag of $750 million to guard its nuclear sites.[292] However, the ability to strike against a single site in Syria does not equate to the ability to conduct successful strikes against Iran's larger nuclear program located in underground-shielded facilities. As discussed in chapter 3, Stuxnet appears to have been an attempt to surmount the logistical difficulties, and political exigencies, of reaching such targets.

The Israeli raid on Syria may be a harbinger of how cyber attacks will be employed in future conflicts. Lewis predicts that cyber exploits will be the "opening salvo"

[287] Fulghum, "Cyber-Combat's First Shot."

[288] Fulghum and Barrie, "Off the Radar,"28-29. According to the authors "the process involves locating enemy emitters with great precision and then directing data streams into them that can include false targets and misleading messages that allow a number of activities including control."

[289] Fulghum and Barrie, "Off the Radar," The authors note that Syria operates the obsolescent S-200(SA-5 Gammon) long-range system and its associated 5N62Square Pair target engagement radar.

[290] Fulghum, "Cyber Combat's First Shot."

[291] Fulghum and Barrie, "Off the Radar," 29-29.

[292] Ibid.

and a "short-notice warning" of impending kinetic attacks.[293] However, this is not to be confused with first strike capability in which one's opponent is completely disarmed; cyber attacks are not nuclear weapons and do not threaten the prospect of societal annihilation. In tandem with electronic warfare and potential physical strikes on communications networks cyber attacks will attempt to degrade command and control, and erase or falsify opponent data, to create uncertainty and doubt among commanders. As such, Lewis concludes cyber attacks will work to densify the "fog of war" in any future conflict. [294]

Crisis Stability and Escalation

> The indefinite combination of human fallibility and nuclear weapons will lead to the destruction of nations[295]

The implications of cyber attacks against C4I[296] of nuclear states introduces potentially destabilizing dynamics to the calculus of nuclear deterrence and crisis stability[297] and yet such impacts remain virtually unexplored in public debates surrounding cyber "war". While it is beyond the scope and purpose of this discussion to review Cold War nuclear strategy, the analysis and forewarnings in regard to nuclear escalation and attacks on command and control are prescient when considering the use of cyber attacks. According to Sagan stable nuclear deterrence exists when both states develop "not just the ability to inflict some level of unacceptable damage to the other side, but also a sufficient degree of 'second strike survivability' so that its forces could

[293] Lewis, "Cyber Attacks, Real or Imagined, and Cyber War."

[294] Lewis, "Cyber Attacks, Real or Imagined, and Cyber War."

[295] Remarks made by Robert McNamara in *The Fog of War: Eleven Lessons From the Life of Robert S. McNamara,* directed by Errol Morris, (Sony Pictures Classics, 2003).

[296] C4SIR stands for Command, Control, Communications, Computers and Intelligence

[297] Crisis stability refers to the state where neither side has the incentive to attack first.

retaliate if attacked first" and "the nuclear arsenals must not be prone to accidental or unauthorized use."[298]

The development and inclusion of cyber attacks as an auxiliary aspect of military campaigns has emerged in an international security environment marked by a fundamental shift in the nuclear strategic balance from mutual assured destruction towards U.S. nuclear primacy vis a vis great power adversaries. Lieber and Press argue: "for the first time in decades, it could conceivably disarm the long-range arsenals of Russia and China with a nuclear first strike." [299] A return to mutual assured destruction between these protagonists would require monetary investment and "years of sustained effort" by China and Russia to offset both current disparities and future planned improvements to the U.S. nuclear arsenal.[300] To address the nuclear imbalance Russia and China will be pressured to "reduce the peacetime vulnerability of their forces by building larger nuclear arsenals, dispersing nuclear forces, possibly pre-delegating launch authority to local commanders and perhaps adopting hair-trigger nuclear retaliatory doctrines." [301] Indeed both the U.S. and Russia retain over 2,000 nuclear weapons on launch on warning alert entailing readiness to launch nuclear war within a half hour of tactical warning of strategic nuclear attack prior to first impact. Such postures are retained due to a "fixation" on the possibility of deliberate nuclear surprise attack that would disable vulnerable command and control systems.[302] Blair argues that launch on warning risks premature release of nuclear weapons on "false warning, miscalculation, or confusion." Hair-trigger alert postures are exacerbated by the

[298] Scott Sagan and Kenneth Waltz, *The Spread of Nuclear Weapons: A Debate* (New York: W.W. Norton & Company, 1995), 51.

[299] Keir A. Lieber and Daryl G. Press, "The End of Mad: The Nuclear Dimension of U.S. Primacy," *International Security* Vol. 30 No. 4 (Spring 2006): 7.

[300] Lieber and Press, "The End of Mad? The Nuclear Dimension of U.S. Primacy," 8. Lieber and Press note that much of this is due to concomitant the decline and reductions in the Russian arsenal coupled with modernization and increased lethality of U.S. strategic forces have shrunk but due to modernization have become more lethal. 12-13.

[301] Lieber and Press, "The End of Mad? The Nuclear Dimension of U.S. Primacy," 10.

[302] Bruce Blair, Harold Feiveson and Frank N. von Hippel, "Who's Got the Button? Taking Nuclear Weapons off Hair-Trigger Alert," *Scientific American*, November 1997.

prospect of inadvertent war launched by commanders in the field who have pre-delegated "nuclear release authority down the chain of command to cover contingencies in which the normal chain of command was severed."[303]

There are several ways in which adding cyber attacks to this dangerous dynamism may aggravate escalation risks during a crisis including crossing the nuclear Rubicon. As a supplemental function to kinetic attacks, cyber attacks may act as a force multiplier for disarming first nuclear strikes by potentially disabling an adversary's C4I. It is not known whether such attacks are technically feasible considering that hackers would need to have extensive knowledge of both information systems and military operational systems; the ability to know all system parameters beforehand is "hardly guaranteed."[304] However, fears of a nuclear decapitation strike[305] may be driven by the perception that this is possible based on and fuelled by speculation surrounding the possession of "secret cyber capabilities."

Koblentz aptly observes that in the absence of firm and reliable intelligence "governments may engage in worst-case planning and undertake an exaggerated reaction to perceived threats."[306] Intelligence acquisition surrounding cyber attack capabilities is seriously curtailed by the fact that such attacks may not be detected until executed. The inability to evaluate the scope and magnitude of threats may thus feed misperceptions and miscalculations regarding the intentions and capabilities of adversaries. These considerations are important as in a crisis scenario between nuclear-armed adversaries, fear may abound that such secret cyber capabilities provide a decisive advantage that could cripple C4I and imperil either party. As both sides fear the worst regarding the capabilities and intentions of their adversary either could launch a disarming first strike based on the premise that if they don't go first, "they won't go at

[303] Bruce Blair, *The Logic of Accidental Nuclear War* (Washington, DC: The Brookings Institution, 1993): 174.

[304] Libicki, *Cyberdeterrence and Cyberwar*, 47 and 55.

[305] A nuclear decapitation strike would aim to remove or disable the command control mechanisms or operation of the adversary.

[306] Koblentz, *Living Weapons: Biological Warfare and International Security,* 198.

all."[307] The prospect of miscalculation and error leading to inadvertent nuclear war in such scenarios is exacerbated by hair trigger launch on warning postures that provide very little time to discern whether an attack has actually started.

This is compounded by the fact that a target party may not be able to distinguish between cyber attack and cyber espionage as both exploit the same system vulnerabilities to gain access. These types of ambiguities are absent with "kinetic, nuclear, biological, and chemical weapons." The discovery of such intrusions makes it difficult to discern whether a cyber attack has started. The victim may have to decide within a very short timescale whether this is the "first move" in a devastating cyber attack or "reconnaissance of a system's capabilities."[308]

Blair argues that the prospect of cyber attacks against nuclear command and control makes de-alerting nuclear forces an urgent priority; "at the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision-making. The potential for perverse consequences with computer-launched weapons on hair-trigger is clear." [309]

According to Libicki, retaliation against cyber attacks may transcend into a violent conventional or nuclear realm if the attacker: "does not believe cyber retaliation is merited; "faces internal pressure to respond"; or believes that they will lose in a cyber "tit for tat" but will enjoy supremacy in other domains.[310] The attacker may also view the retaliation as a disproportionate response and may choose to respond by escalating to kinetic counter retaliation options. [311] This is complicated by the fact that the effects of

[307] I thank Dr.Doug Ross at Simon Fraser University for both suggesting and clarifying this point.

[308] Meyer, "Cyber Security Through Arms Control," 22.

[309] Bruce Blair, "Increasing Warning and Decision Time(De-Alerting)"(paper presented at the International Conference on Nuclear Disarmament, Oslo, Norway, February 26-27, 2008) http://disarmament.nrpa.no/wp-content/uploads/2008/02/Paper_Blair.pdf (accessed July 12, 2011).

[310] Libicki, *Cyberdeterrence and Cyberwar*, 69.

[311] Libicki, *Cyberdeterrence and Cyberwar,* 69.

cyber attacks may be difficult to predict and may spread beyond the bounds of the intended target system.

Attribution in the cyber realm remains a vexing problem as attackers may be patriot hackers, rogue elements of government that employ such individuals or organizations, political factions or criminal networks; the prospect of retaliation either in kind, or through conventional means, presents seemingly intractable obstacles. Investigations by Canadian researchers dubbed "Ghostnet" and "Shadows in the Cloud" revealed extensive cyber espionage against the Tibetan government, the United Nations and other foreign government ministries and embassies.[312] The data exfiltration was tied to Mainland China and known entities within the criminal underground; the PRC has a "vibrant" hacker community linked to the Chinese state through informal channels although the extent and parameters of this relationship are unknown.[313] According to Klimburg, China integrates and co-opts its "netizens" to maintain internal control and assure "internal pacification of "subversives" entailing "most of the large network exploitation attacks are highly opportunistic and not really connected to the Chinese leaderships overall intelligence-gathering priorities."[314] China is an attractive magnet to stage these types of cyber exploits as "bulletproof hosting" guarantees the operational continuity of servers "even if they are linked to spam or other illegal online activity."[315]

[312] Ron Deibert and Rafal Rohozinski, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," *Information Warfare Monitor*, University of Toronto, April 6, 2010, http://www.infowar-monitor.net/research (accessed November 14, 2010). The documents stolen include: India's security situation in several states; India's assessment of its activities in West Africa, Russia and the Commonwealth of independent states and the Middle East; the Pechora Missile System, Iron Dome Missile System and Project Shakti; as well as academic targets and journalists at India Strategic defense magazine.

[313] Deibert and Rohozinski, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," 38. According to the authors the degree of the reported relationship varies between "authorize" to "tacit consent" to "tolerate". Attribution is complicated by the multiple actors in the Chinese government that have factions and rivalries and maintain relationships with organized crime.

[314] Alexander Klimburg, "Mobilising Cyber Power," *Survival* Vol 53. No.1(Spring 2011): 48.

[315] Robert McMillan, "Google Attack Part of Widespread Spying Effort: U.S. Firms Face Ongoing Espionage from China," *ComputerWorld,* January 13, 2010, http://www.computerworld.com/s/article/9144221/Google_attack_part_of_widespread_spying_effort (accessed November 18, 2010).

According to Deibert and Rohozinski cyber exploits which appear to "benefit states may be the work of third-party actors operating under a variety of motivations."[316]

The tentacles of the state extend into and become part of informal criminal underground networks resulting in complex intertwined relationships that make attribution to any one party difficult. The melding of the criminal underground and the organs of the state is entrenched in Russia where nationalist hacker patriots, infamous criminal syndicates and Russian security services work in tandem. According to Klimburg cyber criminals play a substantial role in various attacks, including against Estonia in 2007 and Georgia in 2008; criminal syndicates provide logistical services and execute network exploitation.[317] This complicates both analysis of the threat, attribution and motivation for attacks and consideration of what retaliatory measures may be pursued.

As evidenced in the investigation of Stuxnet, unraveling the mysteries of the code took several months and did not reveal with any degree of certain the identity of the attackers. If hypothetically at some point in the future the Stuxnet attacks were attributed to a definitive source, more than a year after the attack was detected, retaliation may not be considered a retaliatory self-defence blow but an act of open aggression.[318]

Understanding the strategic implications of cyber attacks will entail the type of novel scholarly and policy debates that ensued in the wake of the Cold War. Expanding the perimeters of debate surrounding cyber threats, capabilities, and strategic implications beyond default application of Cold War analytical schematics could be a step in this direction. Some level of bilateral or multilateral discussions surrounding cyber

316 Ronald Deibert and Rafal Rohozinski, *Tracking GhostNet.* Information Warfare Monitor (The Munk Centre for International Studies, March 29, 2009), 12. http://www.infowar-monitor.net/research/ (accessed November 5, 2011).

317 Klimburg, "Mobilising Cyber Power," 49.

318 Libicki, Cyberdeterrence and Cyberwar, 52. Libicki's analysis predates Stuxnet but is applicable as carrying out a delayed return strike may be perceived as an act of aggression rather than a retaliatory blow.

doctrines should be pursued alongside articulated clarification of the many ambiguities and misperceptions that may abound with the development and use of “secret” weapons.

Conclusion

Military capabilities in cyberspace are being actively pursued and incorporated into military doctrines. Analytical and public discourse surrounding the development, acquisition and use of cyber weapons is stifled by secrecy surrounding such capabilities. What counts as a 'cyber incident,' or 'act of war' in cyberspace are fluid and pliable conceptual categories that are negotiated and framed within a politicized process. States pursue contrasting and mutually incompatible approaches to interpreting, managing and responding to cyber incidents. Such disparities in both interpretation of cyber attacks and responses to them are destabilizing forces in international security relations.

This discussion has examined the debate surrounding the disruptive and destructive potential of cyber attacks and recommends a measured and sober assessment of cyber attacks that is grounded in logistical feasibility. The discord in the analytical debate appears to provide an incoherent picture of the risks and threats surrounding cyber attacks that may complicate the development of appropriate policy frameworks and responses to such attacks. Indeed, the uncertainties surrounding cyber attacks may generate paranoid and panicked analysis of both threats and capabilities and this may be a corrosive factor for crisis stability.

A framework for comparing cyber attacks to biological and nuclear weapons highlights some of the similarities and differences between such weapons to provide an understanding of the novel challenges that cyber attacks pose for international security and strategic stability.

A military response to cyber threats shapes and limits both the interpretation of cyber incidents and the responses that may be marshalled to deal with them. The

establishment of U.S. Cyber Command indicates a shift in the way governments operate in cyberspace that has "ripple effects" among U.S. allies and adversaries.[319] The militarization of cyberspace and process of "securing" the global cyber commons creates new insecurities and dilemmas manifest in the development and deployment of offensive cyber capabilities and geo-political contestation in cyberspace. The U.S is pursuing contradictory and duplicitous goals in cyberspace. The drive to militarize cyberspace through the adoption and expansion of offensive cyber capabilities is concurrently pursued along side articulated commitment to preserve cyberspace as an open global commons. On the one hand, cyberspace is a new domain of warfare within which both defensive and offensive operations are prosecuted against adversaries to pursue strategic goals. Conversely, the U.S. wants to purse "robust international relationships", with allies and international partners, to reflect "core commitments and common interests in cyberspace" including collective cyber defense. The drive to develop offensive cyber capabilities is being emulated by allies and peer competitors as they rush to establish their own variants of cyber commands and postures. As most peer competitors and allies are unable to compete with the resources and organizational investments that the U.S. has poured into its burgeoning cyber industrial complex, the cyber war "playing field" is levelled by peer competitors by exploiting criminal networks and patriotic hackers.[320]

Canada's role in terms of a foreign policy approach to cyberspace is defined by a complete lack of approach. According to Deibert, Canada is absent in international arenas in which the governance of cyberspace is debated and defined. Canada may capitalize on its experience in multilateral diplomacy to work with governments to

[319] Ronald Deibert, "Rescuing the Global Cyber Commons: An Urgent Agenda for the G8 Meeting in Deauville, France," *Information Warfare Monitor*, May23, 2011, http://www.infowar-monitor.net/2011/05/rescuing-the-global-cyber-commons/ (accessed August 23, 2011).

[320] Ronald Deibert, "Rescuing the Global Cyber Commons: An Urgent Agenda for the G8 Meeting in Deauville, France."

preserve cyberspace as an open commons but has to date failed to take any such initiative.[321]

Considering that the targets and victims of cyber attacks will be private businesses and civilian entities, greater emphasis should be placed on government civilian contingency programs to mitigate the risks including reporting and assistance mechanisms for cyber attacks. As demonstrated in this discussion, there is no forced entry into cyberspace; such vulnerabilities are not the function of the prowess of the attacker but likely a result of bureaucratic inertia or inefficiencies, dearth or resources for security and lack of intra or inter agency co-ordination. The development of offensive capabilities does not confer protection. Such capabilities cannot deter attackers and do not resolve the underlying vulnerabilities that enable such attacks. The development of such capabilities creates suspicion and hostility in regard to intentions and capabilities among both allies and adversaries.

To date there has been a lack of public discourse surrounding the development of cyber attack capabilities and the militarization of cyberspace. The aim of this discussion is to add to the much needed but nascent debate surrounding the uses and strategic implications of cyber attack capabilities. Some level of bilateral or multilateral discussions surrounding cyber doctrines should be pursued to clarify the many ambiguities and misperceptions that may abound with the development and use of "secret" weapons.

[321] Deibert, "Cyber-Security: Canada is Failing the World."

Bibliography

Government Reports and Document

CRS Report for Congress. "*The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*." By Paul Kerr, John Rollins, and Catherine Theohary. Congressional Research Service, December 9th, 2010.

US Department of Defense. "*U.S Cyber Command Fact Sheet."* May 25, 2010. http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf (accessed December 28, 2010).

US Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. (July 2011): 1-19. http://www.defense.gov/news/d20110714cyber.pdf (accessed July 16, 2011).

United States Air Force. *Cyberspace Operations, Air Force Doctrine Document 3-12*(15 July 2010): 1-51. http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf (accessed September 15, 2010).

United States Army. *Cyberspace Operations Concept Capability Plan* 2016-2028 (22 February 2010): 1-63. http://www.fas.org/irp/doddir/army/pam525-7-8.pdf (accessed September 15, 2010).

United States Navy. *Naval Operations Concept 2010: Implementing the Maritime Strategy, US Navy Operations Concept* (2010): 1-96. http://www.navy.mil/maritime/noc/NOC2010.pdf (accessed September 15, 2010).

Senate Committee on Armed Services. "*Hearing to Consider the Nomination of Hon. Leon E Panetta to be Secretary of Defense*." (June 9, 2011): 1-59. http://armed-services.senate.gov/Transcripts/2011/06%20June/11-47%20-%206-9-11.pdf (July 14, 2011).

The White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, (May 2009): 1-38. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed June 10, 2011).

Secondary Sources

Albright, David, Paul Brennan and Christina Walrond."Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report." *International Institute for Science*

and International Security, 15 February, 2011. http://www.isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/ (accessed May 9, 2011).

———"Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment." *International Institute for Science and International Security,* December 22, 2010. http://www.isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed June 5, 2011).

Albright, David and Christina Walrond. "Iran's Gas Centrifuge Program: Taking Stock." *Institute for Science and International Security* (February 11, 2010). http://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock/8 (accessed June 5, 2011).

Albright, David and Jacqueline Shire. "A Witches' Brew? Evaluating Iran's Uranium Enrichment Progress." *Arms Control Today* 37 (November 2007) http://www.armscontrol.org/act/2007_11/Albright (accessed May 18, 2011).

Alexander, Gen. Keith B. "Building a New Command in Cyberspace." *Strategic Studies Quarterly* (Summer 2011): 3-12. http://www.au.af.mil/au/ssq/2011/summer/alexander.pdf (accessed June 7, 2011).

Bendrath, Ralf. "The American Cyber-Angst and the Real World-Any Link?" In *Bombs and Bandwidth*, edited by Robert Latham, 49-73. New York: The New Press, 2003.

Blair, Bruce, Harold Feiveson and Frank N. von Hippel. "Who's Got the Button? Taking Nuclear Weapons off Hair-Trigger Alert." *Scientific American*, November 1997.

Blair, Bruce. "Increasing Warning and Decision Time (De-Alerting)." Paper presented at the International Conference on Nuclear Disarmament, Oslo, Norway, February 26-27, 2008. http://disarmament.nrpa.no/wp-content/uploads/2008/02/Paper_Blair.pdf (accessed July 12, 2011).

———*The Logic of Accidental Nuclear War* (Washington, DC: The Brookings Institution, 1993.

Blechman, Barry, Daniel Brumber and Steven Heydemann. *Engagement, Coercion and Iran's Nuclear Challenge: A Report of a Joint Study Group on US-Iran Policy. Stimson Centre*, November 16, 2010, http://www.usip.org/files/resources/Engagement_Coercion_and_Irans_Nuclear_Challenge.pdf (accessed May 18, 2011).

Carr, Jeffrey. "Dragons, Tigers, Pearls, and Yellowcake: Four Stuxnet Targeting Scenarios." Taia Global Executive Cyber Protective Services, November 2010. http://nanojv.files.wordpress.com/2011/03/dragons_whitepaper_updated1.pdf (accessed May 2, 2011).

Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (December 2008): 1-87. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed January 17, 2011).

Clarke, Richard and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: Harper Collins, 2010.

Cornish, Paul et al. *On Cyber Warfare*. Chatham House Report, November 2010. http://www.chathamhouse.org/publications/papers/view/109508 (accessed March 25, 2011).

Chen, Thomas. "Stuxnet, The Real Start of Cyber Warfare?" *IEEE Network* Vol. 24 Issue 6 (November/December 2010): 2-3.

Cirincione, Joseph. "U.S. Strategy on Iran is Working." *Ploughshares Fund,* January 18, 2011. http://www.ploughshares.org/news-analysis/blog/us-strategy-iran-working (accessed May 5, 2011).

Chyba, Christopher. "Toward Biological Security." *Foreign Affairs* Vol.81 No.3 (May/June 2002): 122-126.

Crail, Peter. "IAEA Sends Syria Nuclear Case to UN." *Arms Control Today (*July/August 2011). http://www.armscontrol.org/act/2011_%2007-08/%20IAEA_Sends_Syria_Nuclear_Case_to_UN (accessed August 3, 2011).

Deibert, Ronald. "Tracking the Emerging Arms Race in Cyberspace." *Bulletin of the Atomic Scientists*, Vol. 67. No.1 (January/February 2011): 1-8.

Deibert Ronald and Rafal Rohozinski."Liberation Vs. Control." *Journal of Democracy* Vol. 21 No.4 (October 2010): 43-57.

———*Tracking GhostNet.* Information Warfare Monitor (The Munk Centre for International Studies, March 29, 2009) http://www.infowar-monitor.net/research/ (accessed November 5, 2010).

——— *Shadows in the Cloud: Investigating Cyber Espionage 2.0.* Information Warfare Monitor (University of Toronto, April 6, 2010) http://www.infowar-monitor.net/research/ (accessed November 14, 2010).

Devine, James and Julian Schofield. "Coercive Counter-Proliferation and Escalation: Assessing the Iran Military Option," *Defense and Security Analysis* Vol 22. No 2 (June 2006): 141-157.

Dunn, Myriam. "Securing the Digital Age: The Challenge of Complexity for Critical Infrastructure Protection and IR Theory." In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello, 85-105. New York: Routledge, 2007.

Dunn Cavelty, Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge: New York, 2008.

Eriksson,Johan and Giampiero Giacomello eds. *International Relations and Security in the Digital Age*. New York: Routledge, 2007.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. *W.32 Stuxnet Dossier*, Symantec Security Response, September 2010. Quoted in CRS Report for Congress, "*The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*," by Paul Kerr, John Rollins, and Catherine Theohary, Congressional Research Service, December 9th, 2010.

———*W32.Stuxnet Dossier Version 1.3.* Symantec Security Response Centre (November 2010) http://www.symantec.com/index.jsp (accessed May 2, 2011).

———*W.32 2011Stuxnet Dosser 1.4.* Symantec Security Response Centre (February 2011) http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed May 2, 2011).

Farwell, James P. and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* Vol. 53: no.1 (Spring 2011): 23-40.

Hastings Dunn, David. "Real Men Want to go to Tehran: Bush, Pre-Emption and the Iranian Nuclear Challenge." *International Affairs* 83:1(2007):19-38.

Hoffman, David."The New Virology: From Stuxnet to Bio-bombs, the Future of War by Other Means." *Foreign Policy* (March/April 2011): 77-80. http://www.foreignpolicy.com/articles/2011/02/22/the_new_virology?page=full (accessed April 9, 2011).

Hughes, Rex. "A Treaty For Cyberspace." *International Affairs* 86:2 (2010): 523-541.

International Institute of Strategic Studies. *The Military Balance 2011*, Vol. 111, Issue 1(2011): 4-496.

Klimburg, Alexander. "Mobilising Cyber Power," *Survival Vol.* 53: no.1 (Spring 2011): 41-60.

Koblentz, Gregory. *Living Weapons: Biological Warfare and International Security.* Ithaca, NY: Cornell University Press, 2009.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D.Kramer, Stuart H.Starr, and Larry K. Wentz, 24-43.Washington, D.C.: National Defense University Press, 2009.

Kurtz, Ronald. *Securing SCADA Systems.* Indianapolis: Indiana: Wiley Publishing Inc, 2006. http://www.scribd.com/doc/60046847/3/SCADA- (accessed August 15, 2011).

Latham, Robert. “Introduction.” In *Bombs and Bandwidth,* edited by Robert Latham, 1-21. New York: The New Press, 2003.

Lewis, James. “Cyber Attacks, Real or Imagined, and Cyber War.” *Center for Strategic and International Studies* (July 11, 2010). http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war (accessed June 25, 2011).

———“Cross-Domain Deterrence and Credible Threats.” *Center for Strategic and International Studies* (July 2010). http://csis.org/publication/cross-domain-deterrence-and-credible-threats (accessed July 5, 2011).

———“Multilateral Agreements to Constrain Cyberconflict.” *Arms Control Today* (June 2010). http://www.armscontrol.org/act/2010_06/Lewis (accessed July 5, 2011).

———“The Cyber War has Not Begun.” *Center for Strategic and International Studies* (March 2010). http://csis.org/publication/cyber-war-has-not-begun (accessed June 25, 2011).

———“The Korean Cyber Attacks and their Implications for Cyber Conflict.” *Center for Strategic and International Studies* (October 2009) http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict (accessed July 5, 2011).

———“Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.” *Center for Strategic and International Studies* (December 2002): 1-12. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (accessed July 12, 2011).

Langner, Ralph. “Stuxnet: Dissecting a Cyberwarfare Weapon.” *Security & Privacy, IEEE,* Vol. 9 Issue 3 (May/June 2011): 49-51.

Libicki, Martin. “Cyberwar as a Confidence Game,” *Strategic Studies Quarterly* (Spring 2011): 132-146.

———*Cyberdeterrence and Cyberwar*. Santa Monica: RAND, 2009.

Lieber, Keir A. and Daryl G. Press. “The End of Mad: The Nuclear Dimension of U.S. Primacy.” *International Security* Vol. 30 No. 4 (Spring 2006): 7-43.

Lynn III, William J. “Defending a New Domain.” *Foreign Affairs* (Sep/Oct2010) http://web.ebscohost.com.proxy.lib.sfu.ca/ehost/detail?vid=3&hid=18&sid=c1d46fd6-6440-42ae-9a55-b5c9ed99568b%40sessionmgr4&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=aph&AN=52957873 (accessed August 23, 2011).

Miller, Robert, Daniel Kuehl and Irving Lachow. “Cyber War: Issues in Attack and Defense.” *Joint Forces Quarterly*, Issue 61, Second Quarter (2011): 18-23.

Meyer, Paul. “Cyber Security Through Arms Control.” *The RUSI Journal,* 156:2, 22-27.

Morgan, Patrick. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, edited by National Research Council, 55-77. Washington, D.C.: The National Academies Press, 2010.

National Research Council. *Technology, Policy, Law and Ethics Regarding the U.S. Acquisition and Use of Cyber Attack Capabilities*. Washington, D.C.: The National Academies Press, 2009.

OECD. *Reducing Systemic Cybersecurity Risk*. Prepared by Peter Sommer and Ian Brown (14 January, 2011):1-109. http://www.oecd.org/dataoecd/3/42/46894657.pdf (accessed March 12, 2011).

Patel, Sandip, Ganesh Bhatt, and James Graham. “Improving the Cyber Security of SCADA Communication Networks.” *Communications of the ACM* Vol. 52 No.7 (July 2009): 139-142.

Perkovich, George. “Sanctions on Iran-The Least Bad Option.” *Carnegie Endowment for International Peace* (June 28, 2010). http://carnegieendowment.org/2010/06/28/sanctions-on-iran-least-bad-option/4ug (accessed May 2, 2011).

Sagan, Scott and Kenneth Waltz. *The Spread of Nuclear Weapons: A Debate*. New York: W.W. Norton & Company, 1995.

Samaan, Jean-Loup. “Beyond the Rift in Cyber Strategy,” *Strategic Insights* Vol. 10, Issue 1 (Spring 2011): 4-15.

———“Cyber Command: The Rift in US Military Cyber-Strategy.” *The RUSI Journal* Vol. 155 No.6 (December 2010): 16-21.

Spector, Leonard S. “Direct Action: The New Attacks on Iran’s Nuclear Program.” WMD Junction, *James Martin Center for Nonproliferation Studies* (March 26, 2011) http://cns.miis.edu/wmdjunction/110121_iran_direct_action.htm (accessed May 7, 2011).

Swaine, Michael D. “Beijing’s Tightrope Walk on Iran.” Carnegie Endowment for International Peace, *China Leadership Monitor*, No.33, June 28, 2010. http://www.carnegieendowment.org/2010/06/28/beijing-s-tightrope-walk-on-iran/5on Col. (accessed June 3, 2011).

Williamson III, Charles W. “Carpet Bombing in Cyberspace: Why America Needs a Military Botnet.” *Armed Forces Journal (*May 2008). http://www.armedforcesjournal.com/2008/05/3375884 (accessed May 3, 2011).

Zukowski, Simon. “The Nuclear Nonproliferation Regime: Its Status and Prospects.” Un published Master’s Thesis, Simon Fraser University, 2010.

Media, News Magazines and Other Web Sources

Abrams, Randy. “Why Steal Digital Certificates,” *The ESET Threat Blog*. Posted July 22, 2010, http://blog.eset.com/2010/07/22/why-steal-digital-certificatesnotes (accessed August 23, 2011).

Barnes, Julian and Siobhan Gorman. “Cyberwar Plan has New Focus on Deterrence.” *The Wall Street Journal*, July 15, 2011. http://online.wsj.com/article/SB10001424052702304521304576446191468181966.html (accessed August 7, 2011).

Berinato, Scott. “Debunking the Threat to Water Utilities.” http://www.cio.com/article/30935/Debunking_the_Threat_to_Water_Utilities (accessed June 3, 2011).

Bradsher, Keith. “China to Tighten Limits on Rare Earth Exports.” *New York Times*. December 28, 2010, http://www.nytimes.com/2010/12/29/business/global/29rare.html (accessed May 4, 2011).

Bright, Arthur. “Clues Emerge about the Genesis of Stuxnet Worm.” *Christian Science Monitor*, October 1, 2010. http://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm (accessed November 14, 2010).

Broad, William, John Markoff, David Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay.” *New York Times*, January 15, 2011. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all (accessed January 15, 2011).

Broad, William John Markoff, and David Sanger. “Worm was Perfect for Sabotaging Centrifuges.” *New York Times*, November 18, 2010. http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html (accessed December 28, 2010).

Carr, Jeffrey. “Stuxnet’s Finnish-Chinese Connection.” *The Firewall Blog, Forbes*, entry posted December 14, 2010. http://blogs.forbes.com/firewall/2010/12/14/ (accessed December 28, 2010).

———“Did the Stuxnet Worm Kill India’s INSAT-4B Satellite?” *The Firewall, Forbes*. Entry posted September 29, 2010. http://blogs.forbes.com/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/ (accessed, May 4, 2011).

Chien,Eric. “Stuxnet: A Breakthrough.” *Symantec Official Blog*. Entry posted 16 November, 2010, http://www.symantec.com/connect/blogs/stuxnet-breakthrough (accessed May 2, 2011).

Cirincione, Joseph. “Five Myths about Iran’s Nuclear Program.” *Washington Post*, October 18, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/10/15/AR2009101503476.html (accessed May 14, 2011).

Clayton, Mark. “Stuxnet spyware targets industrial facilities, via USB memory stick. “*The Christian Science Monitor*, July 23, 2010. http://www.csmonitor.com/USA/2010/0723/Stuxnet-spyware-targets-industrial-facilities-via-USB-memory-stick (accessed September 9, 2010).

———“Stuxnet Malware is Weapon out to Destroy…Iran’s Bushehr Nuclear Plant?” *The Christian Science Monitor,* September 21, 2010. http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant (accessed November 8, 2010).

Deibert, Ronald. “Cyber Security: Canada is Failing the World.” *Huffington Post Canada,* May 26, 2011. http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html (accessed August 23, 2011).

———“Rescuing the Global Cyber Commons: An Urgent Agenda for the G8 Meeting in Deauville, France.” *Information Warfare Monitor*, May23, 2011. http://www.infowar-monitor.net/2011/05/rescuing-the-global-cyber-commons/ (accessed August 23, 2011).

Dunn Cavelty, Myriam. “As Likely as a Visit from E.T.” *The European*, January 7, 2011. http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear (accessed March 4, 2011).

Dyer, Gwynne. “There’s No Way for the U.S. to Win a Non-Nuclear War with Iran.” *The Georgia Straight*, August 3, 2010. http://www.straight.com/article-336907/vancouver/gwynne-dyer-theres-no-way-us-win-nonnuclear-war-iran (accessed August 5, 2010).

Editorial, “The Iranian Slowdown.” *Washington Post,* January 13, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/12/AR2011011205566.html (accessed May 9, 2011).

Erdbrink,Thomas and Ellen Nakashima, “Iran Struggling to Contain Foreign-made Stuxnet Computer Virus.” *Washington Post,* September 27, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706229.html (accessed November 5, 2010).

Erlanger, Steven. “Little Progress is Seen in Iran Talks.” *New York Times,* January 21, 2011. http://www.nytimes.com/2011/01/22/world/middleeast/22nuke.html (accessed May 5, 2011).

Falkenrath, Richard. “From Bullets to Megabytes.” *New York Times*, January 26, 2011. http://www.nytimes.com/2011/01/27/opinion/27falkenrath.html (accessed July 8, 2011).

Fildes, Jonathan. “Stuxnet worm targeted high-value Iranian assets.” BBC News, 23 September, 2010. http://www.bbc.co.uk/news/technology-11388018 (accessed November 5, 2010).

Fulghum, David, Robert Wall and Douglas Barrie. “All Arms Attack,” *Aviation Week and Space Technology*, Vol. 167 Issue 18 (November 5, 2007): 32-33.

Fulghum, David and Douglas Barrie. “Off the Radar.” *Aviation Week and Space Technology* Vol.167 Issue 14 (October 8, 2007): 28-29.

Fulghum, David. “Cyber Attack Turns Physical.” *Aviation Week and Space Technology*, September 28th, 2010. http://www.aviationweek.com/aw/generic/ (accessed May 15, 2011).

———“What is a Weapon?” *Aviation Week and Space Technology*, Vol. 171 No.12, September 28, 2009: 60-61.

———“Cyber-Combat’s First Shot.” *Aviation Week and Space Technology*, Vol.167, Issue 21(November 26, 2007): 28-31.

Gady, Franz Stefan. “Lost in Translation: Doctrines and Diplomatic Efforts in Cyberspace,” *Huffington Post*, May 11, 2011. http://www.huffingtonpost.com/franzstefan-gady/lost-in-translation-doctr_b_864760.html (accessed June 4, 2011).

Goldberg, Jeffrey. “The Point of No Return.” *The Atlantic,* September 2010. http://www.theatlantic.com/magazine/archive/2010/09/the-point-of-no-return/8186/ (accessed May 5 2011).

Hafezi, Parisa.“Iran Admits Cyber Attack on Nuclear Plants.” *Reuters,* November 29, 2010. http://www.reuters.com/article/2010/11/29/us-iran-idUSTRE6AS4MU20101129 (accessed April 18, 2011).

Hersh, Seymour. “The Online Threat: Should We Be Worried About a Cyber War?” *The New Yorker*, November 1, 2010. http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh (accessed November 5, 2010).

———“A Strike in the Dark.” *The New Yorker,* February 11, 2008.

———“The Iran Plans: Would President Bush Go to War to Stop Tehran from Getting the Bomb?” The New Yorker, April 17, 2006. http://www.newyorker.com/archive/2006/04/17/060417fa_fact (accessed June 4, 2011).

Hertzberg, Hendrik “Iran and the Bomb.” *The New Yorker*, December 13, 2010. http://www.newyorker.com/talk/comment/2010/12/13/101213taco_talk_hertzberg (accessed May 3, 2011).

Jackson, Patrick. “Meet USCybercom,” BBC News, 15 March 2010. http://news.bbc.co.uk/2/hi/8511711.stm (accessed September 14, 2010).

Keizer, Gregg. “Why did Stuxnet Worm Spread.” *Computer World*.” October 1, 2010. http://www.computerworld.com/s/article/9189140/Why_did_Stuxnet_worm_spread_ (accessed, November 18, 2010).

Langner, Ralph. “How to Hijack a Controller.” *Control Global,* January 13, 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html (accessed April 17, 2011).

——— “The Big Picture.” Langner Blog. Entry posted 19 November, 2010. http://www.langner.com/en/2010/11/19/the-big-picture/ (accessed April 17, 2011).

———“Better than Bunker Busters: The Virtual Chinese Water Torture.” *Langner Blog. Entry posted* 15 November 2010. http://www.langner.com/en/2010/11/15/better-than-bunker-busters-the-virtual-chinese-water-torture/ (accessed May 4, 2011).

Laxman, Srinivas. “Cyber Threat: ISRO Rules out Stuxnet Attack on Insat-4 B.” *The Economic Times*, 12 October, 2010. http://articles.economictimes.indiatimes.com/2010-10-12/news/28435956_1_insat-internet-worm-stuxnet-worm (accessed May 4, 2011).

Lewis, Jeffrey. “On Spinning Libyan Centrifuges.” *Arms Control Wonk Blog*. Entry posted 15 February, 2011. http://lewis.armscontrolwonk.com/archive/3551/on-spinning-libyan-centrifuges (accessed May 14, 2011).

Libicki, Martin. “Cyber-Security and Cyber-Deterrence.” Presentation, John Hopkins University, February 16, 2011. https://outerdnn.outer.jhuapl.edu/videos/021611/Libicki.pdf (accessed July 12, 2011).

“Libyan Nuclear Weapons,” GlobalSecurity.Org, http://www.globalsecurity.org/wmd/world/libya/nuclear.htm (accessed May 25, 2011).

Matrosov, Aleksandr. “Stuxnet Under the Microscope: Revision 1.31, “ *ESET*, http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf (accessed May 23, 2011).

Markoff, John. “A Silent Attack but Not a Subtle One.” *New York Times*, September 26th, 2010. http://www.nytimes.com/2010/09/27/technology/27virus.html (accessed November 19, 2010).

Markoff, John and Thom Shanker. “Halted 03 Iraq Plan Illustrates U.S. Fear of Cyber War Risk.” *New York Times*, August 1, 2009. http://www.nytimes.com/2009/08/02/us/politics/02cyber.html (accessed April 18, 2011).

McMillan, Robert. “Google Attack Part of Widespread Spying Effort: U.S. Firms Face Ongoing Espionage from China.” *Computer World,* January 13, 2010. http://www.computerworld.com/s/article/9144221/Google_attack_part_of_widespread_spying_effort (accessed November 18, 2010).

McConnell, Mike. “Mike McConnell on How to Win the Cyber-War We’re Losing.” The Washington Post, February 28, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (accessed May 16, 2010).

Nakashima, Ellen. “List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare.” *Washington Post,* May 31, 2011.

O Murchu, Liam. “Last Minute Paper: An In-depth Look into Stuxnet.” http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml (accessed June 12, 2011).

Sanger, David E. “U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site.” *New York Times*, January 10, 2009. http://www.nytimes.com/2009/01/11/washington/11iran.html (accessed March 22, 2011).

Sanger, David. “Iran Fights Malware Attacking Computers.” *New York Times,* 25 September, 2010. http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html (accessed May 8, 2011).

Schneier, Bruce. “Stuxnet.” *Schneier on Security Blog*. Entry posted October 7, 2010. http://www.schneier.com/blog/archives/2010/10/stuxnet.html (accessed November 14, 2010).

“Siemens and Areva: Nuclear Fission-Franco-German Industrial Relations Take Sharp Turn for the Worse.” *The Economist,* January 29, 2009. http://www.economist.com/node/13022201 (accessed May 14, 2011).

The Fog of War: Eleven Lessons From the Life of Robert S. McNamara. Directed by Errol Morris. Sony Pictures Classics, 2003.

Warrick,Joby. “Iran’s Natanz Nuclear Facility Recovered quickly from Stuxnet Cyberattack.” *Washington Post,* February 16, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html (accessed May 9, 2011).

Wolf, Jim. “The Pentagon’s New Cyber Warriors.” *Reuters*, October 5th, 2010. http://www.reuters.com/article/2010/10/05/us-usa-cyberwar-idUSTRE69433120101005 (accessed January 12, 2011).

Zetter, Kim. “Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant.” *Wired: Threat Level Weblog*, entry posted February 11, 2011. http://www.wired.com/threatlevel/2011/02/stuxnet-five-main-target/ (accessed March 5, 2011).

——— “Blockbuster Worm Aimed for Infrastructure, But no Proof Iran Nukes Were Target,” *Wired Threat Level Weblog,* entry posted September 23, 2010. http://www.wired.com/threatlevel/2010/09/stuxnet/ (accessed November 8, 2010).