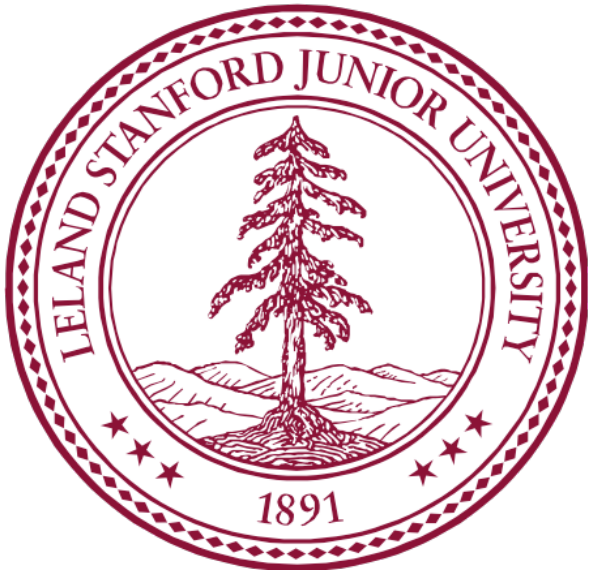
An Evaluation of the Analogy Between Nuclear and Cyber Deterrence

Patrick Cirenza



Advisors: Professor Coit D. Blacker and Phillip Taubman
Center for International Security and Cooperation
Freeman Spogli Institute for International Studies
Stanford University
June 2015

Abstract

The nuclear-cyber deterrence analogy is a popular and controversial comparison to make in American military, policymaking, and academic circles. Leaders in the field, many of who grew up during the Cold War, often draw the parallel to make sense of the impacts of strategic cyber weapons. Analogizing strategic cyber weapons to nuclear weapons has a powerful surface allure; these weapons have intercontinental range, near instantaneous delivery, and a growing potential for destructiveness. In particular, applying nuclear deterrence frameworks to cyberspace is appealing because it promises a way to mitigate a serious emerging threat. However, the analogy is flawed. Nuclear weapons represent a revolution in military affairs that developed into a strategic deterrent because of its unique characteristics. These characteristics include the sheer destructiveness of a single nuclear weapon, the assuredness of that destruction, and the debate over how to use nuclear weapons. Strategic cyber weapons have neither matured as a revolution in military affairs nor developed the characteristics and debate over their use to the same extent as nuclear weapons. Therefore, at this point, it is not possible to make the nuclear-cyber deterrence analogy and basing policy on the assumption that the analogy is correct is erroneous and potentially even dangerous. In the future, as the world becomes more cyber-dependent and the technology of strategic cyber weapons develops, it may be possible that the analogy will become more credible, at which point it will be necessary to re-evaluate it.

Acknowledgements

I am very grateful to have had Professors Chip Blacker and Phillip Taubman as my advisers for this project. As I write these acknowledgements (having just revised my thesis for the final time), I cannot emphasize enough how much you have helped. You have guided, poked, and prodded me in a direction that has made this thesis into something that I am proud to submit. Professor Blacker, I promise that I was listening during our sessions and it was not just all blah, blah, blah Fido. Thank you for your insightful questions, relevant research suggestions, and always keeping an eye out for me in the broader scheme of things. Phil, thank you for pushing me to lighten up my writing and include anecdotes. Thank you also for encouraging me to do interviews and teaching me how to conduct them. They started out small and snowballed into a thoroughly enjoyable and educational enterprise.

I am also indebted to Dr. Herb Lin who was willing to step in as my unofficial adviser on the cyber side. Thank you for letting me Skype you and come into your office with bold visions of cyberspace, get everything wrong, and then have you gently turn me towards the correct answer. On that note, I would also like to thank Dr. Michael Sulmeyer, John Iannerelli, and Russell Wald for the informal conversations we had that helped me think through the issues. Thank you James Honsa for effectively providing the template for my Stanford career, which ended up with me writing a thesis in the same program as you with the same advisers. Thank you also Kate Kuhns for the translation assistance.

I also owe a thank you to the people I interviewed. It is truly a testament to your generosity that all of you were willing to take thirty minutes to an hour to speak with an undergraduate student after a cold-call email. It was an unexpected and exciting honor to hear perspectives from the White House, the civilian and uniform sides of the military, businesses, multiple government agencies, the media, think tanks, universities, and committees in the Senate and the House on this issue.[1]

Finally, I am thankful to my parents who supported me in this project. It is a common cliché to thank ones parents in the acknowledgements, but you have done so much more than just bring me into the world. I would not be where I am today without your steadfast guidance and unfailing care. Thank you for everything that you have sacrificed for my success. I very much hope to be able to parent my children one day as you parented me.

[1] For a full list of interviews, please refer to the Appendix

Table of Contents

Preface: Story of this Thesis

"Being on the forefront of discovery and taking part in the creation of new knowledge is an immensely rewarding and life altering experience."

-John Hennessey, President of Stanford University, at Stanford's 121st Opening Convocation Ceremony[2]

President John Hennessey planted the seeds of this project at the opening convocation ceremony in 2011 when he called upon the Stanford University Class of 2015 to engage in the creation of new knowledge. Although I would not know it at the time, those words would ring in my ears when I was deciding whether to write a thesis. The topic I have chosen to study has greatly evolved over the past year of the thesis process. Late in the spring of my junior year, after having spent three years in the beating heart of Silicon Valley, I knew the importance of leaving university with some degree of cyber literacy. I saw (and still see) my thesis as an opportunity to delve deeply into subjects about which I knew little. Fortunately, I had guidance from several wise mentors who steered me away from a perilously overreaching subject. Broadly interested in the transnational nature of cyberspace and the low barriers to entry, I initially wanted to write this thesis on the growing role of non-state actors in cyberspace. When I approached Professor Scott Sagan with this idea, he rightly questioned my base level of knowledge and urged me to relate the subject to concepts that I understood better.

Stumped, I mentioned this conflict between interest and lack of knowledge to Professor Condoleezza Rice during her office hours. She suggested that I examine the comparison between nuclear weapons and cyber weapons. From there I was drawn, as many who are new to the field are, to the tempting concept of applying nuclear-style deterrence in cyberspace. Although the

[2] "Stanford University 121st Opening Convocation Ceremony." YouTube. October 10, 2011. Accessed April 29, 2015.

project expanded and contracted several times, evaluating the analogy in terms of deterrence remained a constant.

I began this project believing that the nuclear template of strategic deterrence fit neatly onto the emerging world of strategic cyber weapons. As I dived further into the topic, it became increasingly apparent that the analogy only made sense at the surface level. Deeper investigation proved that the nuclear-cyber deterrence analogy is not applicable at the present. During my interviews, I asked every person what they thought of the analogy. I noticed that most of the high-level policymakers and the people who were most removed from the subject thought it made a lot of sense. The people who were closest to the subject thought the opposite and told me it was a badge of credibility to do so. This divergence is concerning and I hope that as the world comes to terms with this new technology this gap will close.

From a personal perspective, this thesis has been a success. Through my research and my conversations on and off of the record, I have become conversant in both the nuclear and cyber fields and can hold my own with various leading luminaries. I have also become a much better writer, interviewer, and thinker as a result of this process. The two principal contributions of this thesis are a deep look at a topic with current policy relevance that has been relatively untouched and the collection a wide array of perspectives on an emerging field of study through a series of interviews. Whether these contributions will be of any significance remains to be seen, but I believe that the findings of the thesis are worthy of note. I hope you enjoy the reading.

-Patrick Cirenza, 5/22/15

Introduction: The Analogy

> "I often will hear people use the nuclear analogy in terms of how we were able to develop the concepts of deterrence, norms and behavior. I try to remind people to remember that the challenge of the nuclear analogy is… that [nuclear weapons] were controlled by a very small number of nation-states -- two really."
>
> -Admiral Michael Rogers, Director of the National Security Agency and Commander of U.S. Cyber Command, before the House Select Intelligence Committee, November 20th 2014[3]

A Power Outage

At 4:10 PM on August 14, 2003, the U.S. experienced the largest electrical power outage in its history. Over 50 million people in the northeast of North America were suddenly without electricity.[4] The sudden power failure trapped thousands in trains and elevators, caused city gridlock as traffic lights flickered off, and left people unable to buy essential supplies as automatic teller machines and cashiers ceased to function.[5] Water stopped flowing in Cleveland to the neighborhoods in the hills because the pumps had no power, raising health and safety concerns.[6] Fearing a terrorist attack only two years after 9/11 and potential widespread looting as there had been in the wake of the 1977 blackout, Governor George Pataki of New York ordered the National Guard to help local authorities.[7] In New York City, well-armed police officers

[3] Rogers, Michael. "Cybersecurity Threats: The Way Forward." House of Representatives Select Committee on Intelligence. November 20, 2014. Accessed May 21, 2015. https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf.
[4] Walsh, Bryan. "10 Years After the Great Blackout, the Grid Is Stronger - but Vulnerable to Extreme Weather." Time Magazine. Accessed April 29, 2015.
[5] Barron, James. "THE BLACKOUT OF 2003: The Overview; POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN 8 STATES AND CANADA; MIDDAY SHUTDOWNS DISRUPT MILLIONS." The New York Times. August 14, 2003. Accessed April 29, 2015.
[6] Wald, Matthew. "The Blackout That Exposed the Flaws in the Grid." The New York Times. November 10, 2013. Accessed April 29, 2015.
[7] Barron, James. "THE BLACKOUT OF 2003: The Overview; POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN 8 STATES AND CANADA; MIDDAY SHUTDOWNS DISRUPT MILLIONS."

deployed to potentially vulnerable targets for terrorism.[8] After just two days, the blackout led to eleven deaths and an estimated $6 billion in costs.[9]

What caused this enormous calamity? As it turns out, it was a combination of human intervention in software, a hot day, and a tree branch. A computer technician of a power company in Ohio switched off the alarm system to perform a software update and went out to lunch without turning it on again.[10] Because it was a hot day, people across the northeast were using air conditioners more than normal, which demanded more energy.[11] This in turn caused the metal in the transmission lines south of Cleveland to sag, brush against unpruned tree branches, and cease functioning.[12] Other power lines increased their power to compensate, but it proved to be too much of a burden on the system.[13] Without proper oversight, it led to a cascade of short-circuiting across the northeast that led to massive power outages.[14]

Introduction

The Northeast Blackout of 2003 occurred because a human caused a computer to fail. It was a self-inflicted cyber accident of limited scope, but it could have just as easily been an intentional act and far more destructive. Strategic cyber weapons, when wielded by a large state such as the U.S., Russia, or China, are potentially capable making computers fail in automobiles, planes, trains, financial systems, municipal sewage systems, and a whole host of other critical

---

[8] Barron, James.
[9] Minkel, JR. "The 2003 Northeast Blackout--Five Years Later." Scientific American. August 13, 2008. Accessed April 29, 2015.
[10] Wald, Matthew. "The Blackout That Exposed the Flaws in the Grid."
[11] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations." U.S.-Canada Power System Outage Task Force. April 1, 2004. Accessed April 29, 2015. 25.
Minkel, JR. "The 2003 Northeast Blackout--Five Years Later." Scientific American. August 13, 2008. Accessed April 29, 2015.
[12] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations." U.S.-Canada Power System Outage Task Force.
Minkel, JR. "The 2003 Northeast Blackout--Five Years Later."
[13] Minkel, JR.
[14] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations."

infrastructure for extended periods of time.[15] Further, it is possible for these states to conduct these attacks with intercontinental range and negligible delivery times without ever having to deploy a single soldier on the adversary's territory. If the attackers have enough time, it is nearly impossible to mount an effective defense against them.

To political and military leaders in the U.S. and elsewhere, the threat posed by strategic cyber weapons seems to be comparable to that of nuclear weapons. Secretary of State John Kerry referred to cyber weapons as "the 21st century nuclear weapons equivalent" during his confirmation hearings and former Chairman of the Joint Chiefs of Staff Admiral Mike Mullen stated that cyber weapons are the "single biggest existential threat that's out there."[16] This

[15] A strategic cyber weapon is malware capable launching an irreversible computer network attack against cyber-dependent economic, military, and political systems and infrastructure that causes a debilitating level of casualties and damage to a state.
For the sake of clarity and consistency, this thesis largely uses definitions of key terms from the Department of Defense.
Deterrence is "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."
Cyber Capability: Any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities. Cyber capabilities do not include a device or software that is solely intended to provide access to an adversarial computer system for data exploitation.
Weapon: Weapons are devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or materiel. Weapons do not include devices developed and used for training, or launch platforms to include aircraft and intercontinental ballistic missiles.
Cyber attack is "a hostile act using computer or related networks or systems, intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."
Cyber warfare is "an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict."
Critical infrastructure are "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health safety, environment, or any combination of these matters, across any Federal, State, regional, territorial or local jurisdiction."
"Deterrence." Department of Defense Dictionary of Military Terms. Accessed April 29, 2015. http://www.dtic.mil/doctrine/dod_dictionary/data/d/3763.html.
"Legal Reviews of Weapons and Cyber Capabilities." Department of the Air Force. May 13, 1994. Accessed March 16, 2015. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-053.pdf.
Cartwright, James. "Cyber Operations Lexicon." Department of Defense. Accessed April 29, 2015. http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[16] Full Quotation from Admiral Mike Mullen: " The single biggest existential threat that's out there, I think, is cyber. I think we're going to have to focus a lot more on it. We're going to have to put more resources against it. We're going to have to train people better. Because cyber actually, more than theoretically, can attack our infrastructure, our financial systems, etc. It's a space that has no boundaries. It has no rules, and there are people who are very good at it. There are countries who are very good at it."

sentiment is not limited to the U.S. leadership. Fang Fenghui, Chairman of the Chinese People's Liberation Army General Staff, claimed, "If Internet security cannot be controlled, it's not an exaggeration to say that the effects could be no less than a nuclear bomb."[17] Dmitriy Rogozin, the Russian deputy prime minister in charge of the defense industry, believes that cyber weapons offer states "first strike" capability to "destroy critical infrastructure of the state… [and] system[s] of political and military control."[18]

For many of these leaders, raised during the final decades of the Cold War, the nuclear-cyber analogy has a strong surface appeal; both weapons systems are capable of inflicting terrible damage in a short amount of time on the homeland and little can be done to prevent their use or defend against them. One of the logical links that policymakers make from this analogy is that if the weapons are similar, then the outcomes must be as well. Of particular interest to U.S. policymakers is whether nuclear deterrence-style thinking can be applied in cyberspace. It is therefore of critical importance to know how applicable the analogy is, especially in respect to the concept of strategic deterrence. If the analogy does apply, then using the framework of deterrence developed for nuclear weapons could be a powerful tool for limiting cyber conflict between large states. If it does not, then basing policy off of incorrect assumptions could lead to potentially dangerous results.

"Senate Foreign Relations Committee Holds Confirmation Hearing on the Nomination of Massachusetts Democratic Sen. John Kerry to Be Secretary of State." Congressional Quarterly. January 24, 2013. Accessed March 8, 2015. http://www.cq.com/doc/congressionaltranscripts-4209477?0&print=true.
Muradian, Vago. "Adm. Michael Mullen." Defense News. July 10, 2011. Accessed March 8, 2015. http://archive.defensenews.com/article/20110710/DEFFEAT03/107100301/Adm-Michael-Mullen.

[17] Forsythe, Michael. "Chinese General With Dempsey Compares Cyber-Attack to Nuke." Bloomberg.com. April 22, 2013. Accessed March 16, 2015.

[18] Translation assistance from Kate Kuhns, Executive Director of Stanford Global Studies
Васенин, Виктор, and Сергей Куксин. "Стенограмма выступления Дмитрия Рогозина на пресс-конференции в "РГ"" Российская газета. June 28, 2013. Accessed March 16, 2015. http://www.rg.ru/2013/06/28/doklad.html. https://translate.google.com/translate?hl=en&sl=ru&tl=en&u=http%3A%2F%2Fwww.rg.ru%2F2013%2F06%2F28%2Fdoklad.html

This thesis argues that the analogy between nuclear and cyber deterrence is not applicable. However it is possible that it might be in the future. To arrive at these conclusions, this thesis limits its analysis to the analogy between strategic cyber weapons and nuclear weapons, as any form of cyber threat below that level is not worth the comparison.[19] The principal framework for evaluating the nuclear-cyber deterrence analogy in this thesis is the revolution in military affairs (RMA).[20] The introduction provides a definition and a set of

[19] This is primarily because the potential destructiveness of a strategic cyber weapon makes it the only malware that is even possibly comparable to a nuclear weapon. Additionally, for now, only a few states are capable of carrying out a strategic cyber attack, meaning that attribution, and consequently deterrence by punishment, is potentially feasible. As Professor Siegfried Hecker, former Director of Los Alamos National Laboratories, said, "the physics of a two or three player problem are very different from that of a n-player problem." Much of the literature that investigates applying nuclear-style deterrence in cyberspace evaluates the analogy between nuclear weapons and all cyber 'weapons' (loosely defined). Given that there is such a vast array of capability in cyberspace from cyber vandalism and espionage to cyber terrorism and kinetic cyber attacks, it is a straw-man comparison. The major critique of deterrence in cyberspace in these studies is that it is not possible to attribute. At the level of strategic cyber weapons, where there are currently only three actors, it is much easier to attribute attacks.
While countries such as North Korea and Iran have demonstrated impressive nascent capabilities in the Sony, Saudi Aramco, and Wall Street attacks and the U.K., France, and South Korea (among other countries) are all investing in cyber offensive capabilities, none of these countries have the national technical means of the U.S., Russia, or China. As Herb Lin notes, intelligence gathering "is superlatively important for cyber conflict." Smaller countries are not capable of designing and using strategic cyber weapons against enough centers of gravity to impose unacceptable costs on an adversary. Only the U.S., Russia, and China have the intelligence gathering and resources necessary to effectively wield strategic cyber weapons at the present. U.S. officials such as Director of National Intelligence James Clapper and Director of the NSA Admiral Michael Rogers have both confirmed this assessment in public testimony to congressional committees.
This thesis also examines the analogy from the U.S. perspective due to language and time constraints. To be clear, this is not a thesis about cyber vandalism, espionage, or terrorism, or cyber deterrence from the Russian or Chinese perspectives. These are important topics that deserve further investigation but are not discussed in this thesis.
Admiral Rogers in response the question: "There was a report that referred to Chinese attributed to the Chinese government hackers being in some of our critical infrastructure systems. Is there any nation-state that you believe has been successful in getting on the systems?" "There are probably one or two other (semi-apologize) If I couldn't consider that classified in an open hearing. I apologize but I am not comfortable spelling out specifics, but I would say there is more than one nation that we believe has the capability."
Director Clapper: "Advanced cyber actors – such as Russia and China – are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests."
Rogers, Michael. "Hearing on Cybersecurity Threats."
Clapper, James. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community." Senate Select Committee on Intelligence. March 12, 2013. Accessed March 16, 2015. http://www.intelligence.senate.gov/130312/clapper.pdf.
Lin, Herb. "Cyber Conflict and National Security." Transnational Actors and New Forces. Accessed May 21, 2015. http://www.lawfareblog.com/wp-content/uploads/2013/01/cyber-conflict-and-national-security-artjervis-reader-2.pdf.
Hecker, Siegfried. Interview by author. February 23, 2015.

[20] It is necessary to ask two questions in order to evaluate the nuclear-cyber deterrence analogy. First, do strategic cyber weapons constitute a revolution in military affairs? Second, do strategic cyber weapons have characteristics comparable to those that made nuclear weapons a strategic deterrent? Policymakers who favor the analogy typically

standards of what qualifies as a revolution in military affairs, as well as an outline of the structure of the thesis. To understand how nuclear and potentially strategic cyber weapons fall on the broader historical continuum of revolutions in military affairs, the first chapter examines the revolutions of the longbow, the tank, and the Offset technologies.[21] The second chapter provides an overview of the nuclear revolution in military affairs, establishing the template against which the following chapter compares strategic cyber weapons. The evaluation of the nuclear-cyber deterrence analogy in the third chapter comprises of testing to see if strategic cyber weapons qualify as a revolution in military affairs and if they have the strategic deterrent characteristics of nuclear weapons. The conclusion summarizes the findings of the thesis, speculates on the future paths of strategic cyber weapons, and suggests further opportunities for research.

Definition of Revolution in Military Affairs

The definition of a revolution in military affairs comes from multiple intellectual roots. Williamson Murray and Macgregor Knox, a pair of military historians, credit British historian Michael Roberts with coining the "related concept of "military revolution,"" in 1955.[22] Roberts was one of the first to apply the term to "fundamental systemic changes" in warfare.[23] Separately, the term "military technical revolution" surfaced in Soviet military journals when describing the Offset technologies "as early as the mid-1970s," according to Admiral William

---

leap to the second question first. This is problematic because the weapon systems are very different and a common denominator is necessary to examine the link. It also takes the maturation of a revolution (i.e. a technological and doctrinal development must have significant impact after its use) in order for its outcomes, (such as deterrence) to solidify. As a consequence, it is necessary to examine both questions.

[21] Offset technologies are technologies developed by the U.S. Department of Defense during the 1970s and 1980s as part of the Offset Strategy, which intended to 'offset' the Soviet conventional military advantage. The technologies include improved precision-guided munitions, stealth aircraft, sensors, GPS satellites and communications devices. The U.S. used these technologies to great effect during the First Gulf War.
Sapolsky, Harvey, Benjamin Friedman, and Brendan Green. U.S. Military Innovation Since the Cold War: Creation Without Destruction. Routledge, 2012. 157.

[22] Knox, MacGregor, and Williamson Murray. "Thinking About Revolutions in Warfare." In *The Dynamics of Military Revolution, 1300-2050*, 12. Cambridge, UK: Cambridge University Press, 2001.

[23] Knox, MacGregor, and Williamson Murray. "Thinking About Revolutions in Warfare."

Owens, former vice chairman of the Joint Chiefs of Staff.[24] Soviet Marshal Nikolai Ogarkov championed the label of military technical revolution as a way to justify requests for additional funding for the Soviet military.[25] Initially, some American analysts thought that the Soviets were propagandistically referring to their own technology, but Andrew Marshall of the Office of Net Assessment of the U.S. Department of Defense, realized that they were discussing the technological progress of American weaponry.[26] He agreed with their conclusions, but by 1993 Marshall thought that the term military technical revolution was "too narrow."[27] He thought that the term revolution in military affairs better represented the phenomenon's ability to "affect the entire spectrum of military affairs."[28] In the wake of the overwhelming U.S. victory in the First Gulf War, the concept became popular in academic and military literature.

Students of revolutions in military affairs have many definitions for the concept. Theodor W. Galdi, an international security specialist at the Congressional Research Service, argued in 1995 that there are three types of people when it comes to defining the term.[29] The first tend to focus "upon changes in the nation state and the role of an organized military in using force… [highlighting] the political, social and economic factors at play."[30] The second, and biggest, group emphasizes "the evolution of weapons, military organizations, and operational concepts

---

[24] Owens, William, and Theo Farrell. "Creating a U.S. Military Revolution." In *The Sources of Military Change: Culture, Politics, Technology*, 207. Boulder: Lynne Rienner Publishers, 2002.
[25] Owens, William, and Theo Farrell. "Creating a U.S. Military Revolution."
Chapman, Gary. "An Introduction to the Revolution in Military Affairs." XV Amaldi Conference on Problems in Global Security. September 1, 2003. Accessed December 4, 2014. http://www.lincei.it/rapporti/amaldi/papers/XV-Chapman.pdf.
[26] Owens, William, and Theo Farrell. "Creating a U.S. Military Revolution."
Sloan, Elinor C. *The Revolution in Military Affairs Implications for Canada and NATO*. Montreal: McGill-Queen's University Press, 2002. 27.
[27] Sloan, Elinor C. *The Revolution in Military Affairs Implications for Canada and NATO*.
[28] Sloan, Elinor C.
Owens, William, and Theo Farrell. "Creating a U.S. Military Revolution."
[29] Galdi, Theodor. "Revolution in Military Affairs? Competing Concepts, Organizational Responses, Outstanding Issues." Congressional Research Service. January 1, 1995. Accessed December 2, 2014. http://www.iwar.org.uk/rma/resources/rma/crs95-1170F.htm.
[30] Galdi, Theodor. "Revolution in Military Affairs? Competing Concepts, Organizational Responses, Outstanding Issues."

among advanced powers… [as well as] the changes made possible by advancing technology."[31] The third believes that "a true revolution in military affairs is unlikely" and that instead "there will be a continuing evolution in equipment, organizations, and tactics to adjust to changes in technology and the international environment."[32] The varying definitions of these groups sometimes make comparing their conversations difficult because they take such different approaches to the concept.

This thesis uses a definition drawn from several academic and military sources in the second group.[33] This definition is the most widely used within the literature and provides a rigorous framework through which to analyze the nuclear-cyber deterrence analogy. There are a few key elements to this definition. First, a revolution in military affairs is the result of a combination of an advance in technology and an adaptation in military organizational structure or doctrine to accommodate that technology. The timeframe for this component of the definition is flexible depending on the context. As Murray and Knox note, "Twentieth-century peacetime revolutions have sometimes required decades, and delays of that magnitude have inevitably led to the argument over the appropriateness of the term *revolutionary* [emphasis in the original]."[34] Second, a revolution in military affairs must fundamentally change the balance of power on the battlefield either by displacing an old power, by creating a new one, or both. RAND researcher

---

[31] Galdi, Theodor.
[32] Galdi, Theodor.
[33] Hundley, Richard. "Past Revolutions, Future Transformations." The RAND Corporation. Accessed December 5, 2014. http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1029.pdf. 13.
Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea." *Military Review* May-June 2010 (2010): 38-46.
Krepinevich, Andrew. "Cavalry to Computer; the Pattern of Military Revolutions." *The National Interest* 30, no. 13 (1994): 1-16.
Galdi, Theodor. "Revolution in Military Affairs? Competing Concepts, Organizational Responses, Outstanding Issues."
Ibrügger, Lothar. "The Revolution in Military Affairs." NATO Science and Technology Committee. Accessed December 8, 2014. http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html#1.
[34] Knox, MacGregor, and Williamson Murray. "Thinking About Revolutions in Warfare." In *The Dynamics of Military Revolution, 1300-2050*, 12. Cambridge, UK: Cambridge University Press, 2001.

Richard Hundley describes this phenomenon by stating that a revolution in military affairs renders "obsolete or irrelevant one or more core competencies of a dominant player, or creates one or more new core competencies of warfare, or both."[35] Third, a revolution in military affairs must result in a decisive victory, "attained in the immediate instance" according to Galdi.[36] Andrew Krepinevich, a defense policy analyst with an extensive U.S. military background, describes this moment as the point when water changes to ice; "Just as water changes to ice only when the falling temperature reaches 32 degrees Fahrenheit, at some critical point the cumulative effects of technological advances will… demand a fundamental change in the accepted definitions and measurement of military effectiveness."[37]

After the First Gulf War, scholars wrote extensively about how to identify a revolution in military affairs before it was demonstrated on the battlefield. Because strategic cyber weapons have never been used, this vibrant debate is particularly relevant. Hundley suggests that are two pathways for a revolution in military affairs to follow. The first goes through four phases (preparatory, breakthrough, exploitation and selling, and payoff) in which various technologies and military challenges combine to create a conceptual breakthrough which in turn leads to system development, testing, and acquisition, before use in combat.[38] The second is a chain (new technology, new device, new system, new operational concept, new doctrine and force structure, new military reality) in which the steps are interchangeable, but an interruption at any point could cause the revolution to fail.[39] Krepinevich's model has four stages: technological change,

---

[35] Hundley, Richard. "Past Revolutions, Future Transformations."
[36] Galdi, Theodor. "Revolution in Military Affairs? Competing Concepts, Organizational Responses, Outstanding Issues."
[37] In sum, this thesis defines revolutions in military affairs as an advance of technology accompanied by a change in strategy and doctrine that changes the balance of power by either displacing an old power or creating a new power in a moment of decisive victory.
Krepinevich, Andrew. "Cavalry to Computer; the Pattern of Military Revolutions."
[38] Hundley, Richard. "Past Revolutions, Future Transformations."
[39] Hundley, Richard.

system development, operational innovation, and organizational adaption.[40] Steven Metz and James Kievit, then an associate professor and an analyst at the U.S. Army War College, claim that there are five stages (stasis/initiation, critical mass, response – either symmetrical, asymmetrical, or both – consolidation, and stasis).[41] Metz and Kievit's model is cyclical, so as soon as an revolution in military affairs reaches stasis, it is primed for the next revolution in military affairs to take its place.[42]

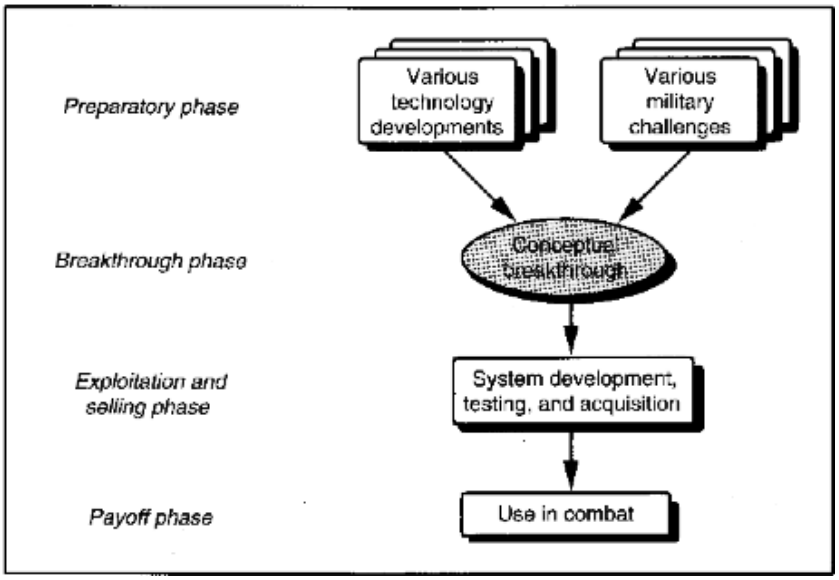


Figure 1: Hundley's First Revolution in Military Affairs Model[43]

[40] Krepinevich, Andrew. "Cavalry to Computer; the Pattern of Military Revolutions."
[41] Metz, Steven, and James Kievit. "Strategy and The Revolution in Military Affairs: From Theory to Policy." Strategic Studies Institute. Accessed December 4, 2014. http://www.au.af.mil/au/awc/awcgate/ssi/stratrma.pdf. 13.
[42] Metz, Steven, and James Kievit. "Strategy and The Revolution in Military Affairs: From Theory to Policy."
[43] Hundley, Richard. "Past Revolutions, Future Transformations."

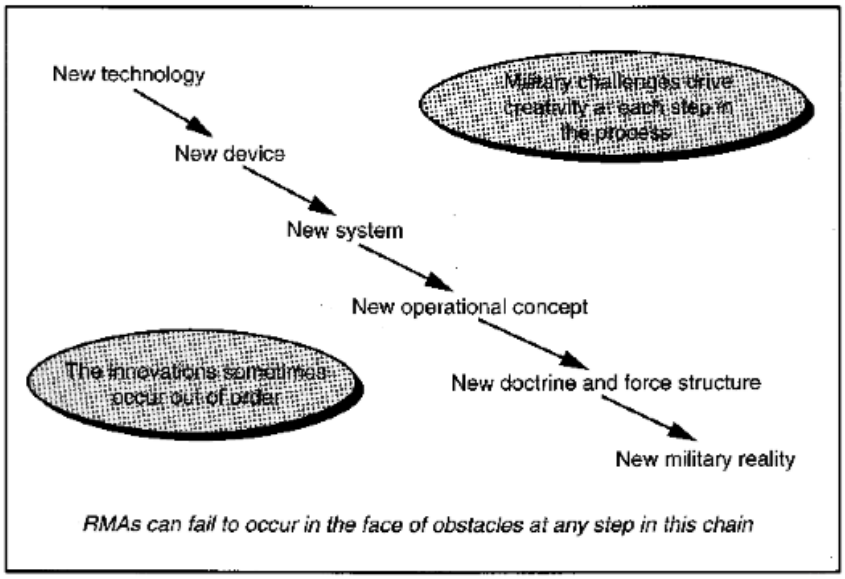


Figure 2: Hundley's Second Revolution in Military Affairs Model[44]

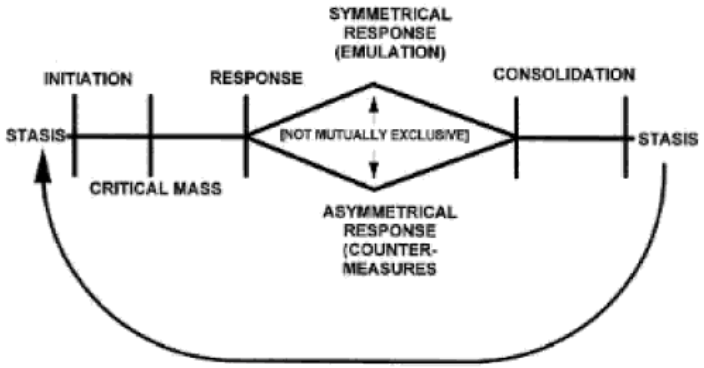


Figure 5. Pattern of Military Revolutions.

Figure 3: Metz and Kievit's Model [45]

Beyond a set of characteristics that apply to all revolutions in military affairs, several authors make a number of useful observations that are true of most revolutions in military affairs. Lieutenant Colonel Scott Stephenson (ret.), an associate professor at the U.S. Army Command and General Staff College, notes that revolutions in military affairs tend develop quickly regardless of whether militaries are ready to adapt or not (and by the same token revolutions in

[44] Hundley, Richard.
[45] Hundley, Richard.

military affairs can end almost as quickly as they begin).[46] He also observes that revolutions in military affairs often inspire counter revolutions in military affairs and that continuously leading revolutions in military affairs is difficult to do.[47] Hundley's observations are similar and help explain some of Stephenson's claims. For instance, Hundley notes that "dominant players" usually do not bring about revolutions in military affairs.[48] He asserts that revolutions in military affairs frequently are "fully exploited by someone other than the nation inventing the new technology," and that while "RMAs are not always technology-driven," "technology-driven RMAs are usually brought about by combinations of technologies, rather than individual technologies."[49] Metz and Kievit note that revolutions in military affairs are "cyclical processes," that require "the empowerment of visionaries."[50] They also state, "responses to revolutions in military affairs can be symmetric or asymmetric; asymmetric responses may be more difficult to counter."[51]

Structure of the Thesis

The first chapter provides an overview of three revolutions in military affairs throughout history to put nuclear weapons and strategic cyber weapons in the context of other revolutionary military technologies. The first is the longbow revolution in military affairs. The English doctrinal decision to mass archers armed with longbows in battle unlocked the weapons latent potential and displaced the armored knight as the primary military power on the battlefield at the time. The English demonstrated this to great effect against a much larger French force at the Battle of Crecy in 1346. The second is the tank revolution in military affairs. Although the

[46] Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea." *Military Review* May-June 2010 (2010): 38-46.
[47] Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea."
[48] Stephenson, Scott.
[49] Stephenson, Scott.
[50] Metz, Steven, and James Kievit. "Strategy and The Revolution in Military Affairs: From Theory to Policy." Strategic Studies Institute. Accessed December 4, 2014. http://www.au.af.mil/au/awc/awcgate/ssi/stratrma.pdf. 12.
[51] Metz, Steven, and James Kievit. "Strategy and The Revolution in Military Affairs: From Theory to Policy."

English invented the tank and used in the First World War, it was the Germans who developed the doctrine to exploit the technology. German tank tactics made the infantry-centric style of warfare of World War One irrelevant. The Germans made this quite clear when they overran the French in a matter of weeks during the Battle of France in 1940. The third is the Offset revolution in military affairs. The U.S. developed a series of technologies under the Offset strategy intended to 'offset' the Soviet conventional military advantage. Although the Americans never demonstrated how successful the weapons were against the Soviets themselves, they did against their technology during the First Gulf War.

The second chapter examines the nuclear revolution in military affairs and the characteristics that made nuclear weapons a strategic deterrent. The American decision to invest in the Manhattan Project to develop nuclear weapons, to change their military doctrine to accommodate them, and to use them on Hiroshima and Nagasaki led to a fundamental shift in the balance of power on the battlefield and a decisive defeat of the Japanese. As a result, nuclear weapons qualify as a revolution in military affairs. However, there are three characteristics that differentiate nuclear weapons from other revolutions in military affairs and make them a strategic deterrent. The first two are technological: the destructiveness of a single weapon and the assuredness of that destruction as a consequence of the delivery revolution.[52] The second is the debate over their use, which guided strategy and technological development to a point where strategic deterrence was possible.

The third chapter evaluates the nuclear-cyber deterrence analogy by comparing strategic cyber weapons to nuclear weapons. Strategic cyber weapons are an advance in technology and have prompted a change in doctrine, qualifying them for the first two standards of a revolution in

[52] The delivery revolution was the rapid development of delivery systems for nuclear weapons, such as long-range bombers, ballistic missiles, and nuclear-powered submarines, during the Cold War.

military affairs. However, they do not fundamentally change the balance of power on the battlefield and have not resulted in a decisive victory because the U.S. (or another large state) has never used them, so they have not matured as a revolution in military affairs. Strategic cyber weapons also do not compare to nuclear weapons' destructiveness or the assuredness of that destruction. Further, they do not have a comparable debate that would enable them to be a stable strategic deterrent. The concluding assessment is that it is not possible to make the nuclear-cyber deterrence analogy at the present.

The conclusion summarizes the findings, postulates several futures for strategic cyber weapons, and suggests avenues for further research. In the future, strategic cyber weapons could become a revolution in military affairs and a strategic deterrent, a revolution in military affairs and not a strategic deterrent, or not mature into a revolution in military affairs at all. Several factors, including the spread of technology, the improvement of strategic cyber weapons, and the development of cyber defenses, could all affect the future of strategic cyber weapons and the nuclear-cyber deterrence analogy. Possible further research includes investigating other aspects of the nuclear-cyber analogy and examining other analogues of strategic cyber weapons.

A Historical Overview: Three Revolutions in Military Affairs

> "Make no mistake, this weapon will change absolutely nothing."
> -French Director General of Infantry, commenting on the machine gun before the French parliament, 1910[53]

Introduction

Revolutions have a tendency of catching people off-guard. The French Director General of Infantry is a prime example. Strategic cyber weapons have the potential to be a revolution, possibly in the way that nuclear weapons were, which is part of the reason that the nuclear-cyber deterrence analogy exists. As noted in the introduction, this thesis uses two questions to evaluate this analogy. The first is whether strategic cyber weapons constitute a revolution in military affairs and the second is whether they have the strategic deterrent characteristics of nuclear weapons. To better understand the context in which this thesis asks the first question, this chapter passes three different military technologies through a set of tests to see if they qualify as revolutions in military affairs by the definition outlined earlier. To be considered a revolution, a weapon must represent an advance in technology, a change in military doctrine, a fundamental change in the balance of power on the battlefield, and a decisive victory. The three technologies that this chapter will examine are: the longbow, the tank, and the array of advanced American military technologies used during the Gulf War.

Those already familiar with the concept of revolutions in military affairs may proceed onto the next chapter. This chapter principally exists to examine these three technologies because they represent a diverse group of revolutions in military affairs that illuminate how the framework applies outside of the nuclear-cyber deterrence analogy. Understanding how the framework clarifies the process of the development, use, and impact of previous revolutionary

[53] Quoted in Hundley, Richard. "Past Revolutions, Future Transformations." The RAND Corporation. Accessed December 5, 2014. http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1029.pdf. 44.

military technologies can have important lessons for deciphering the potentially revolutionary weapons of today. For instance, had the French Director General and his contemporary peers viewed machine guns as more than just rifles that fired quickly, it is possible that they may have changed their tactics and avoided some of the disastrous outcomes of the First World War. This chapter is also important because the subsequent chapters will pass nuclear and strategic cyber weapons through the same set of tests. For each technology, this chapter will provide a brief historical fiction description of what it would be like to experience the maturation of the revolution and then a discussion of how each technology meets the criteria of a revolution in military affairs.

The Longbow Revolution in Military Affairs

John Oates watched as the last of the highly trained Genoese crossbowmen of the French army fled back towards their lines. Outranged and outshot by the English yeomen's longbow's range and rate of fire, they had left many of their companions behind on the field. In the distance, John could see the heavily armored French men-at-arms begin to ride towards his position. He looked back and saw with comfort lines of English men-at-arms on foot – horses hobbled at the rear – ready to support the lightly armored longbow men. He then turned his focus back towards the advancing line of French knights, the cream of the French military. He calmly nocked an arrow in his six-foot tall longbow, drew back the drawstring as he had countless times before, and listened for the order. Fire! John loosed the arrow.[54]

[54] This is an account of historical fiction based on the following sources:
"The Battle of Creçy 1346." British Battles. Accessed May 4, 2015. http://www.britishbattles.com/100-years-war/crecy.htm.
Knox, MacGregor. "England's Fourteenth-century RMA." In The Dynamics of Military Revolution, 1300-2050, 22-28. Cambridge, UK: Cambridge University Press, 2001.
Brodie, Bernard, and Fawn McKay Brodie. *From Crossbow to H-bomb*. Bloomington: Indiana University Press, 1973. 37-40.

When John Oates' arrow hit its intended target at the Battle of Crecy in 1346, it marked the long-coming maturation of the longbow revolution in military affairs.[55] The technological development of the longbow began many years before 1346. Archaeological digs discovered that the technology of the longbow has existed as a hunting weapon in the British Isles since the Neolithic Era.[56] The key difference between the longbow and other types of bows is that it is taller than its peers (typically between five and six feet in length), which enables it to have a longer maximum effective range and draw weight.[57] In military terms, this means it is possible to outrange adversaries and puncture through all but the best mail and plate armor.[58] Because the longbow was still a bow, it had a higher fire rate than other missile weapons. During the Hundred Years War, a bowman could fire as many as 10-12 arrows per minute, but on average during a battle fired around 5 or 6 per minute to conserve stamina.[59] By comparison, a crossbowman in the same time period could only fire a single bolt.[60] However, it took until the Middle Ages to unlock the latent military potential of the longbow.

The adaptation of military doctrine to the technology of the longbow occurred over a couple of centuries. The Welsh are the first recorded to use the longbow in battle to great effect

---

[55] There is an argument that the longbow is part of a larger infantry revolution in military affairs. Andrew Krepinevich contends that it was "tight formations of pole-arms and crossbowmen" elsewhere in Europe (primarily in Switzerland) in combination with English longbowmen that brought an end to the dominance of cavalry in medieval warfare. Instead of the Battle of Crecy in 1346, Krepinevich highlights the role of the Battle of Laupen of 1339, in which tight groups of Swiss pikemen unexpectedly triumphed over much larger forces of Burgundian and Hapsburg cavalry. Oman describes the battle as "the first time almost since the days of the Romans that infantry, entirely unsupported by horsemen… withstood an army in all arms and superior in numbers." However, for the sake of clarity, this chapter focuses only on the longbow.
Krepinevich, Andrew. "Cavalry to Computer; the Pattern of Military Revolutions."
Oman, Charles, and John Beeler. "The Swiss." In *The Art of War in the Middle Ages: A.D. 378-1515*, 49. Ithaca: Cornell University Press, 1968.

[56] "The History of the English Longbow." Historic UK. Accessed May 21, 2015. http://www.historic-uk.com/HistoryUK/HistoryofEngland/The-Longbow/.

[57] Kaiser, Robert. "The Medieval English Longbow." Journal of the Society of Archer-Antiquaries 23 (1980).

[58] "History of the Longbow." The Order of the Rye Longbowmen. Accessed May 21, 2015. http://www.ryelongbowmen.org/history-of-the-longbow/.

[59] Kaiser, Robert. "The Medieval English Longbow."

[60] "The Longbow: Medieval Weaponry." Military History Monthly. January 11, 2011. Accessed May 21, 2015. http://www.military-history.org/articles/medieval/the-longbow.htm.

beginning in 1054.[61] After learning the effectiveness of the weapon in battle, the English began incorporating the weapon into their military doctrine. King Edward I issued the Assize of Arms in 1252, which made it mandatory for yeomen owning land worth more than forty shillings to own and train with a longbow.[62] Because it takes years of training and strengthening to effectively wield the longbow, this act made England the only kingdom capable of fielding a force of thousands of longbowmen.[63] Clifford Rogers, a professor at the United States Military Academy at West Point, traces the birth of the longbow revolution back to a time between the Battle of Bannockburn in 1314 and the Battle of Dupplin Moor in 1332.[64] The English army fielded the longbow against the Scottish in both battles, but lost the first and overwhelmingly beat (by conservative estimates) a Scottish force ten times as large.[65] The primary appeal of incorporating longbowmen into the military is that they were far cheaper than men-at-arms, who were expensive to train and maintain. Andrew Krepinevich argues that the lower cost of longbowmen, which enabled the English to retain more of them, led to "a tactical system based on integrating archers with dismounted men-at-arms."[66] Rogers points to this tactic of combining dismounted men-at-arms armed with lances in close formation supported by longbowmen's "missile superiority" prevented the English from being dispersed by enemy missile fire that would make them vulnerable to cavalry charge.[67] Massing the archers was key to fully exploiting the technology. An often cited, but disputed, statistic is that English archers at the Battle of

[61] "Longbows, Arrows and the Origin of Fletchers." Fletcher Family. Accessed May 21, 2015. http://www.fletcher-family.co.uk/origins p1.html.
[62] "The Longbow." In Proceedings of the Numismatic and Antiquarian Society of Philadelphia, 122. Philadelphia: Franklin Printing Company, 1902.
[63] "History of the Longbow." The Order of the Rye Longbowmen.
[64] Rogers, Clifford. "'As if a New Sun had Arisen": England's Fourteenth-Century RMA." In *The Dynamics of Military Revolution, 1300-2050*, 20. Cambridge, UK: Cambridge University Press, 2001.
[65] Rogers, Clifford. "'As if a New Sun had Arisen": England's Fourteenth-Century RMA."
[66] Krepinevich, Andrew. "Cavalry to Computer; the Pattern of Military Revolutions." 3.
[67] Rogers, Clifford. "The Military Revolutions of the Hundred Years' War." *The Journal of Military History* 57, no. 2 (1993): 251.

Agincourt in 1415 fired 1000 arrows per second.[68] Rogers also notes that while the English were relatively quick to adopt this style of warfare, the tradition-bound French did not, so England was better positioned to take advantaged of the revolution in military affairs when it occurred.[69]

The combination of the unique technological characteristics and the English doctrinal changes shifted the balance of power on the battlefield when it displaced the power of mounted knights. For hundreds of years since the fall of the Roman Empire, nearly invulnerable armored men-at-arms riding horses dominated warfare.[70] C.W.C. Oman, a nineteenth century observer of military tactics, dates the "supremacy of feudal cavalry" from the Battle of Hastings in 1066 until the Battle of Crecy in 1346.[71] Krepinevich highlights that the six-foot yew longbow gave archers an "enhanced ability to penetrate the armor of cavalrymen… [and] also gave archers missile and range superiority over their adversaries."[72] By greatly reducing the protection that armor provided, the expensive and well-trained men-at-arms became less advantageous than cheaper and quicker to train longbowmen.[73] Following the Battle of Crecy, the importance of mounted knights diminished as militaries began to focus on developing their infantry, such as their archers firing longbows.

On August 26, 1346, King Edward III led a force of 12,000 English soldiers onto a ridge between the towns of Crecy and Wadicourt to face a French force of 30,000 led by King Philip

---

[68] "The Longbow." History Magazine. October 31, 1999. Accessed May 21, 2015. http://www.history-magazine.com/longbow.html.
[69] Rogers, Clifford. "The Military Revolutions of the Hundred Years' War." *The Journal of Military History* 57, no. 2 (1993): 250-51.
[70] Oman, Charles, and John Beeler. "The Swiss." In *The Art of War in the Middle Ages: A.D. 378-1515*, 49. Ithaca: Cornell University Press, 1968.
[71] Oman, Charles, and John Beeler. "Supremacy of Feudal Cavalry." In *The Art of War in the Middle Ages: A.D. 378-1515*, 49.
[72] Krepinevich, Andrew. "Cavalry to Computer; the Pattern of Military Revolutions." 2.
[73] Krepinevich, Andrew.

VI.[74] Conventional wisdom of the time dictated that the larger French force that had more armored knights should have slaughtered the lightly armored smaller English force. However, the opposite occurred. The French sent forth a force of 6,000 Genoese crossbowmen to skirmish against the English, but they did not last long against the longbowmen who outranged and out fired them.[75] They suffered heavy casualties and retreated, only for King Philip VI to order his knights to cut them down as they returned to the French lines.[76] The French knights then charged up the slope towards the English position, but clouds of arrows cut down wave after wave of knights to the point that the dead impeded the charges of the living.[77] In all, the French charged the English position 15 times and failed each time.[78] When the French had retreated from the battlefield, the lightly armored English went out onto the battlefield with knives and stabbed to death the French men-at-arms who lay pinned to the ground by the weight of their armor.[79] By the end of the battle, the French sustained an estimated 12,000 casualties and the English only between 100 and 300.[80] Following the battle, there was little question that the longbow had irreversibly changed the face of battle by elevating the role of the infantry, which it maintained arguably in land warfare through to the next revolution in military affairs discussed in this chapter.

[74] "Longbow Archers: The Battle of Crecy, 26 August 1346." Longbow Archers. Accessed May 21, 2015. http://www.longbow-archers.com/historycrecy.html.
[75] "The Battle of Crécy." English Monarchs. Accessed May 21, 2015. http://www.englishmonarchs.co.uk/battle_crecy.html.
[76] Froissart, Jean. "The Campaign of Crecy: Of the Battle of Crecy between the King of England and the French King." The Chronicles of Froissart. 1909. Accessed May 21, 2015. http://www.bartleby.com/35/1/110.html.
[77] "Longbow Archers: The Battle of Crecy, 26 August 1346."
[78] "Longbow Archers: The Battle of Crecy, 26 August 1346."
[79] Froissart, Jean. "The Campaign of Crecy: Of the Battle of Crecy between the King of England and the French King."
[80] "Longbow Archers: The Battle of Crecy, 26 August 1346."

The Tank Revolution in Military Affairs

Capitaine Henri Fortier sat in his office in the Ouvrage Schiesseck, which was located in the fortified sector of Rohrbach on the Maginot Line on the French-German border, mulling over the telegram on his desk. He tried to put the two young, fidgety lieutenants seated in front of him out of his mind and think over the events of the past several weeks that had led to this moment. He and his men had closely followed the frustratingly rapid advance of the German Panzer tank divisions over the radio while they sat in a bunker that had largely avoided contact with German forces. First the Germans bolted through Belgium, then charged into an undefended Paris, and finally throughout the country. They had listened to Marshal Philippe Pétain urging them to cease fighting after the fall of the French government. Now this telegram had arrived from the commander of the sector, ordering him and the other forts on the line to surrender to the Germans. He looked up at the lieutenants, sighed resignedly, and said, "C'est fini, nous devons capituler."[81]

Leonardo da Vinci first conceived of the tank in 1487, writing in a letter to the Duke of Milan, "I can make armored cars, safe and unassailable, which will enter the closed ranks of the enemy with their artillery, and no company of soldiers is so great that it will not break through them."[82] Da Vinci's idea lay dormant for hundreds of years until the development of the first tanks during the First World War, which used tractor technology to move artillery.[83] Lieutenant Colonel Ernest Swinton of the Royal Engineers proposed combining the two and Winston

[81] "Fort Schiesseck." 100th Infantry Division. Accessed May 4, 2015. http://www.100thww2.org/fortsch1.html.
Jackson, Julian. "We Are Beaten." In The Fall of France: The Nazi Invasion of 1940, 9-58. Oxford: Oxford University Press, 2003.
Shepperd, Alan. "The Battle for France." In France 1940: Blitzkrieg in the West, 31-88. London: Osprey, 1990.
[82] "The Tank." Leonardo Da Vinci's Inventions. 2015. Accessed May 21, 2015. http://www.leonardodavincisinventions.com/war-machines/leonardo-da-vincis-tank/.
[83] Walters, Guy. "A History of the Tank: From Leonardo Da Vinci to the Second World War." The Telegraph. 2014. Accessed May 21, 2015. http://www.telegraph.co.uk/sponsored/culture/film-fury/11146708/tank-history.html.

Churchill was enthused with idea of "land ships" to break the stagnant trench warfare.[84] The British built the earliest version of the tank, which was known as the Mark I, and debuted it at the Battle of the Somme in 1916.[85] Unlike the longbow, tanks developed remarkably quickly, going from concept to the battlefield in under three years.[86] The promise of these tanks was that they were bullet proof and could roll over barbed wire and trenches, opening the way for infantry to follow. However, these tanks were largely ineffective and often broke down on the battlefield, killing their crews.[87] While tanks did not play a decisive role in the First World War, all sides observed the potential of the weapon system and began to invest heavily in its development.[88] Interestingly, although the German tank design was initially inferior to those of the Allies at the outbreak of the Second World War, the Germans better exploited the revolutionary technology through the development of their doctrine.[89]

While all of the parties in the First World War studied the impact of the tank, only the Germans fully understood and exploited its potential. Following Germany's defeat in the First World War, German Army Command General Hans von Seeckt ordered and led a careful review of the lessons learned from German failures in the War.[90] The findings of that study led the Germans to write the *Truppenfuhrung* army manual of the early 1930s, which promoted a decentralized, combined-arms set of tactics that emphasized the role of mobile armored units, before the Germans even had developed the weapons.[91] This doctrine led the Germans to invest

[84] Walters, Guy. "A History of the Tank: From Leonardo Da Vinci to the Second World War."
[85] "Tanks in the World Wars." History. August 26, 2014. Accessed May 21, 2015. http://www.history.co.uk/study-topics/history-of-tanks/tanks-in-the-world-wars.
[86] "History of the Tank." Global Security. Accessed May 21, 2015. http://www.globalsecurity.org/military/systems/ground/tank-history1.htm.
[87] "Tanks in the World Wars." History.
[88] "Tanks in the World Wars."
[89] "Tanks in the World Wars."
[90] Murray, Williamson. "Contingency and Fragility of the German RMA." In *The Dynamics of Military Revolution, 1300-2050*, 162. Cambridge, UK: Cambridge University Press, 2001.
[91] Murray, Williamson. "Contingency and Fragility of the German RMA."

heavily in, among other technologies, tanks. By 1934, Germany created the Panzer I, which Germany improved and then used in large numbers initially in the Civil War in Spain and subsequently in the invasions of Poland and France along with the Panzer II.[92] In combination with dive-bombers, two-way radios, and artillery, tanks formed the heart of what would become known to the world as the Blitzkrieg doctrine. The Allies did not fully comprehend the revolutionary impact of the tank when combined with the revised German doctrine. As late as January 1940, U.S. Army Colonel Henry Reilly carefully detailed in *Foreign Affairs* how the Germans had married the lessons of World War One to the technology developed during the interwar period to rapidly defeat Polish forces in 1939, but that "Blitzkrieg would not be tried against the Maginot Line."[93] Instead be better applied in "Central Europe or the Balkans."[94] In a sense he was right, the Germans did not try their new combined-arms tactics against the Maginot Line – they went around it.

It is often said the generals plan to fight the last war. With the exception of the Great Wall of China, the Maginot Line is generally considered to be "the greatest system of permanent fortifications ever built."[95] In the hopes of preventing the bloodshed of the First World War, the French government invested nearly three billion francs into the fortifications along the French northern and northeastern border.[96] French military leadership believed that the fortifications would slow the Germans, who they assumed would invade again for revenge of the stringent

[92] "Panzer: German Tank." Encyclopedia Britannica Online. Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/1057539/panzer.
[93] Reilly, Henry J. "Blitzkrieg." Foreign Affairs 18, no. 2 (1940). Accessed May 21, 2015. https://www.foreignaffairs.com/articles/germany/1940-01-01/blitzkrieg.
[94] Reilly, Henry J. "Blitzkrieg."
[95] Smart, Nick. "The Maginot Line: An Indestructible Inheritance." *International Journal of Heritage Studies*: 225. Kemp, Anthony. *The Maginot Line: Myth and Reality*. New York: Stein and Day, 1982. 9.
[96] Panchasi, Roxanne. ""Fortress France": Protecting the Nation and Its Bodies, 1918-1940." Historical Reflections 33, no. 3 (2007): 477.

terms of the Versailles treaty (they got one thing right), until the French army mobilized.[97] Additionally, The commanders of the *Wehrmacht* and *Luftwaffe* in May of 1940 were well aware of this strategy, so instead of attacking the line directly they circumvented it. Using the mobility of their tanks and armored vehicles and the coordination capabilities of their radios, the Germans overwhelmed the French and the British with what appeared to be lightening quick maneuvers.[98] The advent of tanks in the First World War had shown the promise of these weapons systems in overcoming trench warfare, but the French and the British had maintained the mindset of the First World War, while the Germans had moved on doctrinally. The primary revolutionary impact of the tank was that it made the strategy and tactics of World War One obsolete. The Germans who recognized that benefitted the most initially. Before the German invasion of France, there were observers on both sides who believed that the odds favored the Allies and that the Germans would suffer half a million casualties in the initial outbreak of conflict that would stretch on for months.[99] At the time, France had the "world's most powerful army" which British, Belgian, and Dutch forces supplemented.[100]

The invading force of Germans split into two groups on May 10, 1940. The Germans wanted Army Group B, which invaded Holland and Belgium with 29 divisions, to attract the attention of the Allies while Army Group A forced its way through the Ardennes Forest.[101] The Allies were susceptible to this plan because they believed that the Germans would attack in a

---

[97] "The Maginot Line." History Learning Site. 2015. Accessed May 21, 2015. http://www.historylearningsite.co.uk/maginot_line.htm.
[98] Limbach, Raymond. "Blitzkrieg: Military Tactic." Encyclopedia Britannica Online. Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/69464/blitzkrieg.
[99] Frieser, Karl, and John T. Greenwood. The Blitzkrieg Legend: The 1940 Campaign in the West. Annapolis, Md.: Naval Institute Press, 2005. 151.
[100] Bynes, Eric. "The Line." *Intech*, 2007, 43. Accessed December 3, 2014. http://www.mtl-inst.com/images/uploads/datasheets/Intech_Mar_07_Net_security_(The_Line).pdf.
Hobson, Rolf. "Blitzkrieg, the Revolution in Military Affairs and Defense Intellectuals." *Journal of Strategic Studies*: 626.
[101] "Blitzkrieg (Lightning War)." United States Holocaust Memorial Museum. June 20, 2014. Accessed May 22, 2015. http://www.ushmm.org/wlc/en/article.php?ModuleId=10005437.

manner similar to the Von Schlieffen plan of the First World War and that the Ardennes Forest would be too dense for movement of massed armor.[102] Instead, 41,000 vehicles of *Panzergruppe Kleist* made their way through the closely bunched narrow trees of the Ardennes Forest over the course of two days.[103] When German forces emerged on the other side, they broke through French defenses on the Meuse River. Germans made better use of two-way radio and decentralized tactics to outmaneuver the Allied forces time and again.[104] The Germans quickly exploited the disorganization of French and British forces to force a major evacuation of Allied troops at Dunkirk, cut off the French from their troops on the Maginot Line, and forced the French into an embarrassing armistice.[105] Despite the French and British advantages of having more resources, higher quality tanks, and more time to plan for the invasion, the Germans prevailed with shocking results. Germany conquered France in a little over six weeks with around 27,000 German dead, a fraction of those killed in the multiple battles of the First World War.[106] Although the Germans initially caught the Allies off-guard with their tank and combined-arms tactics, the Allies soon symmetrically responded and defeated the Germans using similar tactics. The rapid, decentralized German style of warfare was the predecessor of what would become known as the Offset revolution in military affairs.

The Offset Revolution in Military Affairs

"Yaela, Yaela!" Corporal Ghalib Abdul-Rahman glanced up at his yelling company commander before hurrying his last-minute repairs of the T-72 tank, which had yet to actually have a kill on a coalition vehicle. This was not how he envisioned the elite 1st Armored Division

[102] Shepperd, Alan. "The Battle for France." In France 1940: Blitzkrieg in the West, 31-88. London: Osprey, 1990.
[103] Shepperd, Alan. "The Battle for France."
[104] Shepperd, Alan. "The Battle for France."
[105] "Franco-German Armistice: 1940." Encyclopedia Britannica Online. Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/216964/Franco-German-Armistice.
[106] "The Battle of France." German Propaganda Archive. July 22, 1940. Accessed May 21, 2015. http://research.calvin.edu/german-propaganda-archive/facts01.htm.

of the Iraqi Republican Guard conducting war against the American-led coalition. Corporal Abdul-Rahman's regiment had put up a solid resistance against the coalition forces, but the combination of the terrible firepower and accuracy of the American M1 Abrams tanks, Apache helicopters, and self-propelled artillery had steadily forced his regiment to withdraw. He shook his head in frustration, jumped up into his tank to join his crew, and gunned the engine to drive off quickly to fall into formation on Highway 8. Out of the corner of the small window portal on the tank, Corporal Abdul-Rahman saw the whirring of a group of Apache helicopters approaching the armor column. His heartbeat quickened. Before he could even open his mouth to warn his comrades, the tank two in front of his erupted into flames and then the one directly in front of his. Realizing there was nothing he could do, he offered a prayer moments before the flames engulfed him.[107]

The doctrinal and technological roots of the Offset revolution in military affairs reach back to the 1970s and 1980s when Secretary of Defense Harold Brown, Undersecretary of Defense William Perry, and Andrew Marshall of the Office of Net Assessment developed what would become known as the Offset Strategy. This strategy aimed to 'offset' the Soviet military's conventional advantage by exploiting U.S. technological advances in electronics and computers. The problem of the U.S. and NATO not having a credible conventional deterrent became increasingly salient as the Soviets weakened the U.S. nuclear advantage.[108] The military translations of that technology were improved precision-guided munitions, stealth aircraft,

[107] Hersh, Seymour. "Overwhelming Force." The New Yorker. March 22, 2000. Accessed May 4, 2015.
Gordon, Michael. "1991 Victory Over Iraq Was Swift, but Hardly Flawless." The New York Times. December 31, 2012. Accessed May 4, 2015.
"Persian Gulf War: 1990-1991." Encyclopedia Britannica Online. Accessed May 4, 2015. http://www.britannica.com/EBchecked/topic/452778/Persian-Gulf-War.

[108] Tomes, Robert R. "Military Innovation in the Shadow of Vietnam: The Offset Strategy." In US Defense Strategy from Vietnam to Operation Iraqi Freedom Military Innovation and the New American Way of War, 1973- 2003, 60. London: Routledge, 2007.

sensors, GPS satellites and communications devices.[109] Bill Perry stated that the Offset Strategy, "sought to use technology as an equalizer or 'force multiplier.'"[110] In other words, the U.S. aimed to deter Soviet conventional forces without having to fight on a tank-to-tank basis, which the U.S. simply was unwilling to match. The vision was to create a 'system of systems' that would coordinate and increase the performance of various systems throughout the U.S. military. Vice Chairman of the Joint Chiefs of Staff Admiral William Owens believed that if this could be achieved then the U.S. would enter a "qualitatively new order of military power."[111]

The impetus for the Offset Strategy was the general perception that Soviets maintained a conventional advantage over the Americans. Throughout the Cold War, the enormous number of Soviet tanks, artillery pieces, and other conventional weapons stationed in Eastern Europe meant that the U.S. would not be able to stop a Soviet incursion into Western Europe. The Offset Strategy technology meant that it would be possible for a smaller Western force to outcompete and defeat a larger Soviet force.[112] Although the U.S. never demonstrated this capability against the Soviets themselves, they did deploy it to great effect in the First Gulf War against the Soviet-armed Iraqi Army. Before the First Gulf War, Iraq had the fourth largest military in the world.[113] Current Secretary of Defense Ash Carter referred to it as "a miniature Warsaw Pact military."[114]After nearly eight years of war with the Iranians, Iraq's armed forces had considerable battle experience using the modern Soviet (and some French) military

[109] The rest of the chapter refers to these technologies as Offset technologies.
Sapolsky, Harvey, Benjamin Friedman, and Brendan Green. U.S. Military Innovation Since the Cold War: Creation Without Destruction. Routledge, 2012. 157.
[110] Tomes, Robert R. "Military Innovation in the Shadow of Vietnam: The Offset Strategy." 58.
[111] Sloan, Elinor C. *The Revolution in Military Affairs Implications for Canada and NATO*.
[112] Work, Bob. "National Defense University Convocation." United States Department of Defense. August 5, 2014. Accessed May 21, 2015. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1873.
[113] Perry, William J. "Desert Storm and Deterrence." Foreign Affairs, 1990, 66-82. Accessed May 21, 2015. https://www.foreignaffairs.com/articles/iraq/1991-09-01/desert-storm-and-deterrence.
[114] Carter, Ashton B. "Keeping America's Military Edge." Foreign Affairs 80, no. 1 (2001): 90. Accessed May 21, 2015. https://www.foreignaffairs.com/articles/united-states/2001-01-01/keeping-americas-military-edge.

technology.[115] Particularly of note, it had what was broadly thought to be a sophisticated air defense system.[116] On the eve of the Gulf War, it seemed likely that the U.S.-led coalition would suffer substantial casualties. A 1990 article in the LA Times reported that, off-the-record, military officials projected U.S. 30,000 casualties.[117] The most conservative estimates had about 160 Americans dead for each day of the war.[118] As it would turn out, even the Americans did not fully understand the revolutionary aspects of the technology from the Offset Strategy until its use. The American technology deceived and decimated the Soviet-provided sensors and weaponry prompting. Soviet foreign minister Aleksandr A. Bessmertynyk had to defend Soviet military technology before the Supreme Soviet by saying the coalition win was "not a reflection of a weakness of [Soviet-provided Iraqi] combat equipment. Ultimately equipment is good when it is in good hands."[119] Knox and Murray responded by observing, "The Iraqis admittedly displayed extraordinary ineptitude at every level. But virtually every other revolution in military affairs has required a victim whose battlefield inadequacies have accentuated the disparity between old and new. Edward III required the poorly organized armies of feudal France to win the great victory of Crécy … and the *Wehrmacht* of 1940 required General Maurice Gamelin to show its capabilities to the fullest."[120]

---

[115] Perry, William J. "Desert Storm and Deterrence."
[116] Perry, William J. "Desert Storm and Deterrence."
[117] "Potential War Casualties Put at 100,000: Gulf Crisis: Fewer U.S. Troops Would Be Killed or Wounded than Iraq Soldiers, Military Experts Predict." Los Angeles Times. September 5, 1990. Accessed May 21, 2015. http://articles.latimes.com/1990-09-05/news/mn-776_1_military-experts.
[118] "Potential War Casualties Put at 100,000: Gulf Crisis: Fewer U.S. Troops Would Be Killed or Wounded than Iraq Soldiers, Military Experts Predict." Los Angeles Times.
[119] "Bessmertnykh Talks About Soviet-Built Weapons." Friends & Partners. Accessed December 8, 2014. http://www.friends-partners.org/friends/news/omri/1991/01/910118.html(opt,mozilla,unix,russian,koi8,new).
[120] Similarly, Marshal of the U.S.S.R. Viktor Kulikov emphasized the "human factor" in an interview with INTERFAX as the key element that led to the Iraqi forces' defeat.
Stephen Biddle, a professor at the Elliot School of International Affairs at George Washington University and a senior fellow on the Council of Foreign Relations, outlines a third view. He states, "in general, late-twentieth century technology may be magnifying the effects of skill differentials on the battlefield… The main effect of new technology may thus be to act as a wedge, gradually driving apart the real military power of states that can field

On January 17, 1991, the Coalition began a month-long bombing campaign of Iraq's military and civilian infrastructure. In total, fighter pilots of the Coalition flew 100,000 sorties and dropped 88,500 tons of bombs.[121] This figure is noteworthy because the tonnage was just a fraction of the tonnage used in the previous wars, meaning that the bombs were effectively targeted.[122] Despite Iraq's vaunted air defense system, the Coalition only suffered 75 aircraft losses and the Iraqis caused just 44 of those losses during this period.[123] The F-117, a stealth bomber developed in the late 1970s under the aegis of Bill Perry, proved to be essential in the air campaign because it was virtually invisible to Iraqi radar.[124] Following the air campaign, which established Coalition air supremacy, the Coalition launched a massive ground campaign. The integration of satellites, location, and communication technology gave U.S. armed forces a massive advantage in being able to maneuver and target enemy forces in the featureless desert,

---

skilled military organizations and those that cannot, but without changing fundamentally the outcomes of wars between equally skilled armies."
Perry, William J. "Desert Storm and Deterrence."
Villahermosa, Gilberto, and David M. Glantz. "Foreign Military Studies Office Publications - Desert Storm: The Soviet View." Foreign Military Studies Office Publications. Accessed December 8, 2014. http://fmso.leavenworth.army.mil/documents/rs-storm.htm#77a.
Knox, MacGregor, and Williamson Murray. "Conclusion: The Future Behind Us." In *The Dynamics of Military Revolution, 1300-2050*, 188.
"Stephen Biddle." Elliott School of International Affairs. Accessed December 8, 2014. https://elliott.gwu.edu/biddle.

[121] Moïse, Edwin. "Limited War: The Stereotypes." Clemson University. November 22, 1998. Accessed May 21, 2015. http://www.clemson.edu/caah/history/FacultyPages/EdMoise/limit1.html.

[122] The U.S. dropped 1,613,000 tons in the European theater of the Second World War and 6,715,000 tons in Vietnam, Cambodia, and Laos.
Moïse, Edwin. "Limited War: The Stereotypes."

[123] "The Unfinished War: A Decade Since Desert Storm." CNN. 2001. Accessed May 21, 2015. https://web.archive.org/web/20080612131747/http://www.cnn.com/SPECIALS/2001/gulf.war/facts/gulfwar/.
Lee, Robin. "Coalition Fixed-Wing Combat Aircraft Attrition in Desert Storm." Estimative Error Probable. 2014. Accessed May 21, 2015. http://www.rjlee.org/air/ds-aaloss/.

[124] The air campaign led Colonel John Warden, an Air Force officer, to claim, "The world has just witnessed a new kind of warfare – hyperwar. It has seen air power become dominant… We have moved from the age of the horse and the sail through the age of the battleship and the tank to the age of the airplane. Like its illustrious ancestors, the airplane will have its day in the sun, and then it too shall be replaced. *Sic transit gloria mundi* [emphasis in the original]"
Warden, John A., and Richard H. Shultz. "Employing Air Power in the Twenty First Century." In *The Future of Air Power in the Aftermath of the Gulf War*, 82. Honolulu: University Press of the Pacific, 2002.
Citino, Robert. "Technology in the Persian Gulf War of 1991." The Gilder Lehrman Institute of American History. 2015. Accessed May 21, 2015. http://www.gilderlehrman.org/history-by-era/facing-new-millennium/essays/technology-persian-gulf-war-1991.

even during sandstorms.[125] Because almost all mechanized vehicles and aircraft had thermal sight capability, the U.S. continued fighting into the night, which helps explain how Coalition forces destroyed 3,847 of 4,280 Iraqi tanks in combat.[126] On February 27, 1991, President George H.W. Bush declared the liberation of Kuwait and a ceasefire after 100 hours of ground combat.[127] The U.S. armed forces sustained a total of 383 deaths, of which only 148 were battlefield deaths.[128] By comparison, U.S. Central Command reported that "more than 100,000 Iraqi soldiers died, 300,000 were wounded, 150,000 deserted, and 60,000 were taken prisoner."[129] The sweeping victory of the U.S.-led forces prompted observers to compare the invasion to the Blitzkrieg invasions of World War Two. However as Lawrence Freedman and Efraim Karsh, professors of War Studies and Middle East and Mediterranean Studies at King's College London, note the Coalition suffered less than one twentieth of the Germans' casualties in their Blitzkriegs against Poland or France in 1930-40."[130] The Gulf War unquestionably placed the technology and tactics of the Offset Strategy in the pantheon of revolutions in military affairs.

Failed Revolutions in Military Affairs

While successful revolutions in military affairs are well known because they result in decisive victories, failed revolutions in military affairs are forgotten because they never became more than peculiarities. However, just because they are obscure does not mean they do not exist.

---

[125] Citino, Robert. "Technology in the Persian Gulf War of 1991."
[126] Citino, Robert. "Technology in the Persian Gulf War of 1991."
[127] Bush, George H. W. "This Day in History: George H.W. Bush Announces End of Gulf War." Miller Center. February 27, 1991. Accessed May 21, 2015. http://millercenter.org/ridingthetiger/george-h.w.-bush-announces-end-of-gulf-war.
[128] DeBruyne, Nese, and Anne Leland. "American War and Military Operations Casualties: Lists and Statistics." Congressional Research Service. January 2, 2015. Accessed May 21, 2015. https://www.fas.org/sgp/crs/natsec/RL32492.pdf.
[129] "The Unfinished War: A Decade Since Desert Storm." CNN.
[130] Freedman, Lawrence, and Efraim Karsh. *The Gulf Conflict 1990-1991: Diplomacy and War in the New World Order*. Princeton, N.J.: Princeton University Press, 1994. 409.
Biddle, Stephen. "Victory Misunderstood: What the Gulf War Tells Us about the Future of Conflict." *International Security*: 139-79.

As Richard Hundley observes, “There are probably as many failed RMAs as successful RMAs.”[131] The Confederate inventors of the double-barreled cannon, for instance, had hoped that two cannon balls connected by a long chain fired out of the gun would "sweep across the battlefield and mow down the enemy somewhat as a scythe cuts wheat."[132] Although intended for battle, the double-barreled cannon dramatically failed its test shots and the South never used the weapon in the Civil War.[133] During the Second World War, the British Department of Miscellaneous Weapons Development had equally ambitious goals for the Great Panjandrum. The Great Panjandrum was a drum with over a ton of high explosive set on a pair of wheels propelled by rockets.[134] It was meant to storm up the beaches of France and blow a tank-size hole in Nazi fortifications.[135] However, it also failed during the testing process and nearly killed the observing general officers.[136] The Boeing YAL-1 Airborne Laser was a chemical oxygen iodine laser mounted on a Boeing 747-400F that was supposed to intercept ballistic missiles.[137] It had a little more success than its peers. Unlike the double-barreled cannon and the Great Panjandrum, the laser actually worked and destroyed a solid-fuelled ballistic missile in its boost phase.[138] However beyond the test range, the Boeing YAL-1 Airborne Laser was not very practical as it was too expensive and did not have enough range to be effective. Secretary Robert Gates reported to Congress “I don't know anybody at the Department of Defense… who thinks that this

[131] Hundley, Richard. xiv.
[132] King, Spencer Bidwell. "Second War for Independence." In Georgia Voices: A Documentary History to 1872, 284. Athens: University of Georgia Press, 2010.
[133] King, Spencer Bidwell. "Second War for Independence."
[134] Johnson, Brian. "Misfortunes of War." In The Secret War, 266-270. Barnsley: Leo Cooper, 2004.
[135] Johnson, Brian. "Misfortunes of War." In The Secret War, 266-270. Barnsley: Leo Cooper, 2004.
[136] Johnson, Brian. "Misfortunes of War." In The Secret War, 266-270.
[137] "'Laser Jumbo' Testing Moves Ahead." BBC News. July 29, 2008. Accessed May 22, 2015. http://news.bbc.co.uk/2/hi/science/nature/7531046.stm.
[138] "Airborne Laser Test Bed Successful in Lethal Intercept Experiment." U.S. Missile Defense Agency. February 11, 2010. Accessed May 22, 2015. http://www.mda.mil/news/10news0002.html.

program should, or would, ever be operationally deployed."[139] After sixteen years of development and five billion dollars of investment, the Pentagon cancelled the program.[140] All of these weapons had the potential to be revolutions in military affairs. They represented advances in technology and militaries prepared to adapt their doctrines to accommodate them. However, ultimately all of the weapons proved to be impractical for combat either during or after the testing phase and never produced a change in the balance of power on the battlefield or a decisive victory.

Conclusion

The concept of revolutions in military affairs is a powerful framework for understanding the impacts of revolutionary military technology throughout history. The cases of the longbow, the tank, and the Offset technologies, each represent an advance in technology, an accompanying advance in military doctrine, a fundamental change in the balance of power on the battlefield, and a decisive victory. For each weapon that overturned the conventional wisdom on warfare, the adversary (and sometimes the user) underestimated or misunderstood the power of the weapons system with highly deleterious consequences. The same potentially could be true for strategic cyber weapons. These weapons could well achieve the revolutionary status of the armor piercing capabilities of the longbow, the speed of blitzkrieg, or the almost bloodlessness (for the attackers) of the Offset revolution in military affairs. It also could fail. Regardless, as history has

[139] Full quotation from Secretary Gates: "I don't know anybody at the Department of Defense, Mr. Tiahrt, who thinks that this program should, or would, ever be operationally deployed. The reality is that you would need a laser something like 20 to 30 times more powerful than the chemical laser in the plane right now to be able to get any distance from the launch site to fire. So, right now the ABL would have to orbit inside the borders of Iran in order to be able to try and use its laser to shoot down that missile in the boost phase. And if you were to operationalize this you would be looking at 10 to 20 747s, at a billion and a half dollars apiece, and $100 million a year to operate. And there's nobody in uniform that I know who believes that this is a workable concept."
"Missile Defense Umbrella?" Center for Strategic and International Studies. Accessed May 22, 2015. http://csis.org/blog/missile-defense-umbrella.

[140] Butler, Amy. "Lights Out For The Airborne Laser." Lights Out For The Airborne Laser. December 21, 2011. Accessed May 22, 2015. http://aviationweek.com/awin/lights-out-airborne-laser.

repeatedly shown, it is better to study potential revolutions in military affairs carefully than to dismiss them out of hand. The next chapter examines the nuclear revolution in military affairs, which out of all of the revolutions to the present, could be the most similar to a potential cyber revolution in military affairs.

The Baseline: The Nuclear Revolution in Military Affairs

"I am become death, destroyer of worlds."
-J. Robert Oppenheimer, Trinity Test Site, July 16, 1945[141]

Introduction

Following the fission of a nuclear weapon's uranium or plutonium, temperatures that peak in the tens of millions of degrees instantly transform the weapon's casings into gases.[142] Less than a millionth of a second later, the energy released from the bomb creates a spherical fireball that rapidly rises to heights of as much as twelve miles while cooling and air drag shape the resulting radioactive cloud into what is popularly known as a 'mushroom cloud.'[143] A shock wave of compressed air and thermal radiation, as well as an electromagnetic pulse and radioactive fallout, accompany the initial explosion.[144] Such a demonstration of raw power at the first nuclear test prompted the scientific director of the Manhattan Project to utter the emblematic phrase in the epigraph above.

Like the longbow, the tank, or the Offset technologies, nuclear weapons qualify as a revolution in military affairs. However, the unique technological characteristics of nuclear weapons and the influential debate over their use set the weapons apart from their peers. Over time, the world came to realize that these distinctive aspects of nuclear weapons made them capable of providing a stable strategic deterrent. To date, there has not been another weapon that can do the same, although there are a considerable number of policymakers today who believe that strategic cyber weapons can. To evaluate the nuclear-cyber deterrence analogy this chapter inspects what made nuclear weapons a strategic deterrent. After it demonstrates that nuclear

[141] "The Gita of J. Robert Oppenheimer." *Proceedings of the American Philosophical Society* 144, no. 2 (2000): 123.
[142] Walker, Gregory. "The Effects of Nuclear Weapons: Descriptions of Nuclear Explosions." Trinity Atomic Web Site. Accessed May 21, 2015. http://www.abomb1.org/nukeffct/enw77b1.html.
[143] Walker, Gregory. "The Effects of Nuclear Weapons: Descriptions of Nuclear Explosions."
[144] Walker, Gregory.

weapons pass the standards of a revolution in military affairs, it then looks at the characteristics that make it different from every other revolution in history. First, it examines the sheer destructiveness of a single nuclear weapon and the assuredness of that destruction via the revolution in the delivery of nuclear weapons (henceforth the delivery revolution).[145] Second, it provides an overview of the American debate over the use of nuclear weapons played an instrumental role in leading to the stabilization of deterrence. In doing this, the chapter creates a template for nuclear weapons and their strategic deterrent capabilities that is possible to compare with strategic cyber weapons.

The Nuclear Revolution in Military Affairs

Tailgunner Staff Sergeant Robert Caron braced himself in his turret at the rear of the Enola Gay for the sudden rise in the airplane as it released its 9700-pound payload. As the atomic bomb, nicknamed Little Boy, fell towards Hiroshima the much lighter B-29 Enola Gay surged up into the air and then banked into planned evasive maneuver. Staff Sergeant Caron watched the city of Hiroshima with dreading anticipation and began counting. One, two, three... For what seemed like an eternity, nothing happened. Thirty-nine, forty-one, forty-two… Then, soundlessly, a blinding flash of light geometrically expanded high into the sky and temporarily blinded him. Forced to look away into the darkness of the cabin, he saw the experienced Colonel Paul Tibbets give radio operator Private Richard Nelson an affirming nod. Private Nelson transmitted a simple, two-word message to the President of the United States, "Results, excellent."[146]

---

[145] The delivery revolution was the rapid development of delivery systems for nuclear weapons, such as long-range bombers, ballistic missiles, and nuclear-powered submarines, during the Cold War.

[146] This is an account of historical fiction based on the following sources:
Caron, George. "Enola Gay - Tail Gunner - Bob Caron Radio Interview - 1953." YouTube. January 1, 1953. Accessed January 27, 2015. https://www.youtube.com/watch?v=ot80m7XWSz4.
"Enola Gay Crew." Atomic Archive. Accessed January 27, 2015. http://www.atomicarchive.com/Photos/Tinian/image1.shtml.

The intellectual roots of nuclear fission, the key technological advance of nuclear weapons, can arguably be traced as far back as 1789 when Martin Kalproth discovered uranium, when Pierre and Marie Curie discovered radium and polonium in 1898, or when Albert Eistein expounded his special theory of relativity in 1905.[147] However, most agree that Leó Szilárd's realization of the possibility a nuclear chain reaction after he stepped off a curb in 1933 was a critical turning point.[148] Subsequent discoveries by German scientists Otto Hahn, Fritz Strassman, and Lise Meitner in the late 1930s led the scientific community to understand that nuclear fission could create a highly destructive bomb.[149] In the context of the geopolitical tensions of the time, this understanding led to the swift translation of the concept from theory into practice. Although Germany was quick to begin a nuclear weapons project in 1939, the demands and pressures of the war forced German Army Ordinance Office to relegate the effort to laboratory research project by 1942.[150] Unaware of this event, a number of scientists – including Leo Szilard, Albert Einstein, and Edward Teller – pressured the U.S. government to

---

Caron, George Robert, and Charlotte Meares. "Chapter 1." In *Fire of a Thousand Suns: The George R. "Bob" Caron Story, Tail Gunner of the Enola Gay*, 1-3. Westminister, Colo.: Web Pub., 1995.
"Manhattan Project: The Atomic Bombing of Hiroshima, August 6, 1945." U.S. Department of Energy. Accessed January 27, 2015. https://www.osti.gov/manhattan-project-history/Events/1945/hiroshima.htm.

[147] "Martin Heinrich Klaproth." Encyclopedia Britannica Online. Accessed January 27, 2015. http://www.britannica.com/EBchecked/topic/319885/Martin-Heinrich-Klaproth.
"Marie and Pierre Curie and the Discovery of Polonium and Radium." Nobel Prize. Accessed January 27, 2015. http://www.nobelprize.org/nobel_prizes/themes/physics/curie/.
"Ernest Rutherford." Chemical Heritage Foundation. Accessed January 27, 2015. http://www.chemheritage.org/discover/online-resources/chemistry-in-history/themes/atomic-and-nuclear-structure/rutherford.aspx.

[148] Rhodes, Richard. "Moonshine." In *The Making of the Atomic Bomb*, 13, 28. 25th Anniversary ed. New York: Simon & Schuster Paperbacks, 2012.
Lackey, Douglas P. "Nuclear Weapons, Politics, and Strategy: A Short History." In *Moral Principles and Nuclear Weapons*, 31-36. Totowa, N.J.: Rowman & Allanheld, 1984.

[149] Rhodes, Richard. "Moonshine."

[150] Walker, Mark. "Lightening War." In *German National Socialism and the Quest for Nuclear Power, 1939-1949*, 17-24. Cambridge: Cambridge Univ. Press, 1989.
Burns, Richard Dean, and Joseph M. Siracusa. "Vying for an A-bomb: World War II Contestants." In *A Global History of the Nuclear Arms Race: Weapons, Strategy, and Politics*, 1-5.

build an atomic bomb before the Nazis did.[151] The United States, in partnership with the British and the Canadians, designed and tested a nuclear weapon in less than 27 months under the aegis of the multi-billon dollar Manhattan Project.[152] The improvement in military technology was substantial. Dr. Sidney Drell, a theoretical physicist and arms control expert, describes increase in the "degree in devastation" from a conventional to a nuclear bomb as "quantum leap."[153]

Such a jump in military capability demanded innumerable changes in military doctrine and strategy. Simply put, nuclear weapons were not treated like any other weapon in the arsenal. Since the beginning of their existence, only the President had the ability to order the use of nuclear weapons.[154] The military did not start planning for the use of nuclear weapons until after their use due to the secrecy surrounding their development.[155] Once it did, the military drastically changed itself to support the delivery of nuclear weapons, making Strategic Air Command its own branch, modifying equipment acquisition planning, and redirecting training programs.[156] The U.S. has spent trillions of dollars investing in scientific research for both increasing the destructiveness and deliverability of nuclear weapons since the beginning of the Manhattan Project.[157] As described later in the chapter, these weapons also sparked an enormous debate in and out of the government over how to use them. Consequently, American doctrine of whether

---

[151] Cantelon, Philip L. "The Nuclear Age." In *The American Atom: A Documentary History of Nuclear Policies from the Discovery of Fission to the Present*, 3-10. 2nd ed. Philadelphia: University of Pennsylvania Press, 1991.
[152] "Manhattan Project." Encyclopedia Britannica Online. Accessed January 28, 2015. http://www.britannica.com/EBchecked/topic/362098/Manhattan-Project.
"The Manhattan Project: Making the Atomic Bomb." The Uranium Committee. Accessed January 28, 2015. http://www.atomicarchive.com/History/mp/p2s1.shtml.
"Manhattan Project." CTBTO Preparatory Commission. Accessed May 10, 2015. http://www.ctbto.org/nuclear-testing/history-of-nuclear-testing/manhattan-project/manhattan-project/.
[153] Drell, Sidney. Interview by author. March 5, 2015
[154] Nelson, Michael. "Commander in Chief." In The Powers of the Presidency, 279. Washington, DC: CQ Press, 2008.
[155] Meilinger, Phillip S. "Formation." In Bomber: The Formation and Early Years of Strategic Air Command, 71. Maxwell Air Force Base, Ala.: Air University Press, Air Force Research Institute, 2012.
[156] Meilinger, Phillip S. "Formation."
[157] Schwartz, Stephen. Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons Since 1940. 3

the U.S. should use nuclear weapons against civilian or military targets, preemptively or only in retaliation, all at once or in waves, changed over time.

Nuclear weapons dramatically shifted the balance of power on the battlefield from the defense to the offense. The result was that they rapidly made many forms of military technology, doctrine, and organization obsolete, as well as created whole new fields of science and technology and altered the conduct of international relations. Although hotly debated, nuclear weapons effectively made defenses against nuclear-armed planes and missiles obsolete because if even a single weapon could get through then the effects would be catastrophic. The effects of a nuclear weapon also meant that for the first time in history, humans used a weapon twice in war and (until this point) never used it again.[158] Some, such as the famous American strategist Bernard Brodie, even suggested that nuclear weapons necessitated a change in the basic motivations for conventional militaries. In *The Absolute Weapon,* Brodie states, "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose."[159] The delivery revolution also expanded the battlefield to a global scale and made the political leader in charge of their use the "first soldier" in war that could end human existence.[160]

On August 6, 1945, the U.S. Air Force dropped an atomic weapon on Hiroshima. Three days later, it dropped another on Nagasaki. The two fission bombs had yields of 15 and 21 kilotons, respectively, that resulted in an estimated combined death toll of around 200,000 people.[161] By contrast, the U.S. did not suffer a single casualty in the two attacks.[162] In both

[158] Cimbala, Stephen J. "Alternative Nuclear Regimes." In *Nuclear Weapons and Cooperative Security in the 21st Century: The New Disorder*, 11. London: Routledge, 2010.
[159] Brodie, Bernard, and Frederick Sherwood Dunn. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and, 1946.
[160] Nelson, Michael. "Commander in Chief."
[161] Malik, John. "The Yields of the Hiroshima and Nagasaki Explosions." Los Alamos National Laboratory. September 1, 1985. Accessed January 27, 2015. http://library.lanl.gov/cgi-bin/getfile?00313791.pdf. 1.

cases, the Japanese detected the bombers, but determined that they were not a threat because there were so few of aircraft.[163] As a 'battle,' it was arguably the most decisive in history. In terms of the larger war, Emperor Hirohito announced the surrender of Japan on August 15th while citing the existence of atomic weapons and the country unconditionally surrendered on September 2nd.[164] In addition this decisive victory, the nuclear revolution in military affairs had another revolution. The detonation of the first thermonuclear weapon in the "Ivy Mike" test in 1952 increased the destructive power of nuclear weapons by several orders of magnitude.[165] Although never used in battle, these weapons also constitute a revolution in their own right.[166]

"The Atomic Bombings of Hiroshima and Nagasaki." Total Casualties. Accessed January 27, 2015. http://www.atomicarchive.com/Docs/MED/med_chp10.shtml.

[162] This is true of the attacking force. A number of American and Allied prisoners of war died on the ground because of the detonation.
"Americans Killed by Atomic Bomb to Be Honored in Hiroshima." AllGov. June 4, 2009. Accessed May 21, 2015. http://www.allgov.com/news/us-and-the-world/americans-killed-by-atomic-bomb-to-be-honored-in-hiroshima?news=838959.
"Nagasaki Memorial Adds British POW as A-bomb Victim." The Japan Times. June 24, 2005. Accessed May 21, 2015. http://www.japantimes.co.jp/news/2005/06/25/national/nagasaki-memorial-adds-british-pow-as-a-bomb-victim/#.VV1qwqZGy2z.

[163] "The Atomic Bombings of Hiroshima and Nagasaki: The Attacks." The Atomic Archive. Accessed May 21, 2015. http://www.atomicarchive.com/Docs/MED/med_chp7.shtml.

[164] There is some controversy over whether Japan surrendered because of the opportunistic Soviet declaration of war on Japan on August 9th, which Emperor Hirohito did not mention in his surrender speech, or the dropping of atomic weapons on Hiroshima and Nagasaki. However, this thesis will not engage in this debate as it is beyond the scope of the project. For further reading on the subject see:
Wilson, Ward. "The Bomb Didn't Beat Japan… Stalin Did." Foreign Policy. May 30, 2013. Accessed May 21, 2015. http://foreignpolicy.com/2013/05/30/the-bomb-didnt-beat-japan-stalin- did/.
Hasegawa, Tsuyoshi. Racing the Enemy: Stalin, Truman, and the Surrender of Japan. Cambridge, Mass.: Belknap Press of Harvard University Press, 2005.
Bix, Herbert P. "Hiroshima in History and Memory: A Symposium, Japan's Delayed Surrender: A Reinterpretation." Diplomatic History: 197-225.
Bernstein, Barton J. "Compelling Japan's Surrender without the A-bomb, Soviet Entry, or Invasion: Reconsidering the Us Bombing Survey's Early-surrender Conclusions." Journal of Strategic Studies 18, no. 2 (1995): 101-48. Pape, Robert A. "Why Japan Surrendered." International Security 18, no. 2 (1993): 154-201.
"1945: Japan Signs Unconditional Surrender." BBC. September 2, 1945. Accessed May 21, 2015. news.bbc.co.uk/onthisday/hi/dates/stories/september/2/newsid_3582000/3582545.stm.

[165] "Ivy Mike, 1 November 1952 - First Full-Scale Thermonuclear Test." 1 November 1952. Accessed January 27, 2015. http://www.ctbto.org/specials/testing-times/1-november-1952-ivy-mike/.
"The 6555th's Role in the Development of Ballistic Missiles." Federation of American Scientists. Accessed January 27, 2015. http://fas.org/spp/military/program/6555th/6555c3-5.htm.

[166] It is possible to view the demise of the Soviet Union as an indirect consequence of the creation and development of thermonuclear weapons because the U.S.S.R. was willing to spend itself into ground rather than test the proposition of thermonuclear war.

Revolutionary Technological Characteristics

There are two revolutionary characteristics of nuclear weapons that contribute to its ability to be a strategic deterrent. The first is the sheer destructiveness of a single weapon's use and the second is the assuredness of that destruction as a result of the delivery revolution. As noted in the introduction, the Department of Defense defines deterrence as, "The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[167] Both characteristics are essential for nuclear weapons to be a deterrent under this definition. The demonstrated destructiveness of nuclear weapons, first in war and then through testing, gives the U.S. the ability to issue threats that are both credible and unacceptable in a previously impossible timeframe. While it is hypothetically possible to kill every human in the world with other weapons, nuclear weapons actually make it feasible. Thomas Schelling, a famous American economist, observes that the U.S. military at the end of the Second World War had "enough 30 caliber bullets to kill the whole population of the planet," but that nuclear bombs are the only weapons where the "pain of extinction" is credible.[168] As Dr. Drell notes, these were the first weapons that truly "threatened the survival of the human race."[169]

However, the destructiveness alone is not enough to ensure that nuclear weapons are a credible strategic deterrent. The delivery revolution was necessary to enhance the credibility of the threat of nuclear weapons virtually to the point of beyond question, which is a feat that no other weapons system has ever accomplished. As Schelling notes, "Nuclear weapons can change

[167] "Deterrence." Department of Defense Dictionary of Military Terms. Accessed April 29, 2015.
[168] Morbidly, he also notes that it would not be much of a strain on the American economy to perform a similar feat with ice picks.
Schelling, Thomas C. "The Diplomacy of Violence." In *Arms and Influence*, 19, 23. New Haven: Yale University Press, 1966.
[169] Drell, Sidney. Interview by author. March 5, 2015.

the speed of events, the control of events, the sequence of events, the relation of victor to vanquished, and the relation of homeland to fighting front."[170] While the invention of aircraft enabled adversaries to 'leapfrog' armies to directly attack civilian populations, the victim could still mount an effective defense or preemptive offense. Since the Captain William Robinson shot down a Zeppelin on September 3rd, 1915, victims have been able to protect themselves from strategic bombing raids by shooting down in the air or destroying on the ground the delivery systems carrying bombs.[171] When the delivery revolution matured, it was not possible to do the same for nuclear weapons.

Destructiveness

While it is widely known that nuclear weapons are highly destructive, few people truly understand the full extent.[172] Before nuclear weapons, there has never been a single device been able to cause as much devastation in so short a time and that destruction dramatically increased over the course of the Cold War. The 15-kiloton nuclear bomb dropped on Hiroshima was 2000 times more destructive than the British 'Grand Slam,' which was the largest conventional explosive of World War Two.[173] The largest U.S. fission weapon, MK-18, had a yield of 500

[170] Schelling, Thomas C. "The Diplomacy of Violence."
[171] "World War I: How the German Zeppelin Wrought Terror." BBC News. August 3, 2014. Accessed January 27, 2015. http://www.bbc.com/news/uk-england-27517166.
[172] This initially included Dwight Einsenhower when he was a general. One of Brodie's earliest statements in *The Absolute Weapon* is, "The power of the present bomb is such that any city in the world can be effectively destroyed by one to ten bombs." In General Eisenhower's copy of the text, there are four frantic questions marks next to this statement.
Brodie, Bernard, and Frederick Sherwood Dunn. *The Absolute Weapon: Atomic Power and World Order*.
[173] The Nagasaki nuclear weapon had a yield of 21 kilotons.
Truman, Harry. "Announcing the Bombing of Hiroshima: Statement by the President of the United States." PBS. August 6, 1945. Accessed January 27, 2015. http://www.pbs.org/wgbh/americanexperience/features/primary-resources/truman-hiroshima/.
Malik, John. "The Yields of the Hiroshima and Nagasaki Explosions."
"The Atomic Bombings of Hiroshima and Nagasaki: Total Casualties." The Atomic Archive. Accessed January 27, 2015. http://www.atomicarchive.com/Docs/MED/med_chp10.shtml.

kilotons.[174] The first American thermonuclear, or fusion, device had a yield of 10.4 megatons, roughly 700 times more destructive than the device dropped on Hiroshima.[175] A fully stocked Ohio-class submarine today is capable of delivering more explosive power in a few hours than all of the gunpowder that has been used in all of the history of combat to date.[176] To put this power in layman's terms, the Air University primer on nuclear weapons compares a nuclear detonation to various forces in nature,

> "Air blast… winds are ten times stronger than those found in the most powerful hurricane… The ground shock is nearly 250 times worse than the greatest earthquake. The lateral accelerations are transmitted over large distances at very high speeds… The temperatures in the fireball reach upwards of 14,000 degrees Fahrenheit. As a comparison, the sun's surface temperature is approximately 11,000 degrees."[177]

The U.S. Department of Health and Human Services provides a more empirical definition. It divides the destruction of a nuclear detonation into the following categories: 50 percent blast, 35 percent thermal, 15 percent ionizing radiation (5 percent initial, 10 percent delayed).[178] All of this is to demonstrate how unique the destructive of nuclear weapons has been up to the present.

The destructiveness of a single nuclear weapon is a critical to it being a strategic deterrent. Unlike any other weapon, it is possible with nuclear weapons to prevent a strategic-level action of an adversary by threatening to credibly impose unacceptable costs. The U.S. demonstrated to its adversaries the destructive power of fission bombs at Hiroshima and

---

[174] "Complete List of All U.S. Nuclear Weapons." Nuclear Weapons Archive. October 14, 2006. Accessed January 27, 2015. http://nuclearweaponarchive.org/Usa/Weapons/Allbombs.html.
[175] "Ivy Mike, 1 November 1952 - First Full-Scale Thermonuclear Test."
[176] Bencivenga, Jim. "Aboard a Nuclear Sub." The Christian Science Monitor. October 14, 1982. Accessed May 15, 2015. http://www.csmonitor.com/1982/1014/101430.html.
"Ohio Class." National Cold War Exhibition. Accessed May 15, 2015. http://www.nationalcoldwarexhibition.org/research/collections/ohio-class/.
[177] "Chapter 17: U.S. Missile Systems." Air University. Accessed January 20, 2015. http://www.au.af.mil/au/awc/space/primer/us_missile_systems.pdf. 17-6.
[178] "Nuclear Detonation: Weapons, Improvised Nuclear Devices." U.S. Department of Health and Human Services: Radiation Emergency Medical Management. Accessed January 27, 2015. http://www.remm.nlm.gov/nuclearexplosion.htm.

Nagasaki and that of fusion bombs in multiple tests during the Cold War. It is impossible to prevent their at least partially successful use because as people from Bernard Brodie to Robert Gates state there is no such thing as "a perfect defense."[179] In the very earliest part of the nuclear era, the ability of the few fission devices to deter the conventional aggression of the Soviet Union was very much in question. However, as the U.S. grew the size of its nuclear arsenal and developed increasingly destructive weapons, those questions faded. Consequently, after the successful testing of thermonuclear weapons in the mid-1950s, it was not the destructiveness that caused people to doubt the strategic deterrent capability of nuclear weapons, but the assurance of their delivery.

Assurance of Destruction: The Delivery Revolution

The delivery revolution was already partially in motion before the advent of nuclear weapons. By the end of the Second World War, the Allies and the Axis powers had already developed long-range bombers, quiet submarines, and ballistic missiles that would form the basis of what would become known as the nuclear triad. The need to protect and ensure the delivery of nuclear weapons drove the effort to build faster, more accurate, and more secure versions of the World War Two-era delivery systems. The U.S. Air Force, which became its own service in 1947, built off of the World War Two B-29 platform to develop a series of strategic bombers (including the B-47, B-50, and B-52) that firmly established American credibility to deliver its nuclear weapons anywhere in the globe.[180] Later iterations of the strategic bomber, such as the F-117 and the B-2, developed stealth technology to avoid detection by anti-aircraft systems.[181]

---

[179] Brodie, Bernard. "Is There Defense?" In Strategy in the Missile Age, 185. Princeton, N.J.: Princeton University Press, 1959.
Gates, Robert. Interview by author. March 23, 2015
[180] "Strategic Airpower: The History of Bombers." Boeing. Accessed May 21, 2015. http://www.boeing.com/bds/strategicairpower/.
[181] "Strategic Airpower: The History of Bombers." Boeing.

Following the Second World War, the U.S. also developed a series of missiles, initially guided by the Nazi's V-1 and V-2 short-range ballistic missiles. By the late 1950s, the U.S. had developed a series of liquid-fuelled inter-regional and inter-continental ballistic missiles (the Atlas, Thor, and Jupiter programs) and by the mid-1960s it largely transitioned to solid-fuelled missiles (the Minuteman, Titan, and Peacekeeper programs).[182] The U.S. also invested in hardening siloes and the dispersing weapons across the country.[183] To complete the triad, the U.S. developed the nuclear-powered submarine and a series of submarine-launched ballistic missiles (Polaris, Poseidon, and Trident).[184] The combination of these technological advances in early and mid-1960s resulted in the U.S. and the U.S.S.R. attaining secure second-strike capability, which was a powerful stabilizing force for deterrence.[185]

The delivery revolution was the crucial complementary technological reason that made nuclear deterrence possible. While the destructiveness of the nuclear weapon was beyond question, its delivery was not. In the early days of the nuclear era, there were several key questions that led to instability in strategic deterrence. Could the U.S. deliver nuclear weapons to the targets? Could the Soviet Union destroy all or most of America's nuclear weapons in a first strike? Could the Soviet Union defend against the delivery systems of nuclear weapons? The

---

[182] "Chapter 17: U.S. Missile Systems." Air University.
"Ballistic Missiles." Federation of American Scientists. Accessed January 21, 2015. http://www.fas.org/spp/military/program/smc_hist/SMCHOV8.HTM.
Gibson, Jane, and Kenneth Kemmerly. "Intercontinental Ballistic Missiles." Air University. Accessed January 27, 2015. http://www.au.af.mil/au/awc/space/au-18-2009/au-18_chap18.pdf.
"Profile for United States." NTI: Nuclear Threat Initiative. Accessed January 27, 2015. http://www.nti.org/country-profiles/united-states/delivery-systems/.
[183] Neufield, Jacob. "The Development of Ballistic Missiles in the United States Air Force 1945-1960." Office of Air Force History. January 1, 1990. Accessed January 28, 2015. http://www.afhso.af.mil/shared/media/document/AFD-100924-024.pdf.
[184] "Submarine Launched Ballistic Missiles: United States Nuclear Forces Guide." Federation of American Scientists. Accessed May 21, 2015. http://fas.org:8080/nuke/guide/usa/slbm/index.html."
Polaris A1 - United States Nuclear Forces." Federation of American Scientists. Accessed January 28, 2015. http://www.fas.org/nuke/guide/usa/slbm/a-1.htm.
[185] "Polaris A1 - United States Nuclear Forces." Federation of American Scientists.
Neufield, Jacob. "The Development of Ballistic Missiles in the United States Air Force 1945-1960."

earliest bombers took hours to reach their destination (and were not guaranteed to make the entire distance), could be destroyed on the runway, and could be shot down by anti-aircraft weapons and interceptor aircraft. Although some of the bombers would likely get through, there was significant debate over whether they were capable of delivering enough of their nuclear payloads to inflict truly unacceptable costs on the adversary and if it were possible to 'survive' or 'win' a nuclear exchange. The saliency of these questions fluctuated with advances in technology and frequently drove the direction of research. With the advent of technology such intercontinental ballistic missiles equipped with multiple independently targetable reentry vehicles and the B-2 stealth bomber, the questions of ability to deliver nuclear payloads to the target and defense against nuclear weapons became less relevant. The advent of the nuclear powered submarine armed with accurate submarine launched ballistic missiles in the mid-1960s largely brought an end to the first-strike question. These submarines were capable of avoiding detection by satellites and (with their quiet systems) by ships and other submarines, making them very difficult to destroy. As the technology of the delivery revolution matured, the doubts over the credibility and stability of strategic deterrence largely faded.

The Bifurcated Debate

The revolutionary technology of nuclear weapons sent geopolitical shock waves around the globe. World leaders were almost immediately cognizant of the potential implications of this new weapon.[186] However, it took some time to come to a consensus on what those implications

[186] President Harry Truman, after the detonation of the bomb said in his address to the nation that the atomic bomb represented a "revolutionary increase in destruction to supplement the growing power of our armed forces." George Kennan, then U.S, Ambassador to the Soviet Union, reported that General Secretary Joseph Stalin said that the bomb "would mean the end of war and aggressors."
Truman, Harry. "Announcing the Bombing of Hiroshima: Statement by the President of the United States." PBS. August 6, 1945. Accessed January 27, 2015. http://www.pbs.org/wgbh/americanexperience/features/primary-resources/truman-hiroshima/.
Kennan, George F. "Far Eastern War and General Situation." George Washington University. August 8, 1945. Accessed January 27, 2015. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB162/57.pdf.

were and the outcome of strategic deterrence was by no means inevitable at the dawn on the nuclear age. The technology sparked a vigorous bifurcated debate that had a critical impact on the strategy and development of nuclear weapons. Thomas Schelling, one of the preeminent participants of the debate, "I give RAND almost complete credit for that turnaround [of stabilizing deterrence]."[187] On the one side, a number of strategists, generals, and policymakers believed that nuclear weapons should only have a limited effect on doctrine and that future strategy should be developed on the same basis as previous weapons systems. The group supported preventative and preemptive strikes, as well as defense against nuclear weapons. It was also skeptical of the theory of deterrence. This group can be thought as the 'continuity' movement because it borrows the majority of its thinking from previous military strategy. On the other side, another group of leaders and thinkers thought that the introduction of nuclear weapons demanded a major shift in policy. It opposed the destabilizing ideology of first strikes and defense against nuclear weapons and supported efforts to reinforce deterrence, such as arms control. This group can be referred to as 'change' movement because it argued that the technology of nuclear weapons necessitated fundamentally different strategy and thinking than before. The debate between these two movements raged throughout the duration of the nuclear revolution. At its core, the debate represents a tension between those who believe that a new technology cannot disrupt history's rhythms a new technology and those who believe that it can.

First Strike and Preventative War

William Liscum Borden, a World War Two army veteran and later the executive director of the Joint Committee on Atomic Energy, is one of the ideological wellheads of the continuity

[187] Schelling, Thomas. Interview by author. February 16, 2015.

movement and strong proponent of the U.S. nuclear first strike.[188] In his 1946 book *There Will Be No Time: A Revolution in Strategy*, Borden decries the "fallacy of the mutual-deterrent thesis."[189] He argues that war is an inevitable part of the human condition and that nuclear weapons will be used, primarily on military targets.[190] Henry Margenau, a physicist, notes that Borden "regards the atomic bomb primarily as a *tactical*, not a *strategic* weapon [emphasis in the original]."[191] However, despite Borden's belief that the U.S. needed to prepare for and then execute a first strike against the Soviet Union, he lamented that it would not happen because "the American people would never strike first."[192] This led Richard Rhodes, an American historian, to observe that Borden at once believes that atomic war will begin with a "rocket Pearl Harbor" and that the threat will only dissipate when American long-term strength forces the Soviet Union to develop into a "more liberal regime."[193] Ethan Heilman, a reviewer, writes that the means rather than the ends of Borden's argument are what set his logic apart from his counterpart Bernard Brodie's pro-deterrence reasoning in *The Absolute Weapon*.[194]

Borden's first strike found sympathetic ears in the military establishment. According to George Quester, another historian, General Curtis LeMay (who was commander of Strategic Air Command and later Chief of Staff of the U.S. Air Force) "saw it as urgent to attack the Soviet Air force before it could attack his own SAC [Strategic Air Command]" and "repeatedly toyed

---

[188] Rhodes, Richard. "This Buck Rogers Universe." In *Dark Sun the Making of the Hydrogen Bomb*, 357-358. New York: Simon & Schuster, 1995.
[189] Borden, William Liscum. "The Certainty of War Amidst Anarchy." In *There Will Be No Time: The Revolution in Strategy*, 24-32. New York: Macmillan Company, 1946.
[190] Borden, William Liscum. "The Certainty of War Amidst Anarchy."
[191] Margenau, Henry. "Reviews." *The Yale Law Journal* 56 (1947): 753-55. Accessed January 22, 2015. http://www.jstor.org/stable/793331?seq=1#page_scan_tab_contents.
In Borden's words, "The tactical issues transcend the strategical."
Borden, William Liscum. "The Pattern of Atomic Warfare."
[192] Borden, William Liscum. "The Certainty of War Amidst Anarchy."
[193] Rhodes, Richard. "This Buck Rogers Universe."
[194] Heilman, Ethan. "A Review of William Liscum Borden's 'There Will Be No Time: The Revolution in Strategy'." Accessed January 27, 2015. http://ethanheilman.tumblr.com/post/29405762446/there-will-be-no-time-a-review.

with the idea of preemptive attack, or even preventative war."[195] (Schelling quipped in his interview, "RAND never succeeded in persuading the Strategic Air Command of anything."[196]) Lemay was not alone. The *Montgomery Advertizer* recorded on September 1, 1950 Major General Orville A. Anderson, the commandant of the Air War College, saying,

> "Give me the order to do it and I can break up Russia's five A-bomb nests in a week! And when I went up to Christ, I think I could explain to him that I saved civilization."[197]

Similarly, Navy Secretary Francis Matthews suggested in a public speech on August 25, 1950 that the U.S. launch a preventative strike "to compel cooperation for peace" making the U.S. "the first aggressor for peace [in history]."[198] While the U.S. government censured both Anderson and Matthews, their views were indicative of the power of the first strike argument at the highest levels of government.

Indeed, while President Harry Truman strongly resisted the idea of preventative war, President Dwight Eisenhower did not rule out the possibility. Given that the cost of an arms race could eventually lead to war or have negative effects on American democracy, Eisenhower stated "we would be forced to consider whether our duty to future generations did not require us to

---

[195] Quester, George H. "Outright Advocates." In *Nuclear Monopoly*, 49. New Brunswick: Transaction Publishers, 2000.

[196] Schelling, Thomas. Interview by author. February 16, 2015.

[197] Willbanks, James H. "Notes." In *Generals of the Army Marshall, MacArthur, Eisenhower, Arnold, Bradley.*, 230. University Press of Kentucky, 2013.
Schaffer, Ronald. "Epilogue." In *Wings of Judgment: American Bombing in World War II*, 202. Oxford; New York: Oxford University Press, 1985.
"The US government promptly repudiated both Matthew's and Anderson's statements and the Pentagon removed Anderson."
Alexander, Bevin. "The Korean War." In *The Strange Connection: U.S. Intervention in China, 1944-1972*, 108-109. New York: Greenwood Press, 1992.

[198] Schaffer, Ronald. "Epilogue." In *Wings of Judgment: American Bombing in World War II*, 202. Oxford; New York: Oxford University Press, 1985.
Abella, Alex. "The Wages of Sin." In *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*, 43. Boston: Mariner Books, 2009.

initiate a war at the most propitious moment we could designate."[199] However, a few months later the Eisenhower administration declared in NSC 5440, "the United States and its allies must reject the concept of preventive war or acts intended to provoke war."[200] Nevertheless, Eisenhower still argued that nuclear weapons had military utility. In March 1955, he announced at a press conference, "Where these things are used on strictly military targets and for strictly military purposes, I see no reason why they shouldn't be used just exactly as you would use a bullet or anything else."[201]

Bernard Brodie, a historian and a military strategist commonly known as "the American Clausewitz," was a foundational thinker for the change movement and for U.S. nuclear deterrence policy in its earliest stages.[202] One of his most famous works, *The Absolute Weapon* demonstrated that nuclear weapons were fundamentally different than other types of weapons, that mutual deterrence was only possible with the Soviet Union (which the book forecasted would happen in five to ten years), and it laid out the requirements for a form of deterrence that needed to be successful.[203] In the essay, he evaluates the case for nuclear first strike and finds it wanting. He considers one of the wished-for "total solutions" along with pre-emptive war and massive retaliation.[204] Brodie argues that nuclear preventative war is only feasible if it is

---

[199] Schaffer, Ronald. "Epilogue."
[200] Silverstone, Scott A. "Eisenhower and the Growth of Soviet and Chinese Power 1953-1955." In *Preventive War and American Democracy*. 101. New York: Routledge, 2007.
[201] Hilsman, Roger. "New Look, Massive Retaliation, and Flexible Response." In *From Nuclear Military Strategy to a World without War: A History and a Proposal*, 33. Westport, Conn.: Praeger, 1999.
[202] "Announcing Publication of State of Doom: Bernard Brodie, the Bomb and the Birth of the Bipolar World." Program for Culture and Conflict Studies at NPS. Accessed November 12, 2014. http://www.nps.edu/Programs/CCS/WebJournal/Article.aspx?ArticleID=107.
[203] Brodie's essay also predicted the need for arms control, second-strike capability, extended deterrence, the nature of what would become the Cold War, and even the potential for nuclear terrorism
"Announcing Publication of State of Doom: Bernard Brodie, the Bomb and the Birth of the Bipolar World."
Brodie, Bernard, and Frederick Sherwood Dunn. *The Absolute Weapon: Atomic Power and World Order*.
[204] Brodie, Bernard. "The Wish for Total Solutions: Preventative War, Pre-Emptive Attack, and Massive Retaliation." In Strategy in the Missile Age, 223.

"decisive" and "inevitable."[205] However, given that "the physical circumstances" that would make a first strike appealing are unlikely to occur, he suggests that the probability of the U.S. launching such a war is "very low."[206] Cognizant of the military's view of the issue, Brodie contends that civilian control over nuclear weapons is problematic because those in charge may not be "statesmen" and may not think about "strategic questions" during peacetime, meaning that they are "dependent upon and somewhat overshadowed by the military."[207] Brodie believes that although civilians have nominal control over the nuclear arsenal, their decisions actually reflect "a kind of forfeiture or abandonment of values other than military at high decision-making levels."[208]

These debates had an important impact on policy. The U.S. came close to considering launching a preventative strike against the Soviet Union. Ultimately, the debate over first strike capability drove both technological efforts to develop first-strike capable delivery systems (such as the Pershing II IRBM and the LGM-118 Peacekeeper ICBM) and support counter-measure efforts such as the hardening of silos and the construction of nuclear submarines capable of launching ballistic missiles.[209] These technological changes fed back into the debate and largely resolved it in combination with arms control agreements that limited first strike capabilities by making a successful first strike not feasible.

Defense and Survivability

The continuity group's type of thinking led many to commit to the idea of rebalancing the offense-defense equilibrium and led to a long-running debate over whether the U.S. could defend

[205] Brodie, Bernard. 229.
[206] Brodie, Bernard. 232.
[207] Brodie, Bernard. 267.
[208] Brodie, Bernard. 268.
[209] "Pershing II Weapon System (System Description)." United States Army. 1986. Accessed May 21, 2015. http://www.scribd.com/doc/64061132/TM-9-1425-386-10-1.
"The Peacekeeper (MX) ICBM." Nuclear Weapon Archive. October 10, 1997. Accessed May 21, 2015. http://nuclearweaponarchive.org/Usa/Weapons/Mx.html.

itself against nuclear weapons.[210] U.S. presidents since Eisenhower have had varying enthusiasm for defense against nuclear-armed long-range bombers and missiles, although despite the technical difficulties associated with it none have given up on the concept.[211] The power of the defense camp reached its apex in 1983 when President Ronald Reagan introduced the Strategic Defense Initiative as a comprehensive continental defense system against nuclear weapons.[212] Reagan hoped to change U.S. defense from mutually assured destruction to prevailing in a nuclear war through sufficient defense and first strike means.[213] Ultimately, the program became publicly discredited after the American Physics Society announced that such defense program would be impossible.[214]

In another one of his great works called *Strategy in the Missile Age*, Brodie examines the issues of the possibility of defending against thermonuclear weapons, among other topics. He largely dismisses the idea that the U.S. could meaningfully defend its civilian population at the time due to issues with warning systems, shelters, and other complicating factors. Brodie suggests that the fallout alone would make it "impossible to set upper limits [on the death toll] appreciably short of the entire population of the nation," but encourages further research into the subject.[215] Brodie is more optimistic about America's ability to protect its nuclear arsenal and believes that it is essential for deterrence. He states, "*Known ability to defend our retaliatory*

---

[210] Baucom, Donald R. "Origins of the Strategic Defense Initiative: Ballistic Missile Defense, 1944-1983." Strategic Defense Initiative Organization. December 1, 1989. Accessed January 20, 2015. http://www.dtic.mil/dtic/tr/fulltext/u2/a242465.pdf.
[211] Bright, Christopher J. "The Origins of Nuclear Air Defense Arms." In *Continental Defense in the Eisenhower Era: Nuclear Antiaircraft Arms and the Cold War*. 22. New York: Palgrave Macmillan, 2010.
[212] Reiss, Edward. "Contexts and Conditions." In *The Strategic Defense Initiative*. 176. Cambridge England: Cambridge University Press, 1992.
[213] Freedman, Lawrence D. "Nuclear Strategy: Alternatives to Assured Destruction." Encyclopedia Britannica Online. Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/421797/nuclear-strategy/52990/Alternatives-to-assured-destruction.
[214] Hertsgaard, Mark. "Star Wars Works!" Salon. Accessed May 21, 2015. http://web.archive.org/web/20010913001732/http://www.salon.com/news/news960607.html.
[215] Brodie, Bernard. "The Advent of Nuclear Weapons." In Strategy in the Missile Age, 167.

force constitutes the only unilaterally attainable situation that provides potentially a perfect defense of our homeland [emphasis in original]."[216]

The 1957 Presidential Science Advisory Committee report entitled "Deterrence & Survival in the Nuclear Age," better known as the Gaither Report, supported Brodie's thinking.[217] Following a recommendation from the Federal Civil Defense Agency (FCDA) to invest $32 billion a shelter program for civilians, President Eisenhower to H. Rowan Gaither, Jr. for guidance. Eisenhower tasked Gaither, a lawyer affiliated with the RAND Corporation, to lead an investigation into the "various active and passive measures to protect the civil population in case of nuclear attack and its aftermath."[218] Although Eisenhower charged the committee with examining the utility of civil defense measures, the report came out strongly against them and warned against complacency. The report claims both that "Active defense programs now in being and programmed for the future will not give adequate assurance of protection" and "Passive defense programs… will afford no significant protection to the civil population."[219] Instead, it claims, "The protection of the United States and its population rests, therefore, primarily upon deterrence provided by SAC."[220] The report then recommends improving the U.S. nuclear deterrent, as well as active and passive defenses with "a $44 billion program."[221] It concludes with an urgent tone, "The next two years seem to us critical. If we fail to act at once,

[216] Brodie, Bernard. "Is there Defense?" 185.
[217] "Deterrence & Survival in the Nuclear Age." Security Resources Panel of the Science Advisory Committee. November 7, 1957. Accessed November 12, 2014. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB139/nitze02.pdf.
[218] Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role." *Diplomatic History* 25, no. 1, 154.
[219] "Deterrence & Survival in the Nuclear Age." Security Resources Panel of the Science Advisory Committee.
[220] "Deterrence & Survival in the Nuclear Age."
[221] "Deterrence & Survival in the Nuclear Age."
Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role." *Diplomatic History* 25, no. 1, 153.

the risk, in our opinion, will be unacceptable."[222] The committee published the report not long after the *Sputnik* launch and, according author David L. Snead, "significantly influenced Eisenhower's national security policies for the remainder of his presidency."[223]

Others were less convinced that it would not be possible to survive a nuclear exchange with the Soviet Union, giving credence the idea that an effective (if not perfect) defense was possible. Herman Kahn, an American physicist and strategist at the RAND Corporation and the Hudson Institute, explores the "feasibility" of thermonuclear war in *The Nature and Feasibility of War and Deterrence*.[224] He examines the issue with in depth discussions of "genetic problems," "postwar medical problems," and "long-term recuperation."[225] For Kahn, although the outcomes of such a war would be serious they would not "jeopardize" the future of the human race.[226] As part of his study of survivability, Kahn also examines how the U.S. could win a nuclear war. He argues that there are three types of deterrence.[227] When evaluating the first type of deterrence, Kahn believes that it is much more important to think in terms of post-strike

---

[222] Adding to the alarmist tone, the report estimates that the Soviet economic growth was quickly reducing the gap between the two state sand that military spending "may be double" that of the U.S. in the 1960s if U.S. military spending remained constant.
"Deterrence & Survival in the Nuclear Age."
Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role." *Diplomatic History* 25, no. 1, 155-156.
"Appendix A: After the Fall." Federation of American Scientists. Accessed November 12, 2014. http://fas.org/sgp/library/moynihan/appa9.html.

[223] Snead authored the leading book on the topic.
Snead, David L. *The Gaither Committee, Eisenhower, and the Cold War*. Columbus: Ohio State University Press, 1999. 3.

[224] "Herman Kahn (American Futurist)." Encyclopedia Britannica Online. Accessed November 12, 2014. http://www.britannica.com/EBchecked/topic/309688/Herman-Kahn.
Kahn, Herman. "The Nature of Feasibility of War and Deterrence." The RAND Corporation. January 20, 1960. Accessed November 12, 2014. http://www.rand.org/content/dam/rand/pubs/papers/2005/P1888.pdf. 4.

[225] Kahn, Herman. "The Nature of Feasibility of War and Deterrence." 5.

[226] Kahn, Herman

[227] Type 1: "deterrence against a direct attack." Type 2: "the use of strategic threats to deter an enemy from engaging in very provocative acts other than a direct attack on the United States." Type 3: "acts that are deterred because the potential aggressor is afraid that the defender or others will take limited actions, military or nonmilitary, to make the aggression unprofitable."
Kahn, Herman 18.

capabilities of retaliatory forces instead of "the preattack inventory."[228] Kahn then poses a number of hypothetical situations testing Type 1 deterrence and concludes that the best way to understand the condition of a country's Type 1 deterrence is "by asking how much strain it could accept and still be depended on."[229] Type 2 involves the possibility that the U.S. could "obtain the first strategic strike or some temporizing move, such as evacuation."[230] Type 3 at its best would "be the capability to fight a limited war of some sort."[231] Kahn concludes that even with "the highest-quality Type 1 Deterrence capability, we must still be able to fight and survive wars as long as it is possible to have such a capability."[232] Kahn's thinking, while different from many of his peers (by his own admission), proved essential in encouraging the development of secure second strike capability such as submarine launched ballistic missiles.

Albert Wohlstetter, another key RAND Corporation strategist, also advocated for increased investment in deterrence-reinforcing systems. Wohlstetter frames "the apparent vulnerability of the US ability to retaliate" as "a delicate balance of terror" in his seminal 1957 work *The Delicate Balance of Terror*.[233] Wohlstetter asserts, "*strategic deterrence, while feasible, will be extremely difficult to achieve, and at critical junctures in the 1960's we may not have the power to deter attack* [emphasis in original]."[234] Wohlstetter then lists a number of "hurdles" that the U.S. government will have to "jump" in order to maintain its strategic deterrence ranging from the survivability of offensive weapons to overcoming Soviet

---

[228] Kahn, Herman 19.
[229] Kahn, Herman 31.
[230] Kahn, Herman 33.
[231] Kahn, Herman 34.
[232] Kahn, Herman 39.
[233] Ayson, Robert. *Thomas Schelling and the Nuclear Age: Strategy as Social Science*. New York: Routledge, 2004. 56-58.
The term "balance of terror" was likely coined by Lester Pearson in June 1955 at the 10th anniversary of the signing of the UN Charter, when he stated, "the balance of terror has replaced the balance of power." "Balance of Terror." In *The Norton Dictionary of Modern Thought*, 65. 3rd ed. Great Britain: W. W. Norton & Company, 1999.
[234] Wohlstetter, Albert. "The Delicate Balance of Terror." The RAND Corporation. November 6, 1958. Accessed November 12, 2014. http://www.rand.org/about/history/wohlstetter/P1472/P1472.html.

defenses.[235] Beyond strategic deterrence, Wohlstetter also states that nuclear deterrence alone is inadequate and that the only way to "retort to peripheral provocations" is to develop "the power to meet limited aggressions."[236] Wohlstetter's ideas were influential enough in the general discourse for President John F. Kennedy to use his term, the "balance of terror" in his 1961 inaugural address.[237] However, Wohlstetter's attempt to prevent the nation from returning to its "deep pre-Sputnik sleep" also left his argument open to criticism of fear mongering.[238] Robert Ayson, a professor of strategic studies at the Victoria University of Wellington, describes Wohlstetter's as one of "the cruder conceptions of the stability of the 'balance of terror.'"[239]

The debate over survivability and defense, like that over first strike, had great significance of U.S. policy and the technological development of its nuclear forces. America spent substantial sums on various defense systems such as SDI and civil defense plans to evacuate and shelter the U.S. population. These projects drew criticism not only from proponents of deterrence who saw them as destabilizing, but also groups such as the Catholic Worker Movement, which believed that civil defense exercises misled Americans into believing that they could survive a nuclear attack.[240] The stabilization of deterrence, due to both the U.S. and the U.S.S.R. attaining secure second strike ability and the maturation of the debate, over time led these debates to move towards the fringe.

Strategic Deterrence

---

[235] Wohlstetter, Albert.
[236] Wohlstetter, Albert.
[237] "But neither can two great and powerful groups of nations take comfort from our present course--both sides overburdened by the cost of modern weapons, both rightly alarmed by the steady spread of the deadly atom, yet both racing to alter that uncertain balance of terror that stays the hand of mankind's final war." Kennedy, John Fitzgerald. "Inaugural Address." The American Presidency Project. January 20, 1961. Accessed November 12, 2014. http://www.presidency.ucsb.edu/ws/?pid=8032.
[238] Wohlstetter, Albert. "The Delicate Balance of Terror." The RAND Corporation. November 6, 1958. Accessed November 12, 2014. http://www.rand.org/about/history/wohlstetter/P1472/P1472.html.
[239] Ayson, Robert. *Thomas Schelling and the Nuclear Age: Strategy as Social Science*.
[240] Allaire, James, and Rosemary Broughton. "Catholic Worker Movement: Dorothy Day." Catholic Worker Movement. Accessed May 21, 2015. http://www.catholicworker.org/dorothyday/ddbiographytext.cfm?Number=3.

Strategic deterrence was a new, non-intuitive way of thinking about nuclear weapons and the U.S. government needed time to get accustomed to the idea because it was such dramatic change from the past. As Frederick Dunn, director of Yale Institute for International Studies and author of the introduction to *The Absolute Weapon*, states nuclear weapons "altered the basic nature of war itself."[241] In the second chapter, Brodie asks, "Is it worth-while to even consider military policy as having any consequence at all in the age of atomic bombs?"[242] Under Brodie's worldview, indicative of the larger message of the change movement, nuclear weapons have the potential to make all non-nuclear forms of warfare obsolete after centuries of strategy based on conventional forces. Brodie's response to this conundrum is deterrence, "If the aggressor state must fear retaliation, it will know that even if it is the victor it will suffer a degree of physical destruction incomparably greater than that suffered by any defeated nation of history… Under those circumstances no victory… would be worth the price."[243] Understanding that he is challenging a fundamental notion that if a nation has advanced weapon, it should use it, he famously states, "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose."[244] While Brodie overstated the matter, as the stability-instability paradox left plenty for conventional forces to do, he captured the essence of the debate.

NSC-68 is a 1950 National Security Council paper that examined what it would take to implement the change movement's concepts of deterrence.[245] As Alexander George and Richard Smoke note in *Deterrence in American Foreign Policy: Theory and Practice*, "Prior to NSC-68

[241] Brodie, Bernard, and Frederick Sherwood Dunn. *The Absolute Weapon: Atomic Power and World Order*.. 2.
[242] Brodie, Bernard, and Frederick Sherwood Dunn. 58.
[243] Brodie, Bernard, and Frederick Sherwood Dunn. 60.
[244] Brodie, Bernard, and Frederick Sherwood Dunn. 62.
[245] Nitze, Paul H. *NSC-68 Forging the Strategy of Containment*. Washington, DC: National Defense University, 1994. 2.

there was very little analysis of the requirements of strategic deterrence, nor the problems of applying deterrence to complicated real crises and small conflicts of the emerging Cold War."[246] At a time when President Truman, responding to immense public pressure to reduce the defense budget, promised defense cuts of "between $5 and $7 billion."[247] NSC-68 called for tripling the defense budget to meet the defense needs of the U.S.[248] The report responded to the "probable fission bomb capability" of the U.S.S.R. by advocating second-strike capability, the rollback of Soviet influence, and the restoration of U.S. military forces.

> "In particular, the United States now faces the contingency that within the next four or five years the Soviet Union will possess the military capability of delivering a surprise atomic attack of such weight that the United States must have substantially increased general air, ground, and sea strength, atomic capabilities, and air and civilian defenses to deter war and to provide reasonable assurance, in the event of war, that it could survive the initial blow and go on to the eventual attainment of its objectives."[249]

After NSC-68, the 1953 NSC-162/2 was the next major document to embody the change movement's support of strategic deterrence.[250] The document argued that the U.S. needed to "develop and maintain" its nuclear arsenal and military, economy, intelligence gathering capabilities, and its scientific research.[251] The document's most famous recommendation to the President is the need to have "A strong military posture, with emphasis on the capability of

---

[246] George, Alexander L., and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press, 1974. 38.
[247] George, Alexander L., and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*.
[248] Nitze, Paul H. *NSC-68 Forging the Strategy of Containment*. Washington, DC: National Defense University, 1994. 3.
[249] The document also advocates that the U.S. should "reduce the power and influence of the USSR to limits which no longer constitute a threat to the peace, national independence, and stability of the world family of nations." As well as "It is imperative that this trend be reversed by a much more rapid and concerted build-up of the actual strength of both the United States and the other nations of the free world. The analysis shows that this will be costly and will involve significant domestic financial and economic adjustments."
"NSC 68: United States Objectives and Programs for National Security." Mtholyoke.edu. April 14, 1950. Accessed November 12, 2014. https://www.mtholyoke.edu/acad/intrel/nsc-68/nsc68-1.htm.
[250] "Eisenhower Approves NSC 162/2." History.com. Accessed November 12, 2014. http://www.history.com/this-day-in-history/eisenhower-approves-nsc-1622.
[251] "NSC162/2: A Report to the National Security Council on Basic National Security Policy." Federation of American Scientists. October 30, 1954. Accessed November 12, 2014. http://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf. 6-7.

inflicting massive retaliatory damage by offensive striking power."[252] NSC-162/2 stated that the U.S. "will consider nuclear weapons as available for use as other munitions," which is understood to mean that the U.S. would respond to a Soviet or Chinese attack on itself or an ally with nuclear weapons either in the theater or in the main territory of the U.S.S.R. or China.[253] NSC-162/2 justifies its recommendation for spending "at exorbitant cost" by noting that the U.S.S.R. "devotes one-sixth of its gross national product to military outlays" and "soon may have the capability of dealing a crippling blow to our industrial base and our continued ability to prosecute a war" with a "surprise attack."[254] NSC-162/2 was a cornerstone of President Eisenhower's New Look foreign policy. New Look addressed Soviet leaders intention to place what President Eisenhower referred to in a radio address on national security as "an unbearable security burden leading to economic disaster."[255] The Eisenhower administration contended that a defense supported by nuclear deterrence would give taxpayers "more bang for your buck."[256]

---

[252] Secretary of State John Foster Dulles more fully expounded this doctrine in his June 9, 1954 speech to the Council on Foreign Relations in which he stated, "Local defenses must be reinforced by the further deterrent of massive retaliatory power," comparing the doctrine to a "community security system" that protects houses in a neighborhood from robbery. The U.S. government quickly realized that while massive retaliation could save costs over the long-term, it was an inflexible doctrine that could have left the U.S. vulnerable to "less-than-total challenges" such as the suppression of uprisings in East Berlin and Hungary in 1953 and 1956 respectively and lowered U.S. credibility. It also made the U.S.S.R. feel more vulnerable and increased the chances that Moscow would feel the need to launch a pre-emptive strike.
"NSC162/2: A Report to the National Security Council on Basic National Security Policy." Federation of American Scientists. October 30, 1954. Accessed November 12, 2014. http://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf. 5.
Eisenhower, Dwight D. "The Strategy of Massive Retaliation." Freerepublic.com. January 12, 1954. Accessed November 14, 2014.
Gaddis, John Lewis. *Strategies of Containment a Critical Appraisal of American National Security Policy during the Cold War*. Rev. and Expanded ed. New York: Oxford University Press, 2005. 169.
"Massive Retaliation." Nuclearfiles.org/. Accessed November 12, 2014. http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/strategy-massive retaliation.htm.
[253] "NSC162/2: A Report to the National Security Council on Basic National Security Policy."
[254] NSC-162/2 also argues for the need to maintain "the collective defense of the free world" and protect allied countries that do not have the nuclear capabilities or the ability to support military forces sufficient to ensure the defense of their countries.
"NSC162/2: A Report to the National Security Council on Basic National Security Policy." 2, 8, 21.
[255] Eisenhower, Dwight D. "Dwight D. Eisenhower: Radio Address to the American People on the National Security and Its Costs." The American Presidency Project. May 19, 1953. Accessed November 12, 2014. http://www.presidency.ucsb.edu/ws/?pid=9854.
[256] Nojeim, Michael J., and David P. Kilroy. *Days of Decision Turning Points in U.S. Foreign Policy*. Washington, D.C.: Potomac Books, 2011. 79. 79

The 1955 'Killian Report' built off of these documents and played a major role in jumpstarting the ICBM program.[257] The Killian report is divided in to three phases – the then present, the near future, and the long-term future – and assesses the U.S. deterrent as a function of it nuclear weapons capability. The report asserts that while the U.S. in 1955 had "a very great offensive advantage relative to the U.S.S.R.," it claims, "SAC is vulnerable and U.S. is open to surprise attack."[258] However, the report believes that the U.S. would take the immediate technological lead in the mid- to late-1950s, at which point its "military power relative to that of Russia [will be] at its maximum."[259] In approximately a decade from the publishing of the report, the Soviets would reach an equilibrium of nuclear capability with the U.S. and "An attack by either side would result in mutual destruction. This is the period when both the U.S. and Russia will be in a position from which neither country can derive a winning advantage."[260] As a consequence of the time table, the committee recommended that the National Security Council (NSC) recognize the Air Force's ICBM program as "a nationally supported effort of highest priority," that actions be taken to reduce "the present unacceptable ground vulnerability of

[257] The Atlas ballistic missile project had been languishing due to technological issues levels of funding. However, a converging set of technological, geopolitical, and research factors changed the prospects of the program and prompted the issuance of the Killian Report. In 1953, the Air Force developed a "high-yield, lightweight" warhead that could be affixed to the top of a missile, encouraging the development of the ICBM. Intelligence estimates that suggested that the Soviet nuclear program was developing quickly enough "to knock out the US in a nuclear strike as early as mid-1954" put increased pressure on the U.S. government to issue the Killian Report. The Killian Report was a crucial element in the wave of pressure that made President Eisenhower "assign the highest national priority" to the Atlas program.
"Report by the Technological Capabilities Panel of the Science Advisory Committee." State.gov. February 14, 1955. Accessed November 12, 2014.
"Early Developments." Federation of American Scientists. Accessed November 12, 2014. http://fas.org/nuke/guide/usa/icbm/early.htm.
"The Missile Race Begins." Vectorsite.net/. Accessed November 12, 2014. http://www.vectorsite.net/tamrc_04.html.
[258] "Report by the Technological Capabilities Panel of the Science Advisory Committee." State.gov. February 14, 1955. Accessed November 12, 2014.
[259] "Report by the Technological Capabilities Panel of the Science Advisory Committee." State.gov.
[260] "Report by the Technological Capabilities Panel of the Science Advisory Committee."

Strategic Air Command," and that efforts be made to improve the early warning system, among others.[261]

The Gaither Report acted as a catalyst along with the *Sputnik* launch to "jolt Eisenhower into action."[262] Before 1957, the Eisenhower administration hoped to wield the doctrine of massive retaliation in the place of substantially investing in conventional forces "to deter any large-scale Soviet aggression while holding down defense spending."[263] The key aspect worth noting in this report is that the U.S. investment in its nuclear deterrent program was not a foregone conclusion. At the time, Democrats in Congress were deeply criticizing the Eisenhower Administration for not investing more in defense, particularly to protect the civilian population.[264] The main problem with the report is its "alarmist view of Soviet" economic and nuclear capabilities overestimated the threat posed by the U.S.S.R. to the U.S.[265] This exaggerated perception of the threat was likely a combination of not having access to sufficient intelligence ("the U-2 program… was in its infancy") and the "across-the-board disenchantment among panel members with the massive retaliation doctrine and with Eisenhower's outwardly blasé attitude toward recent Soviet accomplishments."[266]

The change movement's push for a U.S. nuclear policy centered on strategic deterrence took decades to take hold. With the support of politicians, strategists, and scientists, the idea that the revolutionary technology of nuclear weapons necessitated an entirely new concept matured and became convention. This influenced, like the other portions of the debate, the technological development of nuclear weapons, which resulted in a self-reinforcing cycle between theory and

[261] "Report by the Technological Capabilities Panel of the Science Advisory Committee."
[262] Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role." *Diplomatic History* 25, no. 1, 155.
[263] Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role." 153.
[264] Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role."
[265] Thielmann, Greg. "The Missile Gap Myth and Its Progeny." Arms Control Association. Accessed November 12, 2014. http://www.armscontrol.org/act/2011_05/Thielmann.
[266] Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role."

practice. Had it not, there is a much higher chance that nuclear weapons would have been used in the Cold War.

Impact of the Debate

Albert Einstein said less than a year after Hiroshima and Nagasaki bombings, "The unleashed power of the atom has changed everything save our modes of thinking."[267] The continuity movement maintained a powerful presence in the debate over nuclear weapons throughout the length of the nuclear revolution. The impact of the movement on policy and popular discourse cannot be underestimated. However on balance, the change movement was more successful in pushing its ideas into the mainstream policy and theoretical conversations. The change movement's calls for major revisions of doctrine regarding first strike, defense, and deterrence appear to have largely won out in the battle for U.S. policy. Ultimately, while both movements in the debate were advocating for the same objective of preventing the U.S.S.R. from attacking long enough for it to collapse from stagnation, the theoretical underpinnings of the ultimately successful U.S. policies primarily came from the change movement.

Conclusion

Nuclear weapons are peerless. They qualify as a revolution in military affairs, but have three key aspects that make it a stable strategic deterrent: their destructiveness, the assuredness of their destructiveness, and the debate over their use. Strategic deterrence was not an inevitable outcome of the nuclear revolution in military affairs. Had the debate developed in a different manner and nuclear technology taken an alternative path, it is very possible that the U.S. or the U.S.S.R. would have used nuclear weapons after Hiroshima and Nagasaki. However, they did not and in so doing they created a template that in hindsight looks temptingly clear and replicable

[267] Drell, Sidney D., and James E. Goodby. "Nuclear Deterrence in a Changed World." Arms Control Today. Accessed February 4, 2015. http://www.armscontrol.org/act/2012_06/Nuclear_Deterrence_in_a_Changed_World.

to the policymakers of today. Making the analogy between nuclear and cyber deterrence means that strategic cyber weapons should have similar characteristics. To see if strategic cyber weapons are capable of doing the same, the next chapter will see if they do have similar characteristics in order to evaluate the nuclear-cyber deterrence analogy.

Megatons to Megabytes: A Cyber Revolution in Military Affairs?

> "Someone has crossed the Rubicon… in one sense at least, it's August 1945"
> - Former Director of the NSA and CIA, General Michael V. Hayden, after the Stuxnet attacks[268]

Introduction

To the Iranian operators of the uranium enrichment facility at Natanz, nothing seemed out of the ordinary. Yet, despite the absence of an alarm, a computer worm that would become known after the fact as "the most sophisticated cyberweapon ever deployed" was systematically working its way through their computers and interfering with their software.[269] The worm, called Stuxnet, compromised the programmable logic controllers of the Natanz facility and destroyed about a fifth of Iran's nuclear centrifuges by causing them to spin at internally damaging high speeds.[270] When the worm spread to computers beyond the enrichment plant, various anti-virus companies such as Symantec, Kaspersky, and McAfee began to investigate it and the media launched into reporting frenzy about a new era of cyber warfare.[271] After the news broke, General Michael Hayden dramatically compared the first use of a state-constructed kinetic cyber weapon to the first use of nuclear weapons.

When General Hayden made the comparison he joined a large group of high-level policymakers who have also made the nuclear-cyber analogy, frequently in regards to issues of deterrence. The analogy is problematic because it has a strong surface appeal, but has deep internal flaws. This chapter shines light on those flaws by comparing strategic cyber weapons to

---

[268] Sanger, David. "Mutually Assured Cyberdestruction?" The New York Times. June 2, 2012. Accessed March 16, 2015. http://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html.
[269] Broad, William, John Markoff, and David Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." The New York Times. January 15, 2011. Accessed May 21, 2015. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.
[270] Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. February 26, 2013. Accessed May 21, 2015. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
[271] Kim, Zetter. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." Wired.com. July 7, 2011. Accessed May 21, 2015. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

the strategic deterrent template of nuclear weapons. This evaluation of the analogy limits its analysis to strategic cyber weapons to make a fairer comparison.[272] As President Barack Obama said of the nuclear-cyber analogy, "With nuclear weapons there is a binary. Either there are no nuclear explosions or there are big ones and it is a real problem. In cyberspace, there are all sorts of gradations."[273] There are two key characteristics of strategic cyber weapons that solve this problem of comparing a binary to a spectrum: their destructiveness and their high barriers to entry. The first means that these weapons have the potential to inflict unacceptable costs on an adversary, making them potential candidates to become a strategic deterrent. The second means that a limited number of players are capable of wielding them. Instead of thousands of actors there are only three – the U.S., Russia, and China.[274] After restricting its analysis, the evaluation determines that strategic cyber weapons currently do not meet the standards of a revolution in military affairs and do not have the strategic deterrent characteristics of nuclear weapons. Consequently, it is not possible to make the nuclear-cyber deterrence analogy at the present.

Cyber Revolution in Military Affairs

Jessica Kutz locked the front door of her house and clicked the safety off on her father's shotgun. Before, she had gone out to line up at the gas station for fuel and the bank for money, but now she did not feel safe outside of her home. It had been two months since the power had gone out, a month since the food market and pharmacy shelves had become empty, and a few

[272] A strategic cyber weapon is malware capable launching an irreversible computer network attack against cyber-dependent economic, military, and political systems and infrastructure that causes a debilitating level of casualties and damage to a state. The U.S. Department of Defense does not have a definition for strategic cyber weapons. See footnote fourteen for additional definitions.
"Legal Reviews of Weapons and Cyber Capabilities." Department of the Air Force. May 13, 1994. Accessed March 16, 2015. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-053.pdf.
"Strategic Cyber Weapon: No Results Found." DOD Dictionary of Military and Associated Terms. Accessed May 21, 2015. http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=strategic cyber weapon&zoom_sort=0&zoom_per_page=10&zoom_and=1.
[273] Obama, Barack. Interview by author. February 13, 2015.
[274] Please refer to footnote nineteen for justification.

weeks since prowling looters had replaced patrolling policemen the streets of her small town in rural Washington. Before her portable radio had run out of batteries, she had listened to news reports of American and Chinese naval forces clashing in a series of escalating engagements following China's sudden seizure of Taiwan. The government had issued warnings that China was conducting debilitating strategic cyber attacks on the West Coast. After the radio died, she felt isolated from the world. She and her family had been surviving on five-gallon jugs of water and canned foods from the basement, but their supplies were dwindling. She felt increasingly alone in the neighborhood. Their elderly and sick neighbors had died quickly, while the younger families had left for Seattle. Now she spent her evenings sitting in a chair in the front hall with the shotgun in her lap, protecting her family while they slept. She did not know how much longer she could continue on like this.[275]

Advance in Technology

The ability of states to launch non-physical, intercontinental attacks in an instant with strategic, kinetic effects is a significant leap in military technology in the context of the brief history of cyberspace. Cyber intrusions (the delivery method for all cyber payloads) have grown from small groups performing acts of cyber vandalism and theft to governments conducting

[275] This is an account of fiction based on the following sources:
Smith, Amelia. "China Could Shut Down U.S. Power Grid With Cyber Attack, Says NSA Chief." Newsweek. November 21, 2014. Accessed March 16, 2015.
Lewis, James A. "Thresholds for Cyberwar." Center for Strategic and International Studies. September 1, 2010. Accessed May 21, 2015. http://csis.org/files/publication/101001_ieee_insert.pdf.
Bronk, Christopher. "Hacks on Gas: Energy, Cybersecurity, and U.S. Defense." James A. Baker III Institute for Public Policy. February 5, 2014. Accessed May 21, 2015. http://bakerinstitute.org/research/hacks-gas-energy-cybersecurity-and-us-defense/.
"Critical Infrastructure: Threats and Terrorism." Https://fas.org/irp/threat/terrorism/sup2.pdf. August 6, 2006. Accessed May 21, 2015. https://fas.org/irp/threat/terrorism/sup2.pdf.
Assante, Michael. "America's Critical Infrastructure Is Vulnerable To Cyber Attacks." Forbes. November 11, 2014. Accessed May 21, 2015. http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/.
"Critical Infrastructure Sectors." Department of Homeland Security. Accessed May 14, 2015. http://www.dhs.gov/critical-infrastructure-sectors.

major operations of cyber espionage and sabotage.[276] The first major case of a cyber intrusion occurred when a team of West German hackers working for Soviet intelligence agents stole information from U.S. research and military institutions in 1986.[277] A couple of years later, the Morris Worm spread across the nascent Internet and inadvertently overwhelmed a substantial proportion of online computers.[278] In 1999 and 2001, Chinese patriotic hackers launched distributed denial of service (DDOS) attacks against U.S. government websites in response to the accidental NATO bombing of a Chinese embassy and a collision between American and Chinese military jets.[279] In 2007, Russian hackers used DDOS attacks against Estonian political, financial, and media networks in retaliation for the relocation of a Soviet war memorial.[280] In 2012, U.S. government officials attributed DDOS attacks against U.S. financial institutions and a more sophisticated case of cyber espionage against the company Saudi Aramco to Iran.[281] The

---

[276] Jason Healey defines a cyber intrusion as "Any deliberate and illegal entry into a computer system, such as to exfiltrate (steal) information or conduct a later disruptive attack."
The delivery methods of strategic cyber weapons developed slightly before and in parallel to their payloads, in a manner akin to the invention and improvement of aircraft, submarines, and missiles both preceded and evolved concurrently with nuclear weapons.
A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 21. Cyber Conflict Studies Association, 2013.
[277] In this early case, the U.S. was able to attribute the attacks and arrest the hackers
Markoff, John. "West Germans Raid Spy Ring That Violated U.S. Computers." New York Times. March 3, 1989. Accessed March 16, 2015.
Healey, Jason. "A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 29-30. Cyber Conflict Studies Association, 2013.
[278] Healey, Jason. "A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 30-31.
Spafford, Eugene. "The Internet Worm Program: An Analysis." Purdue University. December 8, 1988. Accessed March 16, 2015.
[279] Brenner, Joel. "Between War and Peace." In *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, 145. New York: Penguin Press, 2011.
Geers, Kenneth. "Cyberspace and the Changing Nature of Warfare." SC Magazine. August 27, 2008. Accessed March 16, 2015.
[280] Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.
[281] Perlroth, Nicole, and Quentin Hardy. "Bank Hacking Was the Work of Iranians, Officials Say." The New York Times. January 8, 2013. Accessed May 21, 2015. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." The New York Times. October 23, 2012. Accessed May 21, 2015. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

U.S. government also accused the North Korean government of penetrating the networks of Sony Pictures to steal, manipulate, and erase data from their servers in 2014.[282] None of these attacks broke the cyber-physical barrier and their effects were largely reversible.

The history of cyber attacks that have traversed the barrier with irreversible effects is much shorter in the open literature. In a series of experiments, university researchers and ethical hackers between 2008 and 2012 revealed that hackers could remotely access medical devices, reprogram them to fail, and cause injury and death.[283] Another set of university researchers demonstrated in 2010 that hackers could place a driver in danger by instructing a car to ignore driver input while they turned off the headlights, switched off the engine, and disabled the brakes.[284] Outside of experiments, disgruntled workers and mischievous teenagers since 2000 have used cyber attacks to misdirect sewage water, to create traffic gridlock, and to derail trams.[285] In terms of government testing and use of kinetic cyber attacks, there are three major known examples. In 2007, the Department of Homeland Security conducted a test called Project Aurora in which it destroyed a large power generator at the Department of Energy's Idaho Laboratory.[286] In the mid-to-late 2000s, Stuxnet (an allegedly joint American and Israeli

---

[282] Cieply, Michael, and Brooks Barnes. "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm." The New York Times. December 30, 2014. Accessed March 16, 2015.

[283] Greenemeier, Larry. "Heart-Stopper: Could Hackers Hit Pacemakers, Other Medical Implants?" Scientific American. March 14, 2008. Accessed March 16, 2015.
Maisel, William H., and Tadayoshi Kohno. "Improving the Security and Privacy of Implantable Medical Devices." *New England Journal of Medicine* 7, no. 1 (2008): 116-166.
Grubb, Ben. "Fatal Risk at Heart of Lax Security." The Sydney Morning Herald. November 6, 2012. Accessed March 16, 2015.

[284] Karl Kosher et al. "Experimental Security Analysis of a Modern Automobile." January 1, 2010. Accessed March 16, 2015.

[285] Slay, Jill, and Michael Miller. "Lessons Learned from the Maroochy Water Breach." International Federation for Information Processing. Accessed March 16, 2015.
http://www.ecdlhealth.it/wcc2008/IFIP_Sample_Chapter_Created_LaTeX.pdf.
Bernstein, Sharon, and Andrew Blankstein. "Key Signals Targeted, Officials Say." Los Angeles Times. January 9, 2007. Accessed March 16, 2015. http://articles.latimes.com/2007/jan/09/local/me-trafficlights9.
Baker, Graeme. "Schoolboy Hacks into City's Tram System." The Telegraph. January 11, 2008. Accessed March 16, 2015. http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

[286] Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." CNN. September 26, 2007. Accessed March 16, 2015. http://www.cnn.com/2007/US/09/26/power.at.risk/.

operation) destroyed almost one thousand centrifuges at the Iranian Natanz enrichment facility.[287] In 2014, the German Federal Office for Information Security announced a cyber attack by an advanced persistent threat group that caused "massive damage" at a German steel mill.[288] Although large governments likely have strategic cyber weapons, they have not used them to date.[289]

Change in Doctrine

In the face of strategic cyber weapons and the broader cyber threat, the U.S. government has changed innumerable doctrines, particularly in regards to cyber deterrence. The development of a deterrence doctrine for cyberspace begins with the 2011 *United States International Strategy for Cyberspace*, which states, "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country… We reserve the right to use all

---

DHS allowed CNN to film the results, which can be watched here: "Staged Cyber Attack Reveals Vulnerability in Power Grid." YouTube. September 27, 2007. Accessed March 16, 2015. https://www.youtube.com/watch?v=fJyWngDco3g.

[287] The "one sense" that General Hayden is referring to in the epigraph of this chapter is that Stuxnet was "the first attack of a major nature in which a cyberattack was used to effect physical destruction." The attack was also unique because the private sector had never seen anything like the state-constructed code or use of zero day exploits before.
Applegate, Scott. "The Dawn of Kinetic Cyber." NATO Cooperative Cyber Defense Center of Excellence. Accessed March 16, 2015. https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf.
Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran." The New York Times. May 31, 2012. Accessed March 16, 2015. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired.com. November 3, 14. Accessed March 16, 2015. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[288] "Hack Attack Causes 'massive Damage' at Steel Works." BBC News. December 22, 2014. Accessed May 21, 2015. http://www.bbc.com/news/technology-30575104.
De Maizière, Thomas. "Die Lage Der IT-Sicherheit in Deutschland 2014." Federal Office for Information Security. 2014. Accessed May 21, 2015. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.

[289] This is possibly more a function of a lack of opportunity than a lack of ability. The U.S. first used nuclear weapons during the Second World War. It is probable that it had developed nuclear weapons during the interwar period (all geopolitical consequences aside) that the U.S. would not have used them until the outbreak of hostilities. Strategic cyber weapons would be very different right now if there was a conflict on the scale of the Second World War ongoing.
Director James Clapper noted in 2013, "Advanced cyber actors – such as Russia and China – are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests."
Rogers, Michael. "Hearing on Cybersecurity Threats."
Clapper, James. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community."

necessary means… as appropriate and consistent with applicable international law."[290] *The Department of Defense Cyber Strategy* of 2015 declares, "In the face of an escalating threat, the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy."[291] It builds upon the 2011 strategy and announces, "The United States will continue to respond to cyberattacks against U.S. interests, at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law."[292] While these doctrines are moving in a promising direction and definitely represent a change from the past, they are still largely inchoate in comparison to the strategies for nuclear and conventional forces. For instance, the cyber deterrence doctrine to date is unclear on thresholds for retaliation, extended deterrence, and who the U.S. is deterring.

Beyond these stated policies, the U.S. has made a number of internal doctrinal changes in anticipation of larger cyber threats such as strategic cyber weapons. The military has designated cyberspace as war-fighting domain, established a U.S. Cyber Command, and stated that a cyber attack from another state can constitute an act of war.[293] The U.S. government currently handles the decision process about cyber weapons in a highly centralized manner. General Hayden recalled that during his time in government that any use of offensive cyber weapons, "had to go through the White House" virtually irrespective of the operational level using it.[294] As with

---

[290] "International Strategy for Cyberspace." White House. May 1, 2011. Accessed May 21, 2015. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[291] "The DoD Cyber Strategy." U.S. Department of Defense. April 1, 2015. Accessed May 21, 2015. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
[292] "The DoD Cyber Strategy." U.S. Department of Defense.
[293] "National Military Strategy for Cyberspace Operations." Department of Defense. December 11, 2006. Accessed March 16, 2015.
"Cyberspace as a Warfighting Domain: Policy, Management, and Technical Challenges to Mission Assurance." House of Representatives Committee on Armed Services. March 5, 2009. Accessed March 16, 2015.
"U.S. Cyber Command." U.S. Strategic Command. Accessed March 16, 2015.
Gorman, Siobhan, and Julian E. Barnes. "Cyber Combat: Act of War." Wall Street Journal. May 31, 2011. Accessed May 21, 2015. http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.
[294] Hayden, Michael. Interview by author. March 10, 2015.

nuclear weapons, it appears the president is once again the "first soldier" in any cyber conflict.[295] This is likely because the government, the military, and civilian strategists are unsure of how to deploy cyber weapons given their novelty. As former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism Richard Clarke said, "It's like the early days of the American-Soviet nuclear balance. We don't know the rules of the road."[296]

Due to the nature of strategic cyber weapons, the government is also adapting doctrinally to having to coordinate with the private sector. With an estimated 85 percent of U.S. critical infrastructure privately owned, the U.S. government is reliant on the private sector to protect its national interests in a way that it never was for nuclear weapons.[297] As Brian White, a former cyber principal at the Chertoff Group put it, "the U.S. government never asked companies to put anti-ballistic missiles on their roofs to protect them against foreign nuclear attack, but it effectively is now with cyber weapons."[298] Top leaders in the private sector recognize the necessity of the government providing them protection from foreign strategic cyber attacks. Anthony Earley, Chairman and CEO of Pacific Gas & Electric, stated that nation-states pose the biggest threat to U.S. critical infrastructure because "our infrastructure is so complicated that only a sophisticated actor could bring it down."[299] Kenneth Chenault, Chairman and CEO of American Express, acknowledged, "private industry is quicker in sharing information in some areas than the government, but the government is necessary to coordinate sharing because companies in private industry have a competitive instinct and do not share as much as they

[295] Nelson, Michael. "Commander in Chief." In The Powers of the Presidency, 279. Washington, DC: CQ Press, 2008.
[296] "Cyber Weapons vs. Nuclear Weapons." Center for Strategic and International Studies. July 26, 2011. Accessed March 16, 2015.
[297] "ISE Mission Partners: Critical Infrastructure and Key Resources." Information Sharing Environment. Accessed March 16, 2015.
[298] White, Brian. Interview by author. August 10, 2014.
[299] Earley, Anthony. Interview by Author. February 13, 2015.

should, which leaves us vulnerable."[300] In the post-Snowden era, both the government and private sector have some distance to go before developing cohesive doctrines that strike the right balance between privacy and security in protecting U.S. interests.

Fundamental Change in the Balance of Power on the Battlefield

Despite these doctrinal changes, it is difficult to argue that strategic cyber weapons have fundamentally changed the balance of power on the battlefield. The most destructive known kinetic cyber attack to date is Stuxnet, which destroyed roughly 1000 centrifuges in an Iranian enrichment facility.[301] It appears that the public knowledge alone of strategic cyber weapons' existence is not sufficient to alter the balance of power.[302] The demonstration effect of a use in battle is likely necessary. The absence of such a shift in power is so perceptible that there many argue that threat of these weapons is exaggerated and may never materialize. A prime proponent of this view is Director of the Atlantic Council's Cyber Statecraft Initiative Jason Healey, who stated, "We have been worrying about a "cyber Pearl Harbor" for twenty of the seventy years since the actual Pearl Harbor"[303] Because strategic cyber weapons do not meet the standard of fundamentally changing the balance of power on the battlefield, the cyber revolution in military affairs has not yet matured.

Decisive Victory

There has never been a use of strategic cyber weapons in battle, so it is not possible for them to have caused a decisive victory. The attack that Jessica Kutz experienced was a hypothetical attempt to imagine what the use of strategic cyber weapons would look like. The

[300] Chennault, Kenneth. Interview by Author. February 13, 2015.
[301] Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran."
[302] Kemp, R. Scott. "Cyberweapons: Bold Steps in a Digital Darkness?" Bulletin of the Atomic Scientists. June 7, 2012. Accessed March 16, 2015.
[303] Concept of Cyber Pearl Harbor from Winn Schwartau testimony to Congress 1991, repeated by Jamie Gorelick deputy attorney general 1998, and Leon Panetta 2012
A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 21. Cyber Conflict Studies Association, 2013.

destructive effects of strategic cyber weapons could be much more or much less. In addition to what Kutz witnessed, strategic cyber weapons could disrupt global positioning systems (GPS), logistics supply chains, U.S. financial systems, energy systems, prison systems, and automobile, airplane, and train transportation networks, as well as military command and control, supply, and communications networks.[304] Depending on the size of the attack, there could be thousands of casualties and immense economic damage.[305] However, the bottom line is that strategic cyber weapons have not resulted in a decisive victory and therefore do not currently constitute a revolution in military affairs.

Potentially Revolutionary Technological Characteristics

Nuclear weapons have two technological characteristics that permit them to be a strategic deterrent: the sheer destructiveness of a single weapon and the assuredness of that destruction. Both are necessary for providing credible, unacceptable threats that form the basis of stable strategic deterrence. Because strategic cyber weapons have never been used, it is not known with certainty if they have these characteristics. The previous chapter provided several descriptions of both the effects of a nuclear detonation and of nuclear weapons delivery systems. While comparable descriptions could exist of strategic cyber weapons, they are highly classified. The following description of the potential damage and delivery of strategic cyber weapons is based on available open source literature. The general consensus in the open literature is that they are far from achieving strategic deterrent traits comparable to those of a mature nuclear arsenal.

Destructiveness

[304] As Jason Healey notes, "The most meaningful cyber conflicts rarely occur at the "speed of light" or "network speed"… conflicts are typically campaigns that encompass weeks, months, or years of hostile contact between adversaries." Healey, Jason. "A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 21. Cyber Conflict Studies Association, 2013.
Geers, Kenneth. "Data Analysis and Research Results." In *Strategic Cyber Security*, 138. Tallinn, Estonia: CCD COE Publication, 2011.

[305] Newton, Scott. "Can Cyberterrorists Actually Kill People?" SANS Institute. November 1, 2001. Accessed March 16, 2015.

While there has never been a use of strategic cyber weapons and the potential destructiveness of such an attack is largely unknown, there has been much speculation. At the highest levels of government, there have been several comparisons of the destructiveness of strategic cyber weapons to nuclear weapons. Secretary of State John Kerry referred to cyber weapons as "the 21st century nuclear weapons equivalent," and former Chairman of the Joint Chiefs of Staff Admiral Mike Mullen said that cyber is the "single biggest existential threat that's out there."[306] Americans are not alone in analogizing the destructiveness of strategic cyber weapons and nuclear weapons. Fang Fenghui, chairman of the People's Liberation Army General Staff stated, "If Internet security cannot be controlled, it's not an exaggeration to say that the effects could be no less than a nuclear bomb."[307] Russian Deputy Prime Minister Dmitriy Rogozin asserts that strategic cyber weapons offer states the first strike capability to "destroy

[306]Additionally, just as U.S. government officials early in the nuclear era worried about an "atomic Pearl Harbor," officials such as Secretaries of Defense Leon Panetta and Ash Carter (among others) have made reference to a "cyber Pearl Harbor."
General Brent Scowcroft, former National Security Advisor, has separately said, "The cyber issue… could be as dangerous as nuclear weapons, and there is no control anywhere about it."
Scowcroft, Brent, and Zbigniew Brzezinski. "Hearing on National Security Threats." Senate Armed Services Committee. January 21, 2015. Accessed May 21, 2015. http://www.c-span.org/video/?323887-1/hearing-national-security-threats.
"Senate Foreign Relations Committee Holds Confirmation Hearing on the Nomination of Massachusetts Democratic Sen. John Kerry to Be Secretary of State." Congressional Quarterly. January 24, 2013. Accessed March 8, 2015. http://www.cq.com/doc/congressionaltranscripts-4209477?0&print=true.
Muradian, Vago. "Adm. Michael Mullen." Defense News. July 10, 2011. Accessed March 8, 2015. http://archive.defensenews.com/article/20110710/DEFFEAT03/107100301/Adm-Michael-Mullen.
Full Quotation of Senator Brien McMahon, "If there is ever an atomic Pearl Harbor, there won't be a coroner's jury of statesmen left to talk about it."
Poundstone, William. Prisoner's Dilemma. New York: Anchor Books, 2011. 144.
"Baring A-Bomb Figures Asked." The Spokesman-Review, June 29, 1953. Accessed May 21, 2015. https://news.google.com/newspapers?nid=1314&dat=19530629&id=aC9WAAAAIBAJ&sjid=IuYDAAAAIBAJ&pg=7306,6991225&hl=en.
Rhodes, Richard. "This Buck Rogers Universe." In *Dark Sun the Making of the Hydrogen Bomb*, 357. New York: Simon & Schuster, 1995. 357.
"Secretary of Defense Confirmation Hearing." C-SPAN.org. June 9, 2011. Accessed March 16, 2015.
"To Consider the Nomination Of: Honorable Ashton B. Carter to Be Secretary of Defense." Senate Committee on Armed Services. February 4, 2015. Accessed March 16, 2015. http://www.c-span.org/video/?324143-1/defense-secretary-nominee-confirmation-hearing.
[307] Forsythe, Michael. "Chinese General With Dempsey Compares Cyber-Attack to Nuke." Bloomberg.com. April 22, 2013. Accessed March 16, 2015.

critical infrastructure of the state… [and] system[s] of political and military control."[308] Additionally, there is also fear of the lasting effects of such an attack. In the estimation of Colonel Martemucci, Commander of the 318th Cyberspace Operations Group, 688th Cyberspace Wing, most of the casualties of a current strategic cyber attack would come from "second and third order effects."[309] Perhaps in response to this potential threat, the White House issued in 2013 an executive order entitled, "Improving Critical Infrastructure Cybersecurity."[310] The order increases measures to protect all critical infrastructure, including infrastructure in the energy, agriculture, and public health sectors.[311] Attacks on these sectors could lead to many deaths due to heat or cold, starvation, and disease.

Outside of the government, there is a wide variance of opinion on the maximum destructiveness that a strategic cyber weapon can inflict. On one end of the spectrum, there are those who believe that the government's statements of the threat are hyperbolic. In an article entitled, "No, Cyberwarfare isn't as Dangerous as Nuclear War," Jason Healey observes, "Any widespread disruptions… have been short-lived causing no significant GDP loss."[312] Professor Derek Reveron of the U.S. Naval War College argues that there has never been a confirmed kill

[308] Translation assistance from Kate Kuhns, Executive Director of Stanford Global Studies
Васенин, Виктор, and Сергей Куксин. "Стенограмма выступления Дмитрия Рогозина на пресс-конференции в "РГ"" Российская газета. June 28, 2013. Accessed March 16, 2015. http://www.rg.ru/2013/06/28/doklad.html. https://translate.google.com/translate?hl=en&sl=ru&tl=en&u=http%3A%2F%2Fwww.rg.ru%2F2013%2F06%2F28%2Fdoklad.html

[309] Martemucci, Matteo. Interview by author. February 26, 2015.

[310] Obama, Barack. "Executive Order: Improving Critical Infrastructure Cybersecurity." The White House. February 12, 2013. Accessed May 21, 2015. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[311] "Critical Infrastructure Sectors." Department of Homeland Security. Accessed May 21, 2015. http://www.dhs.gov/critical-infrastructure-sectors.

[312] Although he also notes, "It is all to likely that America will take its overstretched and insecure electrical system and connect it to the Internet. In this future our electric supply is no more ore less reliable than the Internet and the years when no one died because of cyberattacks will seem like the quaint good ol' days."
Healey, Jason. "No, Cyberwarfare Isn't as Dangerous as Nuclear War." US News. March 20, 2013. Accessed March 16, 2015.

of a cyber attack.[313] Martin Libicki, a senior management scientist at the RAND Corporation, believes that, "It is unclear that a cyberwar campaign would have any more effect than even a universal trade embargo."[314] In another article he states, "most cyber attacks, once discovered are resolved and the effects (apart from leaked information) reversed within a period ranging from hours to days."[315] Admiral Cecil Haney, current commander of U.S. Strategic Command, compared the potential effects of a strategic cyber attack those of 9/11. The attacks "slowed down the economy and the airlines, but it wasn't long until people were flying again, planes filled again."[316] James Lewis, a senior fellow at the Center for Strategic and International Studies is also skeptical of the destructiveness of strategic cyber weapons. He believes that American critical infrastructures "are more distributed, diverse, redundant and self-healing than a cursory assessment may suggest," leading him to conclude that cyber vulnerabilities are "an increasingly serious business problem, but that their threat to national security is overstated."[317] In starker terms he said, "two MIRV'd ICBMs to the East Coast would kill 42 million people, tell me cyber weapons can do the same."[318]

On the other end of the non-government spectrum, there are a few who believe that strategic cyber weapons are currently as destructive as nuclear weapons. A 2013 Defense

---

[313] Reveron, Derek S. "Conclusion."

[314] He states earlier in the text, "One can hardly compare what even a vigorous cyberwar might do to what the inhabitants of Sarajevo had to endure in 1992 through 1995 or to what the denizens of Jerusalem endured in 1947 and 1948. In both cases, solidarity held."
Libicki, Martin. "Strategic Cyberwar." In *Cyber Deterrence and Cyber War*, 123. RAND Corporation, 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[315] Libicki in general is skeptical of the need to have a strategic thinking specifically for cyber weapons because they are not as destructive or as revolutionary as others claim. In this sense, he is somewhat like those who argued that pre-nuclear tactics would be sufficient for nuclear weapons.
Libicki, Martin. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly*, 2014.

[316] Haney, Cecil. Interview by Author. January 24, 2015.

[317] Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats." Center for Strategic and International Studies. December 1, 2002. Accessed May 21, 2015. http://www.enhyper.com/content/0211_lewis.pdf.

[318] Lewis, James. Interview by author. March 18, 2015.

Science Board report states, "The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War."[319] The report goes on to recommend that the U.S. government maintain the option of responding with nuclear weapons if the country suffers an "existential cyber attack."[320] Richard Clarke provides an extreme version of the current capabilities of a strategic cyber weapon. In his book called *Cyberwar*, he describes a scenario in which Chinese hackers use strategic cyber weapons against the U.S. to critically and simultaneously disrupt key critical infrastructure systems all over the country. He states, "In all the wars America has fought, no nation has ever done this kind of damage to our cities. A sophisticated cyber attack by one of several nation-states could do that today, in fifteen minutes."[321]

One potential issue with the destructiveness of strategic cyber weapons is their payloads are not guaranteed to successfully 'detonate.' The barrier to obtaining the desired effect of a strategic cyber weapon after the delivery of its payload is higher than that of a nuclear weapon. The success of a nuclear weapon is not dependent on exploiting pre-existing vulnerabilities; a nuclear bomb simply has to destroy whatever is in its destructive radius. As cyber security analyst Pasi Hakkarainen notes, "[A] cyber weapon system is not intended to destroy everything,

---

[319] The report sources its conclusion from "more than 50 briefings from practitioners and senior officials throughout the DoD, Intelligence community (IC), commercial practitioners, academia, national laboratories, and policymakers."
The Defense Science Board is a group of civilian experts appointed to advise the Department of Defense on technical matters.
"Resilient Military Systems and the Advanced Cyber Threat." Defense Science Board. 2013. Accessed May 21, 2015. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[320] "Resilient Military Systems and the Advanced Cyber Threat." Defense Science Board.

[321] Richard Clarke's views are widely known to represent the extreme end of the spectrum. A review from Wired with the title of "Richard Clarke's Cyberwar: File Under Fiction" calls his description in *Cyberwar* "the Book of Revelation re-written for the internet age, with the end-times heralded by the Four Trojan Horses of the Apocalypse."
Clarke, Richard A., and Robert K. Knake. Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco, 2012. 67.
Singel, Ryan. "Richard Clarke's Cyberwar: File Under Fiction." Wired.com. April 22, 2010. Accessed May 21, 2015. http://www.wired.com/2010/04/cyberwar-richard-clarke/.

which is possible, but it identifies the target before executing the exploits. The key functionality of the cyber weapon is to find and identify the cyber target with the exploitable vulnerability."[322] Cyber weapons meant to have a kinetic effect have to overcome two obstacles: they must gain sufficient control of the targeted computer system and then exploit that control to break the cyber-physical barrier and have the intended effect.[323] For example, a cyber attack on the supervisory control and data acquisition (SCADA) network of a railway company that aims to derail trains by changing track switches needs to first successfully penetrate and alter the networks of the rail company before it can target the train tracks.[324] With a nuclear weapon, the same attack would simply be a matter of delivering and detonating the weapon in the correct place.

From what is available in the open literature, it does not appear that strategic cyber weapons are capable of inflicting the damage of a nuclear weapon at the present. That answer may change as societies become increasingly reliant on computer-based technology and as governments develop more powerful strategic cyber weapons. As cyber attack area increases, more and more of the society will be vulnerable to cyber attack and the number of first-order

---

[322] Hakkarainen, Pasi. "Cyber Weapon System." In *Cyber Weapon Target Analysis*, 43. Books on Demand.

[323] This is a slight oversimplification. Charles Croom, former director of the Defense Information Systems Agency, notes, "The attacker has to take a number of steps: reconnaissance, build a weapon, deliver that weapon, pull information out of the network. Each step creates a vulnerability, and all have to be completed. But a defender can stop the attack at any step."
Langner, Ralph. "Stuxnet's Secret Twin." Foreign Policy. November 19, 2013. Accessed March 16, 2015.
Singer, Peter, and Allan Friedman. "Why It Matters." In *Cybersecurity What Everyone Needs to Know.*, 155. New York: Oxford University Press, 2012.

[324] SCADA systems also control signal and crossing lights, transformers, weather and track sensors, engine monitors, railway car sensors and a plethora of other things. Their use is increasing across the developed nations because, as founder of Casaba Security (security analysis company) Samuel Bucholtz notes, "The benefit of SCADA being 'online' is that the Internet is cheap, robust, standardized and easily accessible." The U.K., for instance, recently awarded a contract to one private company to concentrate control of all of its railways on to one SCADA network.
Rashid, Fahmida. "SCADA Systems in Railways Vulnerable to Attack." EWeek. January 25, 2012. Accessed March 16, 2015.
"Telent to Renew NR's Traction Power Control Network." Railway Gazette. September 12, 2013. Accessed March 16, 2015.

casualties will likely increase. However, it is just as possible that strategic cyber weapons will never be as destructive as nuclear weapons. Because of their lack of demonstrated destructiveness, strategic cyber weapons are not currently capable of being a stable strategic deterrent in their own right.

Assurance of Delivery

There is a broader knowledge of the delivery systems of strategic cyber weapons because they are largely the same as those used for cyber exploitation (such as cyber theft or cyber espionage). As Herb Lin, a senior research scholar for cyber policy at Stanford University, says, "The primary technical difference between cyber attack and cyberexploitation is in the nature of the payload to be executed."[325] Because there have been countless cases of cyberexploitation documented in the open literature, it is possible to have a much clearer idea of the speed, range, and security of the delivery systems of strategic cyber weapons.

Reports in the news often claim that strategic cyber weapons can deliver their payloads in milliseconds. While it is true that the U.S. government can deliver strategic cyber weapons faster than any other weapon in history, the answer is slightly more nuanced than it seems. General Keith Alexander, former Director of the NSA and Commander of Cyber Command, noted in his 2010 testimony to Congress that "time and distance are less relevant in the cyber domain than in any other."[326] *The National Military Strategy for Cyberspace Operations* states that cyber weapons can "deliver effects at speeds that were previously incomprehensible"[327] By comparison, over the course of the nuclear revolution, the speed with which the U.S. could use

[325] "Cyber attacks and cyberexploitation require a vulnerability, access to that vulnerability, and a payload to be executed."
Lin, Herb. "Offensive Cyber Operations and the Use of Force." Journal of International Security, Law, & Policy 4, no. 63 (2010): 63-86. Accessed May 21, 2015. http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
[326] "Statement of General Keith B. Alexander." House of Representatives Committee on Armed Services. September 23, 2010. Accessed March 16, 2015.
[327] "National Military Strategy for Cyberspace Operations." Department of Defense. December 11, 2006. Accessed March 16, 2015.

nuclear weapons dropped from as many as 17 hours with the B-29 Superfortress to around twenty minutes with intercontinental ballistic missiles.[328] However as Peter Singer and Allan Friedman, a political scientist and a cyber security analyst, note, "The cyberattacks that are truly dangerous require a great deal of expertise to put together. And while they might play out in terms of microseconds, they often take long periods of planning and intelligence gathering to lay the groundwork."[329] The speed with which the U.S. can deliver strategic cyber weapons greatly depends on how quickly a hacker can penetrate the defenses of the target. This requires intelligence on the target, a well-designed weapon, and the ability to deliver that weapon. Of course, all of these aspects are true for nuclear weapons as well. What is different for strategic cyber weapons is that it is difficult to maintain a standing 'arsenal' because their delivery is dependent upon the existence of vulnerabilities in the adversary's systems. The attacker is constantly seeking to exploit the systems' vulnerabilities while a defender is trying to patch them.[330] If the defender succeeds, then the attacker must find another way into the system. Thus, while an attack could take place over milliseconds, the defender has the ability to substantially lengthen the time it takes for an attacker to use a strategic cyber weapon.

Similarly, the range of a strategic cyber weapon is also not straightforward. It is bound not by distance, but rather by accessibility to computer systems. Systems that use analog controls, such as nuclear weapons and power plants built in the 1950s, are more resistant to

[328] Slade, Stuart. "Boeing B-29 Superfortress." In *United States Strategic Bombers 1945: 2012.*, 10. Defense Lion Publications, 2012.
[329] Singer, Peter, and Allan Friedman. "Why It Matters." 154.
[330] This also leads to issues of repeatability. Exploiting a vulnerability might work once, but if the victim is aware and capable, he or she could fix it before the next attack. As Libicki states, "As a general rule, tricks exhaust themselves to the extent (1) that their existence and thus the need to protect against their recurrence is obvious and (2) that counters to their recurrence are straightforward to implement."
Libicki, Martin. "Why Cyber Deterrence is Different." In *Cyber Deterrence and Cyber War*, 57.

direct cyber attacks than digitized systems.[331] Areas where there are no man-made systems at all are virtually impervious to direct cyber attack. As General Alexander notes, "In cyberspace the only "perfect" defense is the static one: to disconnect and thereby forfeit the cyber realm and its economic and social benefits to one's adversaries."[332] In a sense, cyber warriors today are limited in where they can strike in a manner that is somewhat comparable to how delivery systems limited the range of nuclear weapons in the 1940s and 1950s.[333] The U.S. government is spending significant quantities on both offensive and defensive efforts to find vulnerabilities within the systems of adversaries and patch vulnerabilities within its own networks in order to expand its range while limiting that of its adversaries. On the offensive side a Russian cyber security company called the Kaspersky Lab, recently attributed a massive effort to discover and exploit cyber vulnerabilities around the world to the Equation Group, which is allegedly linked to the NSA.[334] Kaspersky claimed that it found the Equation Group's software exploiting vulnerabilities in government, military, and research institutions as well as key critical infrastructure in Russia, China, Iran, and a number of other traditional U.S. adversaries.[335]

---

[331] However, as these systems are converted from analog to digital (due to demands for increased efficiency, diminishing analog expertise, etc.) they will become increasingly vulnerable to direct and indirect cyber attacks.
Wiggins, James, C. Erlanger, and T. Harris. "Regulatory Efforts to Improve Cyber Security." U.S. Nuclear Regulatory Commission. Accessed March 16, 2015.

[332] Herb Lin describes the dichotomy as "secure but useless" vs. "useful but potentially insecure."
"Statement of General Keith B. Alexander." House of Representatives Committee on Armed Services. September 23, 2010. Accessed March 16, 2015.
Lin, Herb. "Testimony by Herbert Lin." House Committee on Energy and Commerce Subcommittee on Oversight and Investigations. March 3, 2015. Accessed May 21, 2015. http://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-Wstate-LinH-20150303.pdf.

[333] The range of nuclear weapons grew from 1820 nautical miles (with the B-29) to almost anywhere in the world with intercontinental ballistic missile. As more and more of the world uses computer-reliant technology, the range of strategic cyber weapons expands.
Slade, Stuart. "Boeing B-29 Superfortress."

[334] Zetter, Kim. "How the NSA's Firmware Hacking Works and Why It's So Unsettling." Wired. February 22, 2015. Accessed May 21, 2015. http://www.wired.com/2015/02/nsa-firmware-hacking/.

[335] Menn, Joseph. "Russian Researchers Expose Breakthrough U.S. Spying Program." Reuters. February 16, 2015. Accessed March 16, 2015.

The security of the ability to use strategic cyber weapons is not a shared concern with nuclear weapons as it is not possible to prevent retaliation in cyberspace. While nuclear weapons are vulnerable to a counter force strike that potentially leaves the U.S. unable to respond to an attack, strategic cyber weapons are not. The U.S. can launch strategic cyber weapons from a number of platforms and is not overly dependent on its hardware (perhaps with the exception of the most advanced hardware). As noted earlier, states have difficulty perpetually maintaining standing cyber arsenals because defenders are constantly patching the vulnerabilities in their networks, which means it is hard 'destroy' them. The only way to prevent a strategic cyber attack is through very strong defense, not offense. In this sense, the nature of strategic cyber weapons could potentially be very helpful as a stabilizing deterrent force in cyberspace; the weapons can hold the physical and economic security of an adversary at risk, but they cannot prevent an adversary's ability to respond. This situation is very much akin to how the development of secure second strike forces played a stabilizing role in nuclear strategic deterrence.

The Debate: Defense and Deterrence

The emergence of strategic cyber weapons has prompted a robust debate both in and out of the U.S. government on how the government should use the weapons, just as nuclear weapons did. The potentially revolutionary and highly threatening characteristics of strategic cyber weapons has added a sense of urgency to the debate. However, because strategic cyber weapons remain so highly classified and the government has never publicly demonstrated them the debate remains on two tracks: one in the classified world and one outside of it, with limited interaction between the two. The progress of the former is unknown, but the public debate is still very much in its infancy and has yet to make significant strides. This is largely because, at this point, the participants are mostly speculating and making conclusions off of the limited information

available. It is in this context that there is significant debate over the role of defense and deterrence in cyberspace.[336]

Defense

As with nuclear weapons, the debate over defense against strategic cyber weapons is future looking, because the defense systems have yet to be developed. It is particularly relevant to deterrence because much of policymaker's interest in applying nuclear-style deterrence in cyberspace is because of the offense-dominated nature of strategic cyber weapons. If cyber defenses become highly effective in the future, then they will remove much of the impetus for the discussion for cyber deterrence. If defenses prove to be only effective for lower level threats such as cyber espionage and cyber vandalism, then the cyber deterrence debate will focus on advanced persistent threats posed by large states.

There is a broad range of opinion on the prospects of cyber defense in the open debate. Martin Libicki is one of the most optimistic about the future of cyber defense. He also is one of the most skeptical of the threat posed by strategic cyber weapons. In one of Libicki's articles he states, "It is not obvious that offense will get continually better, particularly when defense (in the form of the target's system and software) defines what offense can do."[337] Others hold a less enthusiastic viewpoint. Former Secretary of Defense Robert Gates said, "I think you can create defenses – they may not be perfect, but you can significantly limit damage"[338] Colonel Martemucci argues that it is possible not only to defend against low-end threats, but also to present "a pretty formidable set of protections that would make a state spend a significant

[336] There is very little debate over first strike using strategic cyber weapons because at the present it is not possible to prevent retaliation in cyberspace with an attack. In essence, secure second-strike capability already exists in cyberspace.

[337] Libicki, Martin. "Why Cyber War Will Not and Should Not Have Its Grand Strategist."

[338] He added, "Our problem is not the absence of the technical defenses, it is the absence of a political consensus about how they would be constructed and role of the private sector vs. the government since the private sector controls most of the infrastructure."
Gates, Robert. Interview by Author. March 23, 2015.

amount of national treasure" to hold American systems at risk.[339] However, he acknowledges that cyber defense "falls apart when you are talking about trying to deter an avowed enemy."[340] On the more pessimistic end of the spectrum, Herb Lin argues, "the offense is inherently superior to the defense, because the offense needs to be successful only once, whereas the defense needs to succeed every time."[341] Former Deputy Secretary for Defense William Lynn concurs, "In cyberspace, the offense has the upper hand."[342] In terms of a solution to the emerging threat, he is wary of defenses ("The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun").[343] At the same time he also points to cyber defense as the future of security of American interests in cyberspace ("The challenge is to make defenses effective enough to deny an adversary the benefit of an attack despite the strength of offensive tools in cyberspace.")[344]

The debate is still immature, but there is general agreement that currently cyber defense is not sufficient for most cyber threats and that it requires more investment and development. The amount of ongoing cyber theft, which General Alexander calls "the greatest transfer of wealth in human history," discredits any conclusion to the contrary.[345] The points of disagreement in the debate are about the future direction of defense. However, it appears that with the exception of the minority in the debate that Martin Libicki leads, most concur that cyber

[339] Martemucci, Matteo. Interview by Author. February 26, 2015.
[340] Martemucci, Matteo. Interview by Author. February 26, 2015.
[341] Lin, Herb. "Cyber Conflict and National Security." Transnational Actors and New Forces. Accessed May 21, 2015. http://www.lawfareblog.com/wp-content/uploads/2013/01/cyber-conflict-and-national-security-artjervis-reader-2.pdf.
[342] Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." Foreign Affairs 89, no. 5 (2010). Accessed May 21, 2015. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.
[343] Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy."
[344] Lynn III, William J.
[345] Alexander, Keith. "The Next Wave: An Introduction by General Alexander." National Security Agency and Central Security Service. 2012. Accessed May 21, 2015. https://www.nsa.gov/research/tnw/tnw194/article2.shtml.

defenses will help only up to a certain point.[346] There is neither consensus on what to do at the present other than to invest more into cyber defenses nor is there a plan for the point at which cyber defenses are not effective. In the case of strategic cyber weapons, it appears that the adage of the Prime Minister Stanley Baldwin, "The bomber will always get through," holds just as true in cyberspace as it did in the nuclear age.[347]

Deterrence

The debate over the applicability of deterrence in cyberspace is one of the most vibrant in the communities that study strategic cyber weapons. The debate is unduly complicated by the fact that many writers often group all cyber attacks into one category, failing to capture how the differences between the types of cyber attack affect how deterrence could apply. As a consequence, many writers believe that deterrence is not possible because of attribution issues. Richard Clarke states, "Of all the nuclear-strategy concepts… deterrence theory is probably the least transferable to cyber war," for this reason.[348] William Lynn has a similar view "the traditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack's perpetrator."[349] While attribution is definitely a problem at the level of cyber vandalism and espionage, where there are so many actors that effective attribution and retaliation is simply not feasible, it is less of an issue at the level of strategic cyber weapons because there are fewer players.

---

[346] Although the promise of improving defense at sub-strategic levels is high. "Verizon found in 2011 that 92 percent of the incidents they investigated client sites did not involve high sophisticated methods; 96 percent of the intrusions could have been prevented with simple or intermediate controls; and 86 percent of the intrusions were discovered by a third party."
"A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 37.

[347] "Past Prime Ministers: History of Stanley Baldwin." Gov.uk. Accessed February 4, 2015. https://www.gov.uk/government/history/past-prime-ministers/stanley-baldwin.

[348] N, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.*

[349] Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy."

This makes Martin Libicki's *Cyberdeterrence and Cyberwar* stand out as a touchstone piece in the literature because of its compelling arguments as to why deterrence would not work at the strategic level. Libicki questions the ability for deterrence to work in cyberspace as it did in the nuclear age because of issues of assurance of destruction, repeatability, and inability to disarm, among other factors.[350] James Lewis maintains that because different countries (such as Iran and North Korea) see the costs of operating offensively cyberspace differently than others that "This alone makes a Cold War, one-size fits all deterrent strategy of dubious value."[351] Herb Lin is less skeptical of deterrence and contends that large states have the capability to attribute attacks with enough time, but argues, "there is no logical necessity for restricting a response to this domain."[352] He believes that policymakers should be free to conduct deterrence across the diplomatic, information, military, and economic (DIME) spectrum. The 2013 Defense Science Board report represents the extreme edge of this view, arguing, "U.S. retaliatory response with our nuclear forces is a credible response to a major cyber attack."[353]

Not all believe that cyber deterrence is currently impossible. Secretary Gates said "At the level of the great powers, there is an implicit understanding not to use these weapons against each other because of escalation and retaliation."[354] He noted that there will be significant challenges transitioning from implicit to explicit deterrence adding, "Unlike in the Cold War,

---

[350] Libicki, Martin. "Strategic Cyberwar." 39-75.
[351] Lewis, James A. "Thresholds for Cyberwar."
[352] Off-the-record interviews with government officials, as well as recent public cases of cyber attribution, have confirmed that the U.S. government has this capability. Examples include the Department of Justice convictions of five Chinese military hackers for cyber espionage and the U.S. government attributing the Sony attacks to North Korea. It is more a question of time than feasibility.
Lin, Herb. "Cyber Conflict and National Security."
"U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." U.S. Department of Justice. May 19, 2014. Accessed May 21, 2015. http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
Sanger, David, and Martin Fackler. "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say." The New York Times. January 18, 2015. Accessed May 21, 2015.
[353] "Resilient Military Systems and the Advanced Cyber Threat." Defense Science Board.
[354] Gates, Robert. Interview by Author. March 23, 2015.

there are no rules of the road."[355] Jason Healey agrees in an article entitled "Cyber Deterrence is Working: Dynamics are Similar to the Cold War Nuclear Standoff." He observes, "Large nations have never launched strategically significant disruptive cyber attacks against other large nations" and attributes this phenomenon to "both deterrence by denial and deterrence by punishment."[356] Joseph Nye, a professor at Harvard University, states "Cyberattacks lack the catastrophic dimensions of nuclear weapons attacks, and attribution is more difficult, but interstate deterrence through entanglement and denial still exists."[357]

The debate over the applicability of nuclear-style deterrence in cyberspace is still quite immature. It is nowhere near ready to provide guidance on how to stabilize strategic deterrence in the way that nuclear debate did. As Martin Libicki observed, the debate does not have a Wohlstetter, a Schelling, or a Kahn.[358] Currently, the open track debate has not arrived at a level of coherence that could prove useful in transforming strategic cyber weapons into a strategic deterrent. However, because the debate has begun before the first use of a strategic cyber weapon, it will have a head start for when a large state does use one (unlike the nuclear debate). Alain Enthoven, then a 29 year old civilian strategist, once told an Air Force general during a intense debate on nuclear strategy, "General, I have fought just as many nuclear wars as you

[355] Gates, Robert. Interview by Author. March 23, 2015.
[356] He concludes, "Leaders of the world's most capable cyber nations have assessed, conscious or otherwise, that it is not worth the potential punishment if they unleashed a strategic cyber campaign, an armed attack causing large-scale destruction, loss of life or economic impact similar to that from a military attack." Healey, Jason. "Commentary: Cyber Deterrence Is Working." Defense News. July 30, 2014. Accessed May 21, 2015. http://archive.defensenews.com/article/20140730/DEFFEAT05/307300017/Commentary-Cyber-Deterrence-Working.
[357] Nye, Joseph S. "Diffusion and Cyberpower." In The Future of Power, 146. New York: Public Affairs, 2011.
[358] He also argues that it does not need one.
Libicki, Martin. "Why Cyber War Will Not and Should Not Have Its Grand Strategist."

have."[359] At this point in time, participants in both the closed and open track debates on strategic cyber weapons are very much following in Enthoven's footsteps.

Conclusion

Strategic cyber weapons do not currently qualify as a revolution in military affairs and it is possible that they may never mature into one. They also do not have the strategic deterrent characteristics of nuclear weapons; they are not as destructive, do not have a surety of that destruction, and the debate over their use is still too immature to be of much practical use. As a result, the nuclear-cyber deterrence analogy cannot be made at this time and applying nuclear deterrence doctrine to cyberspace is erroneous and potentially dangerous. However, there is some hope for those who seek for the stabilizing effects of deterrence in cyberspace. Nuclear deterrence came about as a consequence of the combination of the maturation of the nuclear revolution in military affairs in 1945 and the forward-looking debate that shaped the doctrine of how to use nuclear weapons. Because of the highly classified nature of the Manhattan Project, civilian strategists only began to think about nuclear deterrence doctrine after the effects of nuclear weapons became publicly known. In the case of strategic cyber weapons, the theorizing has already started, so it is possible that when a state utilizes the full power of strategic cyber weapons (and it is a 'when'), that stabilizing strategic deterrence could follow shortly after the revolution in military affairs if it occurs because of the pre-existing theoretical groundwork.

[359] Samaan, Jean. "Introduction." In *The RAND Corporation (1989-2009) the Reconfiguration of Strategic Studies in the United States*, 10. New York: Palgrave Macmillan, 2012.

Conclusion: A Presently Unreliable Analogy

> "Nuclear weapons continue to occupy a unique place in global security affairs. No other weapons… match their potential for prompt and long-term damage and their strategic impact."
>
> -General C. Robert Kehler, former Commander of U.S. Strategic Command[360]

"A dirigible, a flying fortress!"[361] The New York Times sang the praises of the world's first flying aircraft carriers, the U.S.S. Macon and U.S.S. Akron, as they "majestically" sailed above the skylines of New York City.[362] These helium-filled, rigid airships had a range of 5,940 nautical miles and were capable of storing, launching, and catching up to five F9C Sparrowhawk 'parasite fighter' aircraft.[363] The U.S. Navy initially intended to use the flying aircraft carriers for reconnaissance over vast swathes of ocean.[364] In the long term, the low flying cost per ton of the massive airships promised to revolutionize the way the U.S. military moved aircraft, missiles, and personnel to and from the battlefront.[365] However, the limitations of the technology restricted their potentially revolutionary impact; both the U.S.S. Macon and the U.S.S. Akron crashed into the ocean because of bad weather.[366] Because these weapons systems failed to mature as a revolution in military affairs, they did not have the revolutionary impact of their sea-floating peers. As a result, the dictionary definition of an aircraft carrier still begins as "a large warship."[367]

---

[360] Miller, Franklin. "A Conversation with General C. Robert Kehler." Council on Foreign Relations. May 30, 2012. Accessed May 14, 2015. http://www.cfr.org/united-states/conversation-general-c-robert-kehler/p35267.
[361] Lyman, Lauren. "Building Our Biggest Flying Fortress." New York Times, April 5, 1931.
[362] "Throngs Here See Ships." New York Times, November 3, 1931.
Smith, Richard K. The Airships Akron & Macon; Flying Aircraft Carriers of the United States Navy. Annapolis: U.S. Naval Institute, 1965. 210.
[363] Smith, Richard K. The Airships Akron & Macon; Flying Aircraft Carriers of the United States Navy. 27.
[364] Smith, Richard K. 210-215.
[365] Scrivner, Jr., Major John. "The Dirigible – A Reconsideration." Air University Review. 1966. Accessed May 14, 2015. http://www.airpower.maxwell.af.mil/airchronicles/aureview/1966/jan-feb/scrivner.html.
[366] Smith, Richard K. 27.
[367] "Aircraft Carrier, n." Oxford English Dictionary. Accessed May 14, 2015.

Strategic cyber weapons, like flying aircraft carriers during the early 1930s, are being heralded as weapons developed during times of peace that could prove revolutionary in times of war. Further, they are being compared to nuclear weapons as a future potential strategic deterrent. Based on the nature of strategic cyber weapons now, the nuclear-cyber deterrence analogy is not appropriate. That may or may not change in the future. It appears that strategic cyber weapons have the potential to eventually either to occupy a similar "unique place" as nuclear weapons or to suffer the ignoble fate of flying aircraft carriers.[368] In hindsight, seventy years after Hiroshima and Nagasaki, the path that nuclear weapons took seems deceptively clear-cut. Where strategic cyber weapons will be in seventy years from now is very much in question during these early stages of development. Using what is known so far, this conclusion will summarize the thesis and its findings, speculate on the future paths of strategic cyber weapons, and recommend avenues for further research to assist in finding the answer.

Summary of the Thesis and Its Findings

Three Revolutions in Military Affairs

This thesis began with an overview of three revolutions in military affairs: the longbow, the tank, and the Offset technologies. In each case, these weapons qualified as a revolution in military affairs because they fulfilled four criteria: an advance in technology, a change in military doctrine, a fundamental change in the balance of power on the battlefield (either by replacing an old power, by creating a new one, or both), and a decisive victory. For the longbow, the technology of the weapon had existed for millennia before the English used it effectively in battle. The key to unlocking the longbow's latent potential lay in the massing of thousands of archers armed with longbows in battle formations. The combination of the longbow's armor-

[368] Miller, Franklin. "A Conversation with General C. Robert Kehler." Council on Foreign Relations. May 30, 2012. Accessed May 14, 2015. http://www.cfr.org/united-states/conversation-general-c-robert-kehler/p35267.

piercing, quick-firing, and long-range capabilities with the English massed formation doctrinal changes meant that infantry could defeat armored knights for the first time in centuries. The English capably demonstrated this revolutionary ability at the Battle of Crecy in 1346 where they inflicted heavy casualties on a much larger French force while sustaining a comparatively small number of casualties.

Unlike the lengthy development time of the longbow, the tank's maturation took only a couple of years to transition from the concept of placing artillery on tractor treads to armored tanks rolling through barbed wire in the First World War. Although the British were the first to deploy the tank on the battlefield, it was the Germans who developed the doctrine to exploit the revolutionary technology. Their careful study of the lessons of the First World War gave them a firm foundation for the decentralized, combined-arms approach to warfare that later became known as Blitzkrieg. The tank greatly reduced the utility of the infantry-orientated trench warfare that dominated the First World War, much to the chagrin of the Maginot Line's supporters. Germany's blindingly fast invasions of countries across Europe, as well as the Allies swift symmetrical response and counter-invasions, unquestionably demonstrated the revolutionary power of the tank and marked the end of a long period of infantry-centric warfare.

The Nazi's lightening warfare later served as a source of comparison for the hundred-hour First Gulf War. Taking advantage of the commercial information technology revolution in the 1970s and 1980s, the U.S. military designed a series of precision-guided munitions, stealth aircraft, sensors, and satellites with the intention of offsetting the conventional advantage of the Soviets in Europe. The Offset technologies led to a doctrine that revolved around the idea of a 'system of systems' that would enable full awareness and shaping of the battlespace. They also made the Soviet military equipment, training, and tactics, which were geared towards winning

battles similar to those of the Second World War, obsolete. The world was unaware of the full potential of this revolution in military affairs until the U.S.-led coalition used Offset technologies and tactics to devastating effect against Saddam Hussein's Soviet-armed and trained military in the early 1990s.

Several key themes emerge from each of these revolutions. First, each military technology overcame the conventional wisdom of the era. The generals who planned to win the last war were those most caught off guard by the revolution in military affairs. The French thought that their knights would easily hack down the lightly armored English archers; the French also thought that their fortifications and infantry-centric tactics would protect them against German armored vehicles; and the Iraqis believed that that Soviet air defenses and tanks would result in thousands of American casualties. Second, the time it takes for a revolution in military affairs to mature varies. In the case of the longbow it took thousands of years, while in the case of the tank and Offset technologies it took several decades. Third, the time in which a revolution in military affairs has a symmetric or asymmetric response and becomes conventionalized also varies. For the longbow, arguably because it contributed to the infantry revolution that lasted until the advent of the tank, it was several hundred years. For the tank, it took just a few years before the Allies responded symmetrically and defeated the Germans with their own tactics and weapons. For the Offset technologies, America's adversaries responded asymmetrically with guerrilla warfare a little more than a decade later in Iraq and Afghanistan.

An additional theme that applies for the first two revolutions in military affairs is that one state can develop a technology, but another can exploit it. While the Welsh developed the longbow for military use, it was the English who used the weapon in massed formations. Likewise, the British invented the tank, but it was the Germans who strategically and tactically

maximized its potential. Some of these lessons can be applied to the nuclear and possible cyber revolutions in military affairs, while others cannot.

The Nuclear Revolution in Military Affairs

Like their revolutionary predecessors, nuclear weapons clearly meet the criteria of a revolution in military affairs. The development of fission and fusion weapons mark a discrete increase in the destructiveness of man-made weapons. The wide array of changes in military doctrine, both by nuclear and non-nuclear weapons states, demonstrates the revolutionary impact of nuclear weapons on tactical and strategic thinking. This widespread international recognition of a new source of military capability indicates the shift in the balance of power on the battlefield that it caused. America's use of nuclear weapons on Hiroshima and Nagasaki represent such one-sided victories that they are not typically thought of as battles. However, nuclear weapons are also different from their peers in several respects, two of them technological and the other theoretical. The technological aspects of nuclear weapons that set them apart from any other revolution in military affairs are the sheer destructiveness of each weapon and the assuredness of that destruction. Never before have humans had the ability to destroy the entire species in such a short time. Further, the delivery revolution meant that it was also effectively impossible to prevent or avoid that destruction. The theoretical aspect is that these weapons prompted a debate that resulted in an entirely new way of thinking about a single weapons system. Namely, that a single weapon could result in the outcome of strategic deterrence.

The Strategic Cyber Revolution in Military Affairs

Currently, strategic cyber weapons neither constitute a revolution in military affairs nor possess the strategic deterrent characteristics of nuclear weapons. Strategic cyber weapons are an indisputable breakthrough in technology. The ability to near instantly launch an incapacitating,

non-physical intercontinental attack another state's critical infrastructure simply was not possible before the invention of computers and cyberspace. The flurry of doctrinal revisions from the establishment of U.S. Cyber Command to *The Department of Defense Cyber Strategy* of 2015 show how the U.S. is urgently trying to stay abreast of the advancing technology. However, unlike other revolutions in military affairs, strategic cyber weapons have neither fundamentally shifted the balance of power on the battlefield nor produced a decisive victory. Although there is broad knowledge about the existence of these weapons, it has not perceptibly changed the current conduct of battle or the behavior of states in international affairs. Further, because strategic cyber weapons have never been used, they have never precipitated a decisive victory. Having met only two of the four standards of a revolution in military affairs, strategic cyber weapons do not qualify as one. Consequently, nuclear and cyber weapons cannot be compared on the basis of revolution in military affairs at the present.

Strategic cyber weapons also do not yet have the characteristics that made nuclear weapons a strategic deterrent. From what is publicly known about strategic cyber weapons, they do not have the ability to wreak the level of destruction of a single nuclear weapon. As Jim Lewis starkly states, "two MIRV'd ICBMs to the East Coast would kill 42 million people, tell me cyber weapons can do the same."[369] Strategic cyber weapons also do not have a demonstrated ability to assure destruction, which is essential for the credibility of deterrent threats. There is a lot of uncertainty both about the ability of strategic cyber weapons to be able to deliver their payloads and then for the payloads to be able to inflict the intended damage. Finally, the debate is immature, at least on the unclassified side. It is unclear who are currently the Bernard Brodies or the Thomas Schellings or if they exist at all. As General Michael Hayden said, "No one has

[369] Lewis, Jim. Interview by author. March 18, 2015.

yet begun to write the *On Thermonuclear War* for cyber conflict."[370] Consequently, analogizing nuclear and cyber deterrence is a mistake for the present. Policy based on the assumption that the analogy is correct could lead to dangerous outcomes.

The Future of the Analogy

While the nuclear-cyber deterrence analogy is not appropriate at the present, it could in the future. There are three potential pathways that strategic cyber weapons could take going forward. Strategic cyber weapons will either become a revolution in military affairs and a strategic deterrent (like nuclear weapons), a revolution in military affairs but not a strategic deterrent (like the tank), or not become a revolution in military affairs (like the flying aircraft carrier). Because it is hard to imagine how a weapon could become a strategic deterrent without fulfilling the criteria of a revolution in military affairs, it is not discussed in the conclusion.

A Revolution in Military Affairs and a Strategic Deterrent

There are two remaining criteria that strategic cyber weapons need to fulfill in order to become a revolution in military affairs: they need to fundamentally change the balance of power on the battlefield and they need to produce a decisive victory. Both require the use of strategic cyber weapons on the battlefield. Most practitioners and observers believe that these weapons would only be used in the event of a major conflict or period of heightened tensions, as was the case with nuclear weapons.[371] Director James Clapper predicts, "Advanced cyber actors – such as Russia and China – are unlikely to launch such a devastating attack against the United States

[370] Hayden, Michael. Interview by author. March 10, 2015.

[371] If nuclear weapons had been developed during the interwar period (all points aside from how they would have affected geopolitics and the outcomes of World War Two) it is unlikely that they would have been used immediately either.
Rogers, Michael. "Hearing on Cybersecurity Threats."
Hanrahan, Mark. "NSA Chief Warns China Could Launch Cyber Attack Against US Power, Water, Aviation Systems." International Business Times. November 20, 2014. Accessed May 14, 2015. http://www.ibtimes.com/nsa-chief-warns-china-could-launch-cyber-attack-against-us-power-water-aviation-1727326.

outside of a military conflict or crisis that they believe threatens their vital interests."[372] Strategic cyber weapon use would most likely occur either during a period of conflict between the U.S. and China or the U.S. and Russia for three reasons. The first is because these are currently the only countries capable of carrying out an attack that would impose unacceptable costs on an adversary. The second is because Russia or China would benefit from asymmetrically responding to the U.S. conventional military advantage. The third is because the U.S. is one of the most vulnerable countries in the world to cyber attack.[373] While it is possible for it to happen during a conflict between any of these three countries and a third country, given the current cost and unsure capabilities of a strategic cyber weapon, it is likely that the U.S., Russia, or China would instead use cheaper and proven conventional weapons.

A major shift in the balance of power on the battlefield could take many forms, but if one of the outcomes were to be strategic deterrence then it would likely resemble the shift in the balance of power that nuclear weapons caused. For instance, after the first (or second or third) use of strategic cyber weapons, large states would launch massive crash programs to invest in offensive cyber weaponry (on a scale much larger than before), smaller states would push for an international regime to regulate their use, and the nascent debate over their use would become much broader, more intense, and be instrumental in the establishment of norms in cyberspace. A decisive victory could take a number of forms, and while the end-state devastation may be comparable to nuclear weapons, the method and time of delivery would be different. In the

[372] Clapper, James. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community."
[373] William Lynn states, "The U.S. government's digital infrastructure now gives the United States critical advantages over any adversary, but its reliance on computer networks also potentially enables adversaries to gain valuable intelligence about U.S. capabilities and operations, to impede the United States' conventional military forces, and to disrupt the U.S. economy."
Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." Foreign Affairs 89, no. 5 (2010). Accessed May 21, 2015. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

absence of an official acknowledgement or release of information about what the full extent of a strategic cyber attack would be, there has been much speculation.[374]

A decisive victory that would result in the outcome of strategic deterrence would have to impose unacceptable costs on the victim state. Given what is known right now from open source materials and interviews, the use of strategic cyber weapons would likely take place over weeks or even months. Christopher Painter, the first Cyber Coordinator for the State Department, said, "it would require sustained action for an adversary to take down a network for a period of time which would be really debilitating, but it is possible and something that we need to guard against and be concerned about."[375] Such an attack also would largely target what the Department of Homeland Security defines as critical infrastructure sectors along with military targets to inflict maximum destruction.[376] A well-resourced, determined adversary such as China or Russia could be capable of neutralizing American centers of gravity in most or all of these sectors. The result could be devastating. First order casualties could include deaths from the release of hazardous chemicals and radioactive materials from factories and plants near or in urban areas, from the unrestrained release of dam waters, as well as from derailed trains, car accidents, and downed civilian airliners. These first order effects could be compounded by the inability of emergency services and hospitals to effectively respond. While these effects might result in death tolls in the thousands or possibly hundreds of thousands, they would not be as severe as the second and third order effects.

---

[374] N, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.*

[375] He also was formerly the Senior Director for Cybersecurity Policy in the National Security Staff.
Painter, Christopher. Interview with author. March 30, 2015.

[376] Sectors include the Chemical, Commercial Facilities (Public Assembly, Sports Leagues, Lodging, etc.), Communication, Critical Manufacturing (Primary Metal, Machinery, Electrical Equipment, Transportation Equipment Manufacturing), Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Sector Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater System sector.
"Critical Infrastructure Sectors." Department of Homeland Security. Accessed May 14, 2015. http://www.dhs.gov/critical-infrastructure-sectors.

Strategic cyber attacks with irreversible effects on agricultural irrigation, processing, and storage facilities, as well as on public water distribution systems and wastewater treatment facilities could have obvious effects such as the spread of famine, disease, and dehydration, but also less obvious ones such lack of an ability to fight fires. These effects could be exacerbated by an incapacitated government's inability to form a cohesive response and communicate it to the population (or for the population to communicate it amongst itself). Additionally, the U.S. may not be able to transport key resources around the country (such as medicine, gasoline, and food), a compromised electrical grid, and a crashed financial services sector that could eliminate savings of Americans. The combination of all of these effects would likely weaken American morale and confidence in the government and other public institutions, making it difficult to maintain order and possibly leading to anarchy. In a worse case scenario, the second and third order attacks would resemble a mix of the Great Depression, the 1973 Oil Embargo, and the Northeast Blackout of 2003. Martin Libicki believes that a strategic cyber attack could not have more deleterious effects than "a universal trade embargo" or "prevent the emergence of an economy as modern as the U.S. economy was circa 1960."[377] However if the U.S. sustained a strategic cyber attack, its economy could more likely resemble something out of the Middle Ages.[378]

---

[377] Libicki, Martin. "Strategic Cyberwar." In *Cyber Deterrence and Cyber War*, 123.

[378] In a National Defense University report entitled, "The Future of Weapons of Mass Destruction: Their Nature and Role in 2030," John Caves and Seth Carus (the senior and deputy director of Center for the Study of Weapons of Mass Destruction, respectively) wrote, "New forms of WMD—beyond chemical, biological, radiological, and nuclear weapons—are unlikely to emerge by 2030, but cyber weapons will probably be capable of inflicting such widespread disruption that the United States may become as reliant on the threat to impose unacceptable costs to deter large-scale cyber attack as it currently is to deter the use of WMD…Societies in the 21st century will become increasingly vulnerable to forms of disruption, and such disruption may be as strategically important as destruction. They will become more dependent on networked information systems as commercial and governmental entities alike are driven to achieve greater efficiencies"
Caves, John P., and W. Seth Carus. "The Future of Weapons of Mass Destruction: Their Nature and Role in 2030." National Defense University. June 1, 2014. Accessed May 22, 2015. http://wmdcenter.dodlive.mil/files/2014/07/CSWMD_OccationalPaper-10.pdf.

The outcome of strategic deterrence from a strategic cyber revolution in military affairs depends on several key trends. The increasing reliance on cyber-dependent technology around the globe and the direction of improvements in strategic cyber weapons are the primary drivers of these trends. The potential destructiveness of strategic cyber weapons is set to increase as horizontal and vertical reliance on cyber-dependent technologies grows. Increasing the amount of automation in transportation, such as transitioning to self-driving automobiles and planes, could increase the first order effects of a strategic cyber weapon.[379] Similarly, computer-related improvements for the management of wastewater could put more people at risk of second and third order effects. The increasing destruction of strategic cyber weapons is important for making their deterrent threat unacceptable – an unfortunate, but necessary condition for stable strategic deterrence.

As strategic cyber weapons become more sophisticated, the assuredness of their destruction will improve. Adversaries will have less cause to either doubt each other's ability to deliver cyber attacks or for those attacks to inflict the intended harm. After large states demonstrate their strategic cyber weapons capabilities, this will be essential for stable strategic deterrence. As Christopher Painter stated, "We don't know each other's capabilities and it can't be a guessing game."[380] As cyber defenses grow more robust, they could reduce the 'noise' of lower level cyber attacks and exclude lesser states and non-state actors from being able to inflict unacceptable levels of damage. This would maintain a manageable number of actors with strategic cyber capabilities in terms of strategic deterrence. Furthermore, cyber technology advances could help the U.S. and other countries to reduce the level of doubt in attribution

[379] Santens, Scott. "Self-Driving Trucks Are Going to Hit Us Like a Human-Driven Truck." Medium. May 14, 2015. Accessed May 22, 2015. https://medium.com/basic-income/self-driving-trucks-are-going-to-hit-us-like-a-human-driven-truck-b8507d9c5961.
[380] Painter, Christopher. Interview with author. March 30, 2015.

capabilities, which would assure that retaliatory strikes would be correctly targeted. Finally, the use of cyber weapons would also dramatically change the nature of the debate surrounding their use to become more focused and practical. All of these trends could result in the creation and eventual stabilization of strategic deterrence.[381]

Revolution in Military Affairs, but not a Strategic Deterrent

It is also feasible for strategic cyber weapons to become a revolution in military affairs, but not develop into a strategic deterrent. This path would again largely depend on the type of initial use of strategic cyber weapons. Rather than creating a new power (as nuclear weapons did), strategic cyber weapons could displace an old power on the battlefield. For instance, if the Russians could turn on its head the Offset revolution in military affairs by removing the advantages of the Offset technologies and their successors (unmanned aerial vehicles, the B-3 bomber, etc.) with strategic cyber weapons, then they could equalize or regain a conventional advantage that could prove decisive in the moment of battle. This would not necessarily prove to be a strategic deterrent to the U.S., as the costs imposed would not be unacceptable, but it would be a severe set back for American armed forces. Ultimately, it is not possible to know now where, who, or when a state will fully exploit the revolutionary potential of strategic cyber weapons. There are many potential ways in which strategic cyber weapons could revolutionize warfare. As Admiral Cecil Haney said, "I am not sure we have discovered yet [what is revolutionary] in the application of cyber in warfare."[382]

While strategic cyber weapons may come to be a revolution in military affairs, they will not necessarily become a strategic deterrent. Trends in cyber technology use and improvement could bode negatively for strategic cyber weapons' potential as a deterrent just as easily as they

[381] It is also possible that strategic cyber weapons could create strategic deterrence in another way than the nuclear template; it is just currently not clear how.
[382] Haney, Cecil. Interview by author. January 24, 2015.

could bode positively. Improving cyber technology may lower the costs of what it takes to wield a strategic cyber weapon, opening the door to not just smaller states, but non-state actors as well to inflict unacceptable costs upon a state. As Kirk McConnell, a professional staff member on the Senate Armed Services Committee, said, "The water line is being lowered."[383] In that reality it would much more difficult, if not impossible, to effectively deter cyber attacks due to the number of strategic cyber actors. Cyber defenses are also nowhere near the point of achieving their potential. It could be possible that in the future they will prevent any actor from effectively carrying out a strategic cyber attack. This, too, would greatly weaken prospects for deterrence, as it would limit the ability for the assuredness of destruction from strategic cyber weapons. Finally, if the open debate does not find its key strategists, it could remain perpetually immature and never contribute to the stabilization of strategic deterrence.

Not a Revolution in Military Affairs, not a Strategic Deterrent

It is entirely possible that strategic cyber weapons could become a failed revolution in military affairs, partially meeting the criteria, but not meeting all of them. Although there is much speculation about the potential dangers of a cyber attack on U.S. critical infrastructure, it is impossible to truly know if strategic cyber weapons are capable of inflicting the damage imagined until it happens. It is fully within the realm of possibility that strategic cyber weapons constitute an overblown threat and that global leaders are overzealously promoting it in order to gain support for additional investment in offensive cyber programs. It is also conceivable that the world has seen the full extent of these weapons' capabilities and that Stuxnet demonstrated cyber weapon's maximum potential when it disabled centrifuges at an enrichment plant. These weapons may never change the balance of power on the battlefield, produce a decisive victory, or mature as a revolution in military affairs. Further, they may not become a strategic deterrent.

[383] McConnell, Kirk. Interview by author. March 19, 2015.

If strategic cyber weapons are incapable of inflicting unacceptable damage, if they are incapable of assuring that destruction for a variety of reasons, or if the debate over their use never matures, then they cannot become a strategic deterrent.

Further Research

While this project focused on the outcome of strategic deterrence, the nuclear-cyber analogy is broad and has many facets. Several particularly promising avenues for further research include an evaluation of the nuclear-cyber analogy in terms the development of norms (non-proliferation and non-use), arms control, and terrorism. It is unclear at the present whether norms have or will develop in cyberspace on the use of strategic cyber weapons. At the dawn of the nuclear age, it was also unclear if norms were going to develop for nuclear weapons. Learning from the lessons of that time for how to take further norm-promoting steps today in terms of the drafting of international law, directing the tenor of the broader debate, and focusing state leaders could be invaluable. An equally important and related topic is arms control. How to manage the testing, spread, and abilities of strategic cyber weapons to ensure the stability of strategic deterrence could prove to be essential. The challenges of verification and the shifting nature of the arms control debate could find interesting direct and indirect analogues in the cyber world. The analogy to nuclear terrorism could also be a worthwhile research pursuit, especially in light of the direction that strategic cyber weapons may be taking. If any non-state actor were capable of inflicting unacceptable levels of damage through cyber means (perhaps not on the same level as a state, but still considerable) then it would be very important to learn from what best practices exist about nuclear terrorism. These are but three potential further fields of study in

the nuclear-cyber analogy. There are, of course, many other aspects of the analogy and other entire analogies to further investigate.[384]

Additionally, it is also important to periodically revisit the nuclear-cyber deterrence analogy as the technology and trends of strategic cyber weapons develop further. It is possible that they will be used, but it will not be evident which of the three pathways strategic cyber weapons weapons is following. Unlike nuclear weapons, strategic cyber weapons are difficult to neatly categorize. As President Barack Obama observed, "With nuclear weapons there is a binary. Either there are no nuclear explosions or there are big ones and it is a real problem. In cyberspace, there are all sorts of gradations."[385] Consequently, even after the use of strategic cyber weapons, there is significant potential for the analogy to be misinterpreted as it often is now. At the same time, it will also be crucial to know if the analogy is applicable when it is.

Final Words

President Abraham Lincoln once said, "we know nothing of what will happen in the future, but by the analogy of experience."[386] At the present, nuclear weapons remain unique. Indeed, the longbow, the tank, and the Offset technologies also continue to be without a cyber counterpart. Strategic cyber weapons neither qualify as a revolution in military affairs nor do they possess the characteristics necessary to make them a strategic deterrent. While it is erroneous and possibly dangerous to suggest that the nuclear-cyber deterrence analogy is currently correct, that may change in the future. Strategic cyber weapons have the potential to be extremely dangerous and could significantly impact the lives of everyone on the planet. If it is

[384] For example, how should the U.S. conceive of strategic cyber deterrence towards nations with limited cyber-dependence (such as North Korea for example)? How does strategic cyber deterrence fit into the broader spectrum of deterrence and cross-domain deterrence? How should the U.S. determine its thresholds for strategic cyber attack? On the last question: "Secretary Panetta vaguely stated that a "cyber 9/11" was a "red line," but there has been little else forthcoming from the administration on thresholds."
Sanger, David, and Thom Shanker. "Broad Powers Seen for Obama in Cyberstrikes."
[385] Obama, Barack. Interview by author. February 13, 2015.
[386] Lincoln, Abraham. Abraham Lincoln: Speeches and Writings. New York: Library of America, 1989. 50.

possible to prevent their use through a framework that already exists, then it should be used. If it is not, then it is necessary to think of another way to handle the threat.

Works Cited

"1945: Japan Signs Unconditional Surrender." BBC. September 2, 1945. Accessed May 21, 2015. news.bbc.co.uk/onthisday/hi/dates/stories/september/2/newsid_3582000/3582545.stm.

"A Brief History of US Cyber Conflict. In A Fierce Domain: Conflict in Cyberspace, 1986 to 2012." 21. Cyber Conflict Studies Association, 2013.

Abella, Alex. "The Wages of Sin." In *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*, 43. Boston: Mariner Books, 2009.

"Airborne Laser Test Bed Successful in Lethal Intercept Experiment." U.S. Missile Defense Agency. February 11, 2010. Accessed May 22, 2015. http://www.mda.mil/news/10news0002.html.

"Aircraft Carrier, n." Oxford English Dictionary. Accessed May 14, 2015.

Alexander, Bevin. "The Korean War." In *The Strange Connection: U.S. Intervention in China, 1944-1972*, 108-109. New York: Greenwood Press, 1992.

Alexander, Keith. "The Next Wave: An Introduction by General Alexander." National Security Agency and Central Security Service. 2012. Accessed May 21, 2015. https://www.nsa.gov/research/tnw/tnw194/article2.shtml.

Allaire, James, and Rosemary Broughton. "Catholic Worker Movement: Dorothy Day." Catholic Worker Movement. Accessed May 21, 2015. http://www.catholicworker.org/dorothyday/ddbiographytext.cfm?Number=3.

"Americans Killed by Atomic Bomb to Be Honored in Hiroshima." AllGov. June 4, 2009. Accessed May 21, 2015. http://www.allgov.com/news/us-and-the-world/americans-killed-by-atomic-bomb-to-be-honored-in-hiroshima?news=838959.

"Announcing Publication of State of Doom: Bernard Brodie, the Bomb and the Birth of the Bipolar World. Program for Culture and Conflict Studies at NPS." Accessed November 12, 2014. http://www.nps.edu/Programs/CCS/WebJournal/Article.aspx?ArticleID=107.

"Appendix A: After the Fall." Federation of American Scientists. Accessed November 12, 2014. http://fas.org/sgp/library/moynihan/appa9.html.

Applegate, Scott. "The Dawn of Kinetic Cyber." NATO Cooperative Cyber Defense Center of Excellence. Accessed March 16, 2015. https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf.

Assante, Michael. "America's Critical Infrastructure Is Vulnerable To Cyber Attacks." Forbes.

November 11, 2014. Accessed May 21, 2015. http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/.

Ayson, Robert. *Thomas Schelling and the Nuclear Age: Strategy as Social Science*. New York: Routledge, 2004. 56-58.

Baker, Graeme. "Schoolboy Hacks into City's Tram System." The Telegraph. January 11, 2008. Accessed March 16, 2015. http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

"Balance of Terror." In The Norton Dictionary of Modern Thought, 65. 3rd ed. Great Britain: W. W. Norton & Company, 1999.

"Ballistic Missiles." Federation of American Scientists. Accessed January 21, 2015. http://www.fas.org/spp/military/program/smc_hist/SMCHOV8.HTM.

"Baring A-Bomb Figures Asked." The Spokesman-Review, June 29, 1953. Accessed May 21, 2015. https://news.google.com/newspapers?nid=1314&dat=19530629&id=aC9WAAAAIBAJ&sjid=IuYDAAAAIBAJ&pg=7306,6991225&hl=en.

Barron, James. "THE BLACKOUT OF 2003: The Overview; POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN 8 STATES AND CANADA; MIDDAY SHUTDOWNS DISRUPT MILLIONS." The New York Times. August 14, 2003. Accessed April 29, 2015. http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html.

Baucom, Donald R. "Origins of the Strategic Defense Initiative: Ballistic Missile Defense, 1944-1983." Strategic Defense Initiative Organization. December 1, 1989. Accessed January 20, 2015. http://www.dtic.mil/dtic/tr/fulltext/u2/a242465.pdf.

Bencivenga, Jim. "Aboard a Nuclear Sub." The Christian Science Monitor. October 14, 1982. Accessed May 15, 2015. http://www.csmonitor.com/1982/1014/101430.html.

Bernstein, Barton J. "Compelling Japan's Surrender without the A-bomb, Soviet Entry, or Invasion: Reconsidering the Us Bombing Survey's Early-surrender Conclusions." Journal of Strategic Studies 18, no. 2 (1995): 101-48.

Bernstein, Sharon, and Andrew Blankstein. "Key Signals Targeted, Officials Say." Los Angeles Times. January 9, 2007. Accessed March 16, 2015. http://articles.latimes.com/2007/jan/09/local/me-trafficlights9.

"Bessmertnykh Talks About Soviet-Built Weapons." Accessed December 8, 2014. http://www.friends

partners.org/friends/news/omri/1991/01/910118.html(opt,mozilla,unix,russian,koi8,new).

Biddle, Stephen. "Victory Misunderstood: What the Gulf War Tells Us about the Future of Conflict." *International Security*: 139-79.

Bix, Herbert P. "Hiroshima in History and Memory: A Symposium, Japan's Delayed Surrender: A Reinterpretation." Diplomatic History: 197-225.

"Blitzkrieg (Lightning War)." United States Holocaust Memorial Museum. June 20, 2014. Accessed May 22, 2015. http://www.ushmm.org/wlc/en/article.php?ModuleId=10005437.

Borden, William Liscum. "The Certainty of War Amidst Anarchy." In *There Will Be No Time: The Revolution in Strategy*, 24-32. New York: Macmillan Company, 1946.

Brenner, Joel. "Between War and Peace." In *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, 145. New York: Penguin Press, 2011.

Bright, Christopher J. "The Origins of Nuclear Air Defense Arms." In *Continental Defense in the Eisenhower Era: Nuclear Antiaircraft Arms and the Cold War*. 22. New York: Palgrave Macmillan, 2010.

Broad, William, John Markoff, and David Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." The New York Times. January 15, 2011. Accessed May 21, 2015. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

Brodie, Bernard, and Fawn McKay Brodie. *From Crossbow to H-bomb*. Bloomington: Indiana University Press, 1973. 37-40.

Brodie, Bernard, and Frederick Sherwood Dunn. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and, 1946.

Brodie, Bernard. "Is There Defense?" In Strategy in the Missile Age, 185. Princeton, N.J.: Princeton University Press, 1959.

Bronk, Christopher. "Hacks on Gas: Energy, Cybersecurity, and U.S. Defense." James A. Baker III Institute for Public Policy. February 5, 2014. Accessed May 21, 2015. http://bakerinstitute.org/research/hacks-gas-energy-cybersecurity-and-us-defense/.

Burns, Richard Dean, and Joseph M. Siracusa. "Vying for an A-bomb: World War II Contestants." In *A Global History of the Nuclear Arms Race: Weapons, Strategy, and Politics*, 1-5.

Bush, George H. W. "This Day in History: George H.W. Bush Announces End of Gulf War."

Miller Center. February 27, 1991. Accessed May 21, 2015. http://millercenter.org/ridingthetiger/george-h.w.-bush-announces-end-of-gulf-war.

Butler, Amy. "Lights Out For The Airborne Laser." Lights Out For The Airborne Laser. December 21, 2011. Accessed May 22, 2015. http://aviationweek.com/awin/lights-out-airborne-laser.

Bynes, Eric. "The Line." *Intech*, 2007, 43. Accessed December 3, 2014. http://www.mtl-inst.com/images/uploads/datasheets/Intech_Mar_07_Net_security_(The_Line).pdf.

Cantelon, Philip L. "The Nuclear Age." In *The American Atom: A Documentary History of Nuclear Policies from the Discovery of Fission to the Present*, 3-10. 2nd ed. Philadelphia: University of Pennsylvania Press, 1991.

Caron, George Robert, and Charlotte Meares. "Chapter 1." In *Fire of a Thousand Suns: The George R. "Bob" Caron Story, Tail Gunner of the Enola Gay*, 1-3. Westminister, Colo.: Web Pub., 1995.

Caron, George. "Enola Gay - Tail Gunner - Bob Caron Radio Interview - 1953." YouTube. January 1, 1953. Accessed January 27, 2015. https://www.youtube.com/watch?v=ot80m7XWSz4.

Carter, Ashton B. "Keeping America's Military Edge." Foreign Affairs 80, no. 1 (2001): 90. Accessed May 21, 2015. https://www.foreignaffairs.com/articles/united-states/2001-01-01/keeping-americas-military-edge.

Cartwright, James. "Cyber Operations Lexicon." Department of Defense. Accessed April 29, 2015. http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

Caves, John P., and W. Seth Carus. "The Future of Weapons of Mass Destruction: Their Nature and Role in 2030." National Defense University. June 1, 2014. Accessed May 22, 2015. http://wmdcenter.dodlive.mil/files/2014/07/CSWMD_OccationalPaper-10.pdf.

Chapman, Gary. "An Introduction to the Revolution in Military Affairs." XV Amaldi Conference on Problems in Global Security. September 1, 2003. Accessed December 4, 2014. http://www.lincei.it/rapporti/amaldi/papers/XV-Chapman.pdf.

"Chapter 17: U.S. Missile Systems." Air University. Accessed January 20, 2015. http://www.au.af.mil/au/awc/space/primer/us_missile_systems.pdf. 17-6.

Cieply, Michael, and Brooks Barnes. "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm." The New York Times. December 30, 2014. Accessed March 16, 2015. http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

Cimbala, Stephen J. "Alternative Nuclear Regimes." In *Nuclear Weapons and Cooperative Security in the 21st Century: The New Disorder*, 11. London: Routledge, 2010.

Citino, Robert. "Technology in the Persian Gulf War of 1991." The Gilder Lehrman Institute of American History. 2015. Accessed May 21, 2015. http://www.gilderlehrman.org/history-by-era/facing-new-millennium/essays/technology-persian-gulf-war-1991.

Clapper, James. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community." Senate Select Committee on Intelligence. March 12, 2013. Accessed March 16, 2015. http://www.intelligence.senate.gov/130312/clapper.pdf.

Clarke, Richard A., and Robert K. Knake. Cyber War: The next Threat to National Security and What to Do about It. New York: Ecco, 2012. 67.

"Complete List of All U.S. Nuclear Weapons." Nuclear Weapons Archive. October 14, 2006. Accessed January 27, 2015. http://nuclearweaponarchive.org/Usa/Weapons/Allbombs.html.

"Critical Infrastructure Sectors." Department of Homeland Security. Accessed May 14, 2015. http://www.dhs.gov/critical-infrastructure-sectors.

"Critical Infrastructure: Threats and Terrorism." Federation of American Scientists. August 6, 2006. Accessed May 21, 2015. https://fas.org/irp/threat/terrorism/sup2.pdf.

"Cyber Weapons vs. Nuclear Weapons." Center for Strategic and International Studies. July 26, 2011. Accessed March 16, 2015. http://csis.org/blog/cyber-weapons-vs-nuclear-weapons.

"Cyberspace as a Warfighting Domain: Policy, Management, and Technical Challenges to Mission Assurance." House of Representatives Committee on Armed Services. March 5, 2009. Accessed March 16, 2015. http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57218/pdf/CHRG-111hhrg57218.pdf.

De Maizière, Thomas. "Die Lage Der IT-Sicherheit in Deutschland 2014." Federal Office for Information Security. 2014. Accessed May 21, 2015. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.

DeBruyne, Nese, and Anne Leland. "American War and Military Operations Casualties: Lists and Statistics." Congressional Research Service. January 2, 2015. Accessed May 21, 2015. https://www.fas.org/sgp/crs/natsec/RL32492.pdf.

DeGroot, Gerard J. "Embracing Armageddon." In *The Bomb: A Life*, 153. Cambridge, Mass.: Harvard, 2005.

"Deterrence & Survival in the Nuclear Age." Security Resources Panel of the Science Advisory Committee. November 7, 1957. Accessed November 12, 2014. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB139/nitze02.pdf.

"Deterrence." Department of Defense Dictionary of Military Terms. Accessed April 29, 2015. http://www.dtic.mil/doctrine/dod_dictionary/data/d/3763.html.

Drell, Sidney D., and James E. Goodby. "Nuclear Deterrence in a Changed World." Arms Control Today. Accessed February 4, 2015. http://www.armscontrol.org/act/2012_06/Nuclear_Deterrence_in_a_Changed_World.

"Early Developments." Federation of American Scientists. Accessed November 12, 2014. http://fas.org/nuke/guide/usa/icbm/early.htm.

"Eisenhower Approves NSC 162/2." History.com. Accessed November 12, 2014. http://www.history.com/this-day-in-history/eisenhower-approves-nsc-1622.

Eisenhower, Dwight D. "Dwight D. Eisenhower: Radio Address to the American People on the National Security and Its Costs." presidency.ucsb.edu. May 19, 1953. Accessed November 12, 2014.

Eisenhower, Dwight D. "The Strategy of Massive Retaliation." Freerepublic.com. January 12, 1954. Accessed November 14, 2014. http://www.freerepublic.com/focus/f-news/1556858/posts.

"Enola Gay Crew." Atomic Archive. Accessed January 27, 2015. http://www.atomicarchive.com/Photos/Tinian/image1.shtml.

Ernest Rutherford. Chemical Heritage Foundation. Accessed January 27, 2015. http://www.chemheritage.org/discover/online-resources/chemistry-in-history/themes/atomic-and-nuclear-structure/rutherford.aspx.

"Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations." U.S.-Canada Power System Outage Task Force. April 1, 2004. Accessed April 29, 2015. 25. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

Foley, Robert T. "Blitzkrieg." BBC News. March 30, 2011. Accessed May 22, 2015. http://www.bbc.co.uk/history/worldwars/wwtwo/blitzkrieg_01.shtml.

Forsythe, Michael. "Chinese General With Dempsey Compares Cyber-Attack to Nuke." Bloomberg.com. April 22, 2013. Accessed March 16, 2015. http://www.bloomberg.com/news/articles/2013-04-22/china-seeks-to-forge-new-type-of-military-relationship-with-u-s-.

"Fort Schiesseck." 100th Infantry Division. Accessed May 4, 2015. http://www.100thww2.org/fortsch1.html.

"Franco-German Armistice: 1940. Encyclopedia Britannica Online." Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/216964/Franco-German-Armistice.

Freedman, Lawrence D. "Nuclear Strategy: Alternatives to Assured Destruction." Encyclopedia Britannica Online. Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/421797/nuclear-strategy/52990/Alternatives-to-assured-destruction.

Freedman, Lawrence, and Efraim Karsh. *The Gulf Conflict 1990-1991: Diplomacy and War in the New World Order*. Princeton, N.J.: Princeton University Press, 1994. 409.

Frieser, Karl, and John T. Greenwood. *The Blitzkrieg Legend: The 1940 Campaign in the West.* Annapolis, Md.: Naval Institute Press, 2005. 151.

Froissart, Jean. "The Campaign of Crecy: Of the Battle of Crecy between the King of England and the French King." The Chronicles of Froissart. 1909. Accessed May 21, 2015. http://www.bartleby.com/35/1/110.html.

Gaddis, John Lewis. *Strategies of Containment a Critical Appraisal of American National Security Policy during the Cold War*. Rev. and Expanded ed. New York: Oxford University Press, 2005. 169.

Galdi, Theodor. "Revolution in Military Affairs? Competing Concepts, Organizational Responses, Outstanding Issues." Congressional Research Service. January 1, 1995. Accessed December 2, 2014. http://www.iwar.org.uk/rma/resources/rma/crs95-1170F.htm.

Geers, Kenneth. "Cyberspace and the Changing Nature of Warfare." SC Magazine. August 27, 2008. Accessed March 16, 2015. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.

Geers, Kenneth. "Data Analysis and Research Results." In *Strategic Cyber Security*, 138. Tallinn, Estonia: CCD COE Publication, 2011. https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf.

George, Alexander L., and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press, 1974. 38.

Gibson, Jane, and Kenneth Kemmerly. "Intercontinental Ballistic Missiles." Air University. Accessed January 27, 2015. http://www.au.af.mil/au/awc/space/au-18-2009/au-

18_chap18.pdf.

Gordon, Michael. "1991 Victory Over Iraq Was Swift, but Hardly Flawless." The New York Times. December 31, 2012. Accessed May 4, 2015. http://www.nytimes.com/2013/01/01/world/middleeast/victory-over-iraq-in-1991-was-swift-but-flawed.html.

Gorman, Siobhan, and Julian E. Barnes. "Cyber Combat: Act of War." Wall Street Journal. May 31, 2011. Accessed May 21, 2015. http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

Greenemeier, Larry. "Heart-Stopper: Could Hackers Hit Pacemakers, Other Medical Implants?" Scientific American. March 14, 2008. Accessed March 16, 2015. http://www.scientificamerican.com/article/heart-stopper-med-device-hack/.

Grubb, Ben. "Fatal Risk at Heart of Lax Security." The Sydney Morning Herald. November 6, 2012. Accessed March 16, 2015. http://www.smh.com.au/digital-life/consumer-security/fatal-risk-at-heart-of-lax-security-20121105-28ore.html

"Hack Attack Causes 'Massive Damage' at Steel Works." BBC News. December 22, 2014. Accessed May 21, 2015. http://www.bbc.com/news/technology-30575104.

Hakkarainen, Pasi. "Cyber Weapon System." In *Cyber Weapon Target Analysis*, 43.

Hanrahan, Mark. "NSA Chief Warns China Could Launch Cyber Attack Against US Power, Water, Aviation Systems." International Business Times. November 20, 2014. Accessed May 14, 2015. http://www.ibtimes.com/nsa-chief-warns-china-could-launch-cyber-attack-against-us-power-water-aviation-1727326.

Hasegawa, Tsuyoshi. Racing the Enemy: Stalin, Truman, and the Surrender of Japan. Cambridge, Mass.: Belknap Press of Harvard University Press, 2005.

Healey, Jason. "A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 29-30. Cyber Conflict Studies Association, 2013.

Healey, Jason. "Commentary: Cyber Deterrence Is Working." Defense News. July 30, 2014. Accessed May 21, 2015. http://archive.defensenews.com/article/20140730/DEFFEAT05/307300017/Commentary-Cyber-Deterrence-Working.

Healey, Jason. "No, Cyberwarfare Isn't as Dangerous as Nuclear War." US News. March 20, 2013. Accessed March 16, 2015.

Heilman, Ethan. "A Review of William Liscum Borden's 'There Will Be No Time: The Revolution in Strategy'." Accessed January 27, 2015.

http://ethanheilman.tumblr.com/post/29405762446/there-will-be-no-time-a-review.

Herman Kahn (American Futurist). Encyclopedia Britannica Online. Accessed November 12, 2014. http://www.britannica.com/EBchecked/topic/309688/Herman-Kahn.

Hersh, Seymour. "Overwhelming Force." The New Yorker. March 22, 2000. Accessed May 4, 2015. http://www.newyorker.com/magazine/2000/05/22/overwhelming-force-2.

Hertsgaard, Mark. "Star Wars Works!" Salon. Accessed May 21, 2015. http://web.archive.org/web/20010913001732/http://www.salon.com/news/news960607.html.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.

Hilsman, Roger. "New Look, Massive Retaliation, and Flexible Response." In *From Nuclear Military Strategy to a World without War: A History and a Proposal*, 33. Westport, Conn.: Praeger, 1999.

"History of the Longbow." The Order of the Rye Longbowmen. Accessed May 21, 2015. http://www.ryelongbowmen.org/history-of-the-longbow/.

"History of the Tank." Global Security. Accessed May 21, 2015. http://www.globalsecurity.org/military/systems/ground/tank-history1.htm.

Hobson, Rolf. "Blitzkrieg, the Revolution in Military Affairs and Defense Intellectuals." *Journal of Strategic Studies*: 626.

https://translate.google.com/translate?hl=en&sl=ru&tl=en&u=http%3A%2F%2Fwww.rg.ru%2F2013%2F06%2F28%2Fdoklad.html

Hundley, Richard. "Past Revolutions, Future Transformations." The RAND Corporation. Accessed December 5, 2014. http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1029.pdf. 13.

Ibrügger, Lothar. "The Revolution in Military Affairs." NATO Science and Technology Committee. Accessed December 8, 2014. http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html#1.

"International Strategy for Cyberspace." White House. May 1, 2011. Accessed May 21, 2015. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

"ISE Mission Partners: Critical Infrastructure and Key Resources." Information Sharing Environment. Accessed March 16, 2015. http://www.ise.gov/mission-partner/critical-

infrastructure-and-key-resources.

“Ivy Mike, 1 November 1952 - First Full-Scale Thermonuclear Test.” 1 November 1952. Accessed January 27, 2015. http://www.ctbto.org/specials/testing-times/1-november-1952-ivy-mike/.

Jackson, Julian. "We Are Beaten." In The Fall of France: The Nazi Invasion of 1940, 9-58. Oxford: Oxford University Press, 2003.

Johnson, Brian. "Misfortunes of War." In The Secret War, 266-270. Barnsley: Leo Cooper, 2004.

Kahn, Herman. "The Nature of Feasibility of War and Deterrence." The RAND Corporation. January 20, 1960. Accessed November 12, 2014. http://www.rand.org/content/dam/rand/pubs/papers/2005/P1888.pdf. 4.

Kaiser, Robert. "The Medieval English Longbow." Journal of the Society of Archer-Antiquaries 23 (1980).

Karl Kosher et al. "Experimental Security Analysis of a Modern Automobile." January 1, 2010. Accessed March 16, 2015. http://www.autosec.org/pubs/cars-oakland2010.pdf.

Kemp, Anthony. *The Maginot Line: Myth and Reality*. New York: Stein and Day, 1982. 9.

Kemp, R. Scott. "Cyberweapons: Bold Steps in a Digital Darkness?" Bulletin of the Atomic Scientists. June 7, 2012. Accessed March 16, 2015. http://thebulletin.org/cyberweapons-bold-steps-digital-darkness/.

Kennan, George F. "Far Eastern War and General Situation." George Washington University. August 8, 1945. Accessed January 27, 2015. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB162/57.pdf.

Kennedy, John Fitzgerald. "Inaugural Address." The American Presidency Project. January 20, 1961. Accessed November 12, 2014. http://www.presidency.ucsb.edu/ws/?pid=8032.

Kim, Zetter. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." Wired.com. July 7, 2011. Accessed May 21, 2015. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

King, Spencer Bidwell. "Second War for Independence." In Georgia Voices: A Documentary History to 1872, 284. Athens: University of Georgia Press, 2010.

Knox, MacGregor, and Williamson Murray. "Thinking About Revolutions in Warfare." In *The Dynamics of Military Revolution, 1300-2050*, 12. Cambridge, UK: Cambridge University Press, 2001.

Knox, MacGregor. "“As if a New Sun had Arisen”: England's Fourteenth-century RMA." In The Dynamics of Military Revolution, 1300-2050, 22-28. Cambridge, UK: Cambridge University Press, 2001.

Krepinevich, Andrew. "Cavalry to Computer; the Pattern of Military Revolutions." *The National Interest* 30, no. 13 (1994): 1-16.

Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. February 26, 2013. Accessed May 21, 2015. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Lackey, Douglas P. "Nuclear Weapons, Politics, and Strategy: A Short History." In *Moral Principles and Nuclear Weapons*, 31-36. Totowa, N.J.: Rowman & Allanheld, 1984.

Langner, Ralph. "Stuxnet’s Secret Twin." Foreign Policy. November 19, 2013. Accessed March 16, 2015.

"'Laser Jumbo' Testing Moves Ahead." BBC News. July 29, 2008. Accessed May 22, 2015. http://news.bbc.co.uk/2/hi/science/nature/7531046.stm.

Lee, Robin. "Coalition Fixed-Wing Combat Aircraft Attrition in Desert Storm." Estimative Error Probable. 2014. Accessed May 21, 2015. http://www.rjlee.org/air/ds-aaloss/.

“Legal Reviews of Weapons and Cyber Capabilities.” Department of the Air Force. May 13, 1994. Accessed March 16, 2015. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-053.pdf.

Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats." Center for Strategic and International Studies. December 1, 2002. Accessed May 21, 2015. http://www.enhyper.com/content/0211_lewis.pdf.

Lewis, James A. "Thresholds for Cyberwar." Center for Strategic and International Studies. September 1, 2010. Accessed May 21, 2015. http://csis.org/files/publication/101001_ieee_insert.pdf.

Libicki, Martin. "Strategic Cyberwar." In *Cyber Deterrence and Cyber War*, 123. RAND Corporation, 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Libicki, Martin. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly*, 2014.

Limbach, Raymond. "Blitzkrieg: Military Tactic." Encyclopedia Britannica Online. Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/69464/blitzkrieg.

Lin, Herb. "Cyber Conflict and National Security." Transnational Actors and New Forces. Accessed May 21, 2015. http://www.lawfareblog.com/wp-content/uploads/2013/01/cyber-conflict-and-national-security-artjervis-reader-2.pdf.

Lin, Herb. "Offensive Cyber Operations and the Use of Force." Journal of International Security, Law, & Policy 4, no. 63 (2010): 63-86. Accessed May 21, 2015. http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

Lin, Herb. "Testimony by Herbert Lin." House Committee on Energy and Commerce Subcommittee on Oversight and Investigations. March 3, 2015. Accessed May 21, 2015. http://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-Wstate-LinH-20150303.pdf.

"Longbow Archers: The Battle of Crecy, 26 August 1346." Longbow Archers. Accessed May 21, 2015. http://www.longbow-archers.com/historycrecy.html.

"Longbows, Arrows and the Origin of Fletchers." Fletcher Family. Accessed May 21, 2015. http://www.fletcher-family.co.uk/origins p1.html.

Lyman, Lauren. "Building Our Biggest Flying Fortress." New York Times, April 5, 1931.

Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." Foreign Affairs 89, no. 5 (2010). Accessed May 21, 2015. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Maisel, William H., and Tadayoshi Kohno. "Improving the Security and Privacy of Implantable Medical Devices." *New England Journal of Medicine* 7, no. 1 (2008): 116-166.

Malik, John. "The Yields of the Hiroshima and Nagasaki Explosions." Los Alamos National Laboratory. September 1, 1985. Accessed January 27, 2015. http://library.lanl.gov/cgi-bin/getfile?00313791.pdf. 1.

"Manhattan Project: The Atomic Bombing of Hiroshima, August 6, 1945." U.S. Department of Energy. Accessed January 27, 2015. https://www.osti.gov/manhattan-project-history/Events/1945/hiroshima.htm.

"Manhattan Project." CTBTO Preparatory Commission. Accessed May 10, 2015. http://www.ctbto.org/nuclear-testing/history-of-nuclear-testing/manhattan-project/manhattan-project/.

"Manhattan Project." Encyclopedia Britannica Online. Accessed January 28, 2015. http://www.britannica.com/EBchecked/topic/362098/Manhattan-Project.

Margenau, Henry. "Reviews." *The Yale Law Journal* 56 (1947): 753-55. Accessed January 22,

2015. http://www.jstor.org/stable/793331?seq=1#page_scan_tab_contents.

“Marie and Pierre Curie and the Discovery of Polonium and Radium.” Nobel Prize. Accessed January 27, 2015. http://www.nobelprize.org/nobel_prizes/themes/physics/curie/.

Markoff, John. "West Germans Raid Spy Ring That Violated U.S. Computers." New York Times. March 3, 1989. Accessed March 16, 2015.

Martin Heinrich Klaproth. Encyclopedia Britannica Online. Accessed January 27, 2015. http://www.britannica.com/EBchecked/topic/319885/Martin-Heinrich-Klaproth.

“Massive Retaliation.” Nuclearfiles.org/. Accessed November 12, 2014. http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/strategy-massive retaliation.htm.

Meilinger, Phillip S. "Formation." In Bomber: The Formation and Early Years of Strategic Air Command, 71. Maxwell Air Force Base, Ala.: Air University Press, Air Force Research Institute, 2012.

Menn, Joseph. "Russian Researchers Expose Breakthrough U.S. Spying Program." Reuters. February 16, 2015. Accessed March 16, 2015.

Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." CNN. September 26, 2007. Accessed March 16, 2015. http://www.cnn.com/2007/US/09/26/power.at.risk/

Metz, Steven, and James Kievit. "Strategy and The Revolution in Military Affairs: From Theory to Policy." Strategic Studies Institute. Accessed December 4, 2014. http://www.au.af.mil/au/awc/awcgate/ssi/stratrma.pdf. 13.

Miller, Franklin. "A Conversation with General C. Robert Kehler." Council on Foreign Relations. May 30, 2012. Accessed May 14, 2015. http://www.cfr.org/united-states/conversation-general-c-robert-kehler/p35267.

Minkel, JR. "The 2003 Northeast Blackout--Five Years Later." Scientific American. August 13, 2008. Accessed April 29, 2015. https://www.scientificamerican.com/article/2003-blackout-five-years-later/.

Moïse, Edwin. "Limited War: The Stereotypes." Clemson University. November 22, 1998. Accessed May 21, 2015. http://www.clemson.edu/caah/history/FacultyPages/EdMoise/limit1.html.

Muradian, Vago. "Adm. Michael Mullen." Defense News. July 10, 2011. Accessed March 8, 2015. http://archive.defensenews.com/article/20110710/DEFFEAT03/107100301/Adm-Michael-Mullen.

Murray, Williamson. "Contingency and Fragility of the German RMA." In *The Dynamics of Military Revolution, 1300-2050*, 162. Cambridge, UK: Cambridge University Press, 2001.

"Nagasaki Memorial Adds British POW as A-Bomb Victim." The Japan Times. June 24, 2005. Accessed May 21, 2015. http://www.japantimes.co.jp/news/2005/06/25/national/nagasaki-memorial-adds-british-pow-as-a-bomb-victim/#.VV1qwqZGy2z.

"National Military Strategy for Cyberspace Operations." Department of Defense. December 11, 2006. Accessed March 16, 2015. http://www.space-library.com/0612dod_The%20National%20Military%20Strategy%20for%20Cyberspace%20Operations%28U%29_2+52pages.pdf.

Nelson, Michael. "Commander in Chief." In The Powers of the Presidency, 279. Washington, DC: CQ Press, 2008.

Neufield, Jacob. "The Development of Ballistic Missiles in the United States Air Force 1945-1960." Office of Air Force History. January 1, 1990. Accessed January 28, 2015. http://www.afhso.af.mil/shared/media/document/AFD-100924-024.pdf.

Newton, Scott. "Can Cyberterrorists Actually Kill People?" SANS Institute. November 1, 2001. Accessed March 16, 2015. http://www.sans.org/reading-room/whitepapers/warfare/cyberterrorists-kill-people-820.

Nitze, Paul H. *NSC-68 Forging the Strategy of Containment*. Washington, DC: National Defense University, 1994. 2.

Nojeim, Michael J., and David P. Kilroy. *Days of Decision Turning Points in U.S. Foreign Policy*. Washington, D.C.: Potomac Books, 2011. 79. 79

"NSC 68: United States Objectives and Programs for National Security." Mtholyoke.edu. April 14, 1950. Accessed November 12, 2014. https://www.mtholyoke.edu/acad/intrel/nsc-68/nsc68-1.htm.

"NSC162/2: A Report to the National Security Council on Basic National Security Policy." Federation of American Scientists. October 30, 1954. Accessed November 12, 2014. http://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf. 6-7.

"Nuclear Detonation: Weapons, Improvised Nuclear Devices." U.S. Department of Health and Human Services: Radiation Emergency Medical Management. Accessed January 27, 2015. http://www.remm.nlm.gov/nuclearexplosion.htm.

Nye, Joseph S. "Diffusion and Cyberpower." In The Future of Power, 146. New York: Public

Affairs, 2011.

Obama, Barack. "Executive Order: Improving Critical Infrastructure Cybersecurity." The White House. February 12, 2013. Accessed May 21, 2015. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

"Ohio Class." National Cold War Exhibition. Accessed May 15, 2015. http://www.nationalcoldwarexhibition.org/research/collections/ohio-class/.

Oman, Charles, and John Beeler. "The Swiss." In *The Art of War in the Middle Ages: A.D. 378-1515*, 49. Ithaca: Cornell University Press, 1968.

Owens, William, and Theo Farrell. "Creating a U.S. Military Revolution." In *The Sources of Military Change: Culture, Politics, Technology*, 207. Boulder: Lynne Rienner Publishers, 2002.

Owens, William, and Theo Farrell. "Creating a U.S. Military Revolution." In *The Sources of Military Change: Culture, Politics, Technology*, 209. Boulder: Lynne Rienner Publishers, 2002.

Panchasi, Roxanne. ""Fortress France": Protecting the Nation and Its Bodies, 1918-1940." Historical Reflections 33, no. 3 (2007): 477.

"Panzer: German Tank." Encyclopedia Britannica Online. Accessed May 21, 2015. http://www.britannica.com/EBchecked/topic/1057539/panzer.

Pape, Robert A. "Why Japan Surrendered." International Security 18, no. 2 (1993): 154-201.

"Past Prime Ministers: History of Stanley Baldwin." Gov.uk. Accessed February 4, 2015. https://www.gov.uk/government/history/past-prime-ministers/stanley-baldwin.

Perlroth, Nicole, and Quentin Hardy. "Bank Hacking Was the Work of Iranians, Officials Say." The New York Times. January 8, 2013. Accessed May 21, 2015. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." The New York Times. October 23, 2012. Accessed May 21, 2015. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Perry, William J. "Desert Storm and Deterrence." Foreign Affairs, 1990, 66-82. Accessed May 21, 2015. https://www.foreignaffairs.com/articles/iraq/1991-09-01/desert-storm-and-deterrence.

"Pershing II Weapon System (System Description)." United States Army. 1986. Accessed May 21, 2015. http://www.scribd.com/doc/64061132/TM-9-1425-386-10-1.

"Persian Gulf War: 1990-1991." Encyclopedia Britannica Online. Accessed May 4, 2015. http://www.britannica.com/EBchecked/topic/452778/Persian-Gulf-War.

"Polaris A1 - United States Nuclear Forces." Federation of American Scientists. Accessed January 28, 2015. http://www.fas.org/nuke/guide/usa/slbm/a-1.htm.

"Potential War Casualties Put at 100,000: Gulf Crisis: Fewer U.S. Troops Would Be Killed or Wounded than Iraq Soldiers, Military Experts Predict." Los Angeles Times. September 5, 1990. Accessed May 21, 2015. http://articles.latimes.com/1990-09-05/news/mn-776_1_military-experts.

Poundstone, William. Prisoner's Dilemma. New York: Anchor Books, 2011. 144.

"Profile for United States." NTI: Nuclear Threat Initiative. Accessed January 27, 2015. http://www.nti.org/country-profiles/united-states/delivery-systems/.

Quester, George H. "Outright Advocates." In *Nuclear Monopoly*, 49. New Brunswick: Transaction Publishers, 2000.

Rashid, Fahmida. "SCADA Systems in Railways Vulnerable to Attack." EWeek. January 25, 2012. Accessed March 16, 2015.

Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role." *Diplomatic History* 25, no. 1, 154.

Rearden, Steven L. "Feature Review: Reassessing the Gaither Report's Role." *Diplomatic History* 25, no. 1, 155.

Reilly, Henry J. "Blitzkrieg." Foreign Affairs 18, no. 2 (1940). Accessed May 21, 2015. https://www.foreignaffairs.com/articles/germany/1940-01-01/blitzkrieg.

Reiss, Edward. "Contexts and Conditions." In *The Strategic Defense Initiative*. 176. Cambridge England: Cambridge University Press, 1992.

"Report by the Technological Capabilities Panel of the Science Advisory Committee." State.gov. February 14, 1955. Accessed November 12, 2014.

"Resilient Military Systems and the Advanced Cyber Threat." Defense Science Board. 2013. Accessed May 21, 2015. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

Reveron, Derek S. "Conclusion." In *Cyber Challenges and National Security: Threats,*

Opportunities, and Power in a Virtual World, 220. Washington, D.C.: Georgetown University Press, 2012.

Rhodes, Richard. "Moonshine." In *The Making of the Atomic Bomb*, 13, 28. 25th Anniversary ed. New York: Simon & Schuster Paperbacks, 2012.

Rhodes, Richard. "This Buck Rogers Universe." In *Dark Sun the Making of the Hydrogen Bomb*, 357-358. New York: Simon & Schuster, 1995.

Rogers, Clifford. "The Military Revolutions of the Hundred Years' War." *The Journal of Military History* 57, no. 2 (1993): 251.

Rogers, Michael. "Cybersecurity Threats: The Way Forward." House of Representatives Select Committee on Intelligence. November 20, 2014. Accessed May 21, 2015. https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf.

Samaan, Jean. "Introduction." In *The RAND Corporation (1989-2009) the Reconfiguration of Strategic Studies in the United States*, 10. New York: Palgrave Macmillan, 2012.

Sanger, David, and Martin Fackler. "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say." The New York Times. January 18, 2015. Accessed May 21, 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

Sanger, David, and Thom Shanker. "Broad Powers Seen for Obama in Cyberstrikes." The New York Times. February 3, 2013. Accessed March 16, 2015. http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html.

Sanger, David. "Mutually Assured Cyberdestruction?" The New York Times. June 2, 2012. Accessed March 16, 2015. http://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html.

Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran." The New York Times. May 31, 2012. Accessed March 16, 2015. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Santens, Scott. "Self-Driving Trucks Are Going to Hit Us Like a Human-Driven Truck." Medium. May 14, 2015. Accessed May 22, 2015. https://medium.com/basic-income/self-driving-trucks-are-going-to-hit-us-like-a-human-driven-truck-b8507d9c5961.

Sapolsky, Harvey, Benjamin Friedman, and Brendan Green. U.S. Military Innovation Since the Cold War: Creation Without Destruction. Routledge, 2012. 157.

Schaffer, Ronald. "Epilogue." In *Wings of Judgment: American Bombing in World War II*, 202. Oxford; New York: Oxford University Press, 1985.

Schelling, Thomas C. "The Diplomacy of Violence." In *Arms and Influence*, 19, 23. New Haven: Yale University Press, 1966.

Schwartz, Stephen I. Atomic Audit the Costs and Consequences of U.S. Nuclear Weapons since 1940. Washington, D.C.: Brookings Institution Press, 1998. 3.

Scrivner, Jr., Major John. "The Dirigible – A Reconsideration." Air University Review. 1966. Accessed May 14, 2015. http://www.airpower.maxwell.af.mil/airchronicles/aureview/1966/jan-feb/scrivner.html.

"Secretary of Defense Confirmation Hearing." C-SPAN.org. June 9, 2011. Accessed March 16, 2015. http://www.c-span.org/video/?299943-1/secretary-defense-confirmation-hearing.

"Senate Foreign Relations Committee Holds Confirmation Hearing on the Nomination of Massachusetts Democratic Sen. John Kerry to Be Secretary of State." Congressional Quarterly. January 24, 2013. Accessed March 8, 2015. http://www.cq.com/doc/congressionaltranscripts-4209477?0&print=true.

Shepperd, Alan. "The Battle for France." In France 1940: Blitzkrieg in the West, 31-88. London: Osprey, 1990.

Silverstone, Scott A. "Eisenhower and the Growth of Soviet and Chinese Power 1953-1955." In *Preventive War and American Democracy*. 101. New York: Routledge, 2007.

Singel, Ryan. "Richard Clarke's Cyberwar: File Under Fiction." Wired.com. April 22, 2010. Accessed May 21, 2015. http://www.wired.com/2010/04/cyberwar-richard-clarke/.

Singer, Peter, and Allan Friedman. "Why It Matters." In *Cybersecurity What Everyone Needs to Know.*, 155. New York: Oxford University Press, 2012.

Slade, Stuart. "Boeing B-29 Superfortress." In *United States Strategic Bombers 1945: 2012.*, 10. Defense Lion Publications, 2012.

Slay, Jill, and Michael Miller. "Lessons Learned from the Maroochy Water Breach." International Federation for Information Processing. Accessed March 16, 2015. http://www.ecdlhealth.it/wcc2008/IFIP_Sample_Chapter_Created_LaTeX.pdf.

Sloan, Elinor C. *The Revolution in Military Affairs Implications for Canada and NATO*. Montreal: McGill-Queen's University Press, 2002. 27.

Smart, Nick. "The Maginot Line: An Indestructible Inheritance." *International Journal of*

Heritage Studies: 225.

Smith, Amelia. "China Could Shut Down U.S. Power Grid With Cyber Attack, Says NSA Chief." Newsweek. November 21, 2014. Accessed March 16, 2015. http://europe.newsweek.com/china-could-shut-down-us-power-grid-cyber-attack-says-nsa-chief-286119.

Smith, Richard K. The Airships Akron & Macon; Flying Aircraft Carriers of the United States Navy. Annapolis: U.S. Naval Institute, 1965. 210.

Snead, David L. *The Gaither Committee, Eisenhower, and the Cold War*. Columbus: Ohio State University Press, 1999. 3.

Snowcroft, Brent, and Zbigniew Brzezinski. "Hearing on National Security Threats." Senate Armed Services Committee. January 21, 2015. Accessed May 21, 2015. http://www.c-span.org/video/?323887-1/hearing-national-security-threats.

Soman, Appu Kuttan. "Setting the Stage." In *Double-edged Sword Nuclear Diplomacy in Unequal Conflicts : The United States and China, 1950-1958*, 22. Westport, Conn.: Praeger, 2000.

Spafford, Eugene. "The Internet Worm Program: An Analysis." Purdue University. December 8, 1988. Accessed March 16, 2015. http://spaf.cerias.purdue.edu/tech-reps/823.pdf.

"Staged Cyber Attack Reveals Vulnerability in Power Grid." YouTube. September 27, 2007. Accessed March 16, 2015. https://www.youtube.com/watch?v=fJyWngDco3g.

"Stanford University 121st Opening Convocation Ceremony." YouTube. October 10, 2011. Accessed April 29, 2015.

"Statement of General Keith B. Alexander." House of Representatives Committee on Armed Services. September 23, 2010. Accessed March 16, 2015. http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf.

"Stephen Biddle." Elliott School of International Affairs. Accessed December 8, 2014. https://elliott.gwu.edu/biddle.

Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea." *Military Review* May-June 2010 (2010): 38-46.

"Strategic Airpower: The History of Bombers." Boeing. Accessed May 21, 2015. http://www.boeing.com/bds/strategicairpower/.

"Strategic Cyber Weapon: No Results Found." DOD Dictionary of Military and Associated

Terms. Accessed May 21, 2015. http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=strategic cyber weapon&zoom_sort=0&zoom_per_page=10&zoom_and=1.

"Submarine Launched Ballistic Missiles: United States Nuclear Forces Guide." Federation of American Scientists. Accessed May 21, 2015. http://fas.org:8080/nuke/guide/usa/slbm/index.html.

"Tanks in the World Wars." History. August 26, 2014. Accessed May 21, 2015. http://www.history.co.uk/study-topics/history-of-tanks/tanks-in-the-world-wars.

"Telent to Renew NR's Traction Power Control Network." Railway Gazette. September 12, 2013. Accessed March 16, 2015. http://www.railwaygazette.com/news/infrastructure/single-view/view/telent-to-renew-nrs-traction-power-control-network.html.

"The 6555th's Role in the Development of Ballistic Missiles." Federation of American Scientists. Accessed January 27, 2015. http://fas.org/spp/military/program/6555th/6555c3-5.htm.

"The Atomic Bombings of Hiroshima and Nagasaki: The Attacks." The Atomic Archive. Accessed May 21, 2015. http://www.atomicarchive.com/Docs/MED/med_chp7.shtml.

"The Atomic Bombings of Hiroshima and Nagasaki: Total Casualties." The Atomic Archive. Accessed January 27, 2015. http://www.atomicarchive.com/Docs/MED/med_chp10.shtml.

"The Battle of Creçy 1346." British Battles. Accessed May 4, 2015. http://www.britishbattles.com/100-years-war/crecy.htm.

"The Battle of Crécy." English Monarchs. Accessed May 21, 2015. http://www.englishmonarchs.co.uk/battle_crecy.html.

"The Battle of France." German Propaganda Archive. July 22, 1940. Accessed May 21, 2015. http://research.calvin.edu/german-propaganda-archive/facts01.htm.

"The DoD Cyber Strategy." U.S. Department of Defense. April 1, 2015. Accessed May 21, 2015. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

"The Gita of J. Robert Oppenheimer." Proceedings of the American Philosophical Society 144, no. 2 (2000): 123.

"The History of the English Longbow." Historic UK. Accessed May 21, 2015. http://www.historic-uk.com/HistoryUK/HistoryofEngland/The-Longbow/.

"The Longbow: Medieval Weaponry." Military History Monthly. January 11, 2011. Accessed May 21, 2015. http://www.military-history.org/articles/medieval/the-longbow.htm.

"The Longbow." History Magazine. October 31, 1999. Accessed May 21, 2015. http://www.history-magazine.com/longbow.html.

"The Longbow." In Proceedings of the Numismatic and Antiquarian Society of Philadelphia, 122. Philadelphia: Franklin Printing Company, 1902.

"The Maginot Line." History Learning Site. 2015. Accessed May 21, 2015. http://www.historylearningsite.co.uk/maginot_line.htm.

"The Manhattan Project: Making the Atomic Bomb." The Uranium Committee. Accessed January 28, 2015. http://www.atomicarchive.com/History/mp/p2s1.shtml.

"The Missile Race Begins." Vectorsite.net/. Accessed November 12, 2014. http://www.vectorsite.net/tamrc_04.html.

"The Peacekeeper (MX) ICBM." Nuclear Weapon Archive. October 10, 1997. Accessed May 21, 2015. http://nuclearweaponarchive.org/Usa/Weapons/Mx.html.

"The Tank." Leonardo Da Vinci's Inventions. 2015. Accessed May 21, 2015. http://www.leonardodavincisinventions.com/war-machines/leonardo-da-vincis-tank/.

"The Unfinished War: A Decade Since Desert Storm." CNN. 2001. Accessed May 21, 2015. https://web.archive.org/web/20080612131747/http://www.cnn.com/SPECIALS/2001/gulf.war/facts/gulfwar/.

Thielmann, Greg. "The Missile Gap Myth and Its Progeny." Arms Control Association. Accessed November 12, 2014. http://www.armscontrol.org/act/2011_05/Thielmann.

"Throngs Here See Ships." New York Times, November 3, 1931.

"To Consider the Nomination Of: Honorable Ashton B. Carter to Be Secretary of Defense." Senate Committee on Armed Services. February 4, 2015. Accessed March 16, 2015.

Tomes, Robert R. "Military Innovation in the Shadow of Vietnam: The Offset Strategy." In US Defense Strategy from Vietnam to Operation Iraqi Freedom Military Innovation and the New American Way of War, 1973- 2003, 60. London: Routledge, 2007.

Truman, Harry. "Announcing the Bombing of Hiroshima: Statement by the President of the United States." PBS. August 6, 1945. Accessed January 27, 2015. http://www.pbs.org/wgbh/americanexperience/features/primary-resources/truman-hiroshima/.

"U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." U.S. Department of Justice. May 19, 2014. Accessed May 21, 2015. http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

"U.S. Cyber Command." U.S. Strategic Command. Accessed March 16, 2015. http://www.stratcom.mil/factsheets/2/Cyber_Command/.

Villahermosa, Gilberto, and David M. Glantz. "Foreign Military Studies Office Publications - Desert Storm: The Soviet View." Foreign Military Studies Office Publications. Accessed December 8, 2014. http://fmso.leavenworth.army.mil/documents/rs-storm.htm#77a.

Wald, Matthew. "The Blackout That Exposed the Flaws in the Grid." The New York Times. November 10, 2013. Accessed April 29, 2015. http://www.nytimes.com/2013/11/11/booming/the-blackout-that-exposed-the-flaws-in-the-grid.html.

Walker, Gregory. "The Effects of Nuclear Weapons: Descriptions of Nuclear Explosions." Trinity Atomic Web Site. Accessed May 21, 2015. http://www.abomb1.org/nukeffct/enw77b1.html.

Walker, Mark. "Lightening War." In *German National Socialism and the Quest for Nuclear Power, 1939-1949*, 17-24. Cambridge: Cambridge Univ. Press, 1989.

Walsh, Bryan. "10 Years After the Great Blackout, the Grid Is Stronger - but Vulnerable to Extreme Weather." Time Magazine. Accessed April 29, 2015. http://science.time.com/2013/08/13/ten-years-after-the-great-blackout-the-grid-is-stronger-but-vulnerable-to-extreme-weather/.

Walters, Guy. "A History of the Tank: From Leonardo Da Vinci to the Second World War." The Telegraph. 2014. Accessed May 21, 2015. http://www.telegraph.co.uk/sponsored/culture/film-fury/11146708/tank-history.html

Warden, John A., and Richard H. Shultz. "Employing Air Power in the Twenty First Century." In *The Future of Air Power in the Aftermath of the Gulf War*, 82. Honolulu: University Press of the Pacific, 2002.

Wiggins, James, C. Erlanger, and T. Harris. "Regulatory Efforts to Improve Cyber Security." U.S. Nuclear Regulatory Commission. Accessed March 16, 2015.

Willbanks, James H. "Notes." In *Generals of the Army Marshall, MacArthur, Eisenhower, Arnold, Bradley.*, 230. University Press of Kentucky, 2013.

Wilson, Ward. "The Bomb Didn't Beat Japan… Stalin Did." Foreign Policy. May 30, 2013. Accessed May 21, 2015. http://foreignpolicy.com/2013/05/30/the-bomb-didnt-beat-japan-stalin- did/.

Wohlstetter, Albert. "The Delicate Balance of Terror." The RAND Corporation. November 6, 1958. Accessed November 12, 2014. http://www.rand.org/about/history/wohlstetter/P1472/P1472.html.

Work, Bob. "National Defense University Convocation." United States Department of Defense. August 5, 2014. Accessed May 21, 2015. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1873.

"World War I: How the German Zeppelin Wrought Terror." BBC News. August 3, 2014. Accessed January 27, 2015. http://www.bbc.com/news/uk-england-27517166.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired.com. November 3, 14. Accessed March 16, 2015. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zetter, Kim. "How the NSA's Firmware Hacking Works and Why It's So Unsettling." Wired. February 22, 2015. Accessed May 21, 2015. http://www.wired.com/2015/02/nsa-firmware-hacking/.

Васенин, Виктор, and Сергей Куксин. "Стенограмма выступления Дмитрия Рогозина на пресс-конференции в "РГ"" Российская газета. June 28, 2013. Accessed March 16, 2015. http://www.rg.ru/2013/06/28/doklad.html.

Appendix: Interview List

Name	Organization	Role	Sector	Contact	Date
Barack Obama	U.S. Government	President	Public	In Person	2/13/15
Robert Gates	Department of Defense	Secretary	Public	Phone	3/23/15
Bill Perry	Department of Defense	Secretary	Public	In Person	1/28/15
Cecil Haney	Strategic Command	Commander/ Admiral	Military	In Person	1/24/15
C. Robert Kehler	Strategic Command	Commander/ General	Military	In Person	2/10/15
James Ellis	Strategic Command	Commander/ Admiral	Public/ Military	Phone	3/10/15
Michael Hayden	National Security Agency/ Central Intelligence Agency	Director/ General	Public/ Military	Phone	3/10/15
Kenneth Chennault	American Express	Chairman and CEO	Private	In Person	2/13/15
Anthony Earley, Jr.	Pacific Gas & Electric	Chairman and CEO	Private	In Person	2/13/15
Brian White	Chertoff Group	Principal (Cyber)	Private	In Person	8/10/14
Chris Painter	Department of State	Cyber Coordinator	Public	Phone	3/30/15
Michelle Markoff	Department of State	Deputy Cyber Coordinator	Public	Phone	4/1/15
Phyllis Schneck	Department of Homeland Security	Deputy Undersecretary for Cybersecurity and Communications	Public	Phone	4/10/15
Siegfried Hecker	Los Alamos National Laboratories	Director	Science	Phone	2/23/15
Mark Ghilarducci	California Governor's Office of Emergency Services	Director	Public	Phone	3/10/15

Sidney Drell	SLAC National Accelerator Laboratory	Deputy Director	Science	In Person	3/5/15
Thomas Schelling	RAND Corporation	Economist/ Strategist	Think Tank/ Academia	Phone	2/16/15
Martin Libicki	RAND Corporation	Senior Management Scientist	Think Tank/ Academia	In Person	3/20/15
James Lewis	Center for Strategic and International Studies	Director/Senior Fellow	Think Tank/ Academia	In Person	3/18/15
Robert Jervis	Columbia University	Professor	Academia	Phone	2/19/15
Mark Ghilarducci	California Governor's Office of Emergency Services	Director	Public	Phone	3/10/15
Matteo Martemucci	688th Cyberspace Wing, Air Force	Colonel	Military	Phone	2/26/15
James Wakefield	Air Force	Lieutenant Colonel	Military	In Person	4/12/15
Enrique Oti	Air Force	Lieutenant Colonel	Military	In Person	4/29/15
Kirk McConnell	Senate Armed Services Committee	Staffer	Public	In Person	3/19/15
Kevin Gates	House Armed Services Committee	Staffer	Public	In Person	3/18/15
Emily Goldman	Cyber Command	Strategic Advisor	Military	Phone	3/20/15
Michael Warner (on background)	Cyber Command	Command Historian	Military	Phone	3/26/15
Kim Zetter	Wired	Journalist	Media	Phone	2/11/15
Jackie Schneider	Elliot School of International Affairs	Doctoral Student	Academia	In Person	3/18/15