National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER: BETWEEN MELTING REACTORS AND HURTING FEELINGS, HOW THE CAF NEEDS TO PRIORITIZE DEFENCE

Maj Travis Field

JCSP 43 DL

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 43 AD

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER: BETWEEN MELTING REACTORS AND HURTING FEELINGS, HOW THE CAF NEEDS TO PRIORITIZE DEFENCE

Maj Travis Field

Word Count: 2933

Compte de mots: 2933

CYBER: BETWEEN MELTING REACTORS AND HURTING FEELINGS, HOW THE CAF NEEDS TO PRIORITIZE DEFENCE

The potential span of cyberwarfare is massive. This paper argues how the Canadian Armed Forces (CAF) needs to categorize and prioritize its limited resources regarding cyber defence. Canada must first be concerned with attacks that can result in a direct physical effect. It must secondly be concerned with preventing attacks where information compromised may lead to physical damage or injury. Thirdly, aspects of cyberwarfare, such as its use as a platform for influence activities, are tertiary and need to be prioritized as such. And lastly, the responsibility for defending critical federal infrastructure from a cyberattack is not clear but ultimately should not be an area where the CAF prioritizes efforts.

In order to demonstrate how Canada needs to prioritize cyber efforts, this paper will describe a number of historical examples of cyber attacks that have had drastic physical consequences. It will also touch on a number of non-kinetic examples of harassment to offer as a foil. Finally, the complicated topic of cyber attacks on non-military institutions will be discussed.

As far as definition, this paper contends that computers and networks need to be involved for an event to qualify as a cyber attack. There are many definitions on offer for cyber warfare but the two main requirements, according to this author, is that computers must be involved and there must be a network in place that is utilized to some extent. Thus, this author rejects any discussion of Mongols as being a network from a cyber perspective.[1]

[1]John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Athena's Camp: Preparing for Conflict in the Information Age,* (Santa Monica: RAND Corporation, 1997), 34.

Some have argued that the effect caused by the inception of cyberpower is similar to that during the inception of airpower.[2] However, most cyber attacks are unable to cause actual physical harm which is the primary realm in which the military operates. If threatened with an attack by air, land, or sea, most people would lock themselves in a bunker and hope for the best. If threatened by a cyber attack the same people would turn the computer off and make a sandwich. Cyber attacks that can cause a meaningful change in the physical realm are of critical interest and there are a number of recent instances.

The first example, and the gold standard with regards to the physical destruction caused by a network attack, is known as Stuxnet. Widely suspected as a US and Israeli-backed offensive against Iranian development of nuclear weapons, Stuxnet utilized a network to spread. There were two separate stages to the Stuxnet attack on Iran's nuclear program between 2007 and 2010. The first infiltrated the network that controlled centrifuge operation, the method by which uranium is enriched for use in nuclear weapons.[3] This very complicated attack used a number of vulnerabilities and knowledge of Iran's enrichment operations to over-pressurize centrifuges.[4]

In the second and more simple component to the effort, the attackers found a way to manipulate the speed of centrifuge rotation, often spooling up to a very high speed before causing a sudden stop in order to induce mechanical failure of physical components.[5] These failures were aggravating to the engineers who could not understand the reason for the failures.

---

[2]Matthew Dallek, "To Understand the Future of Cyber Power, Look to The Past of Air Power," *Huffington Post* online, 3 March 2017, last accessed 26 May 2018, https://www.huffingtonpost.com/entry/cyber-war-technology_us_58dbfab2e4b01ca7b4294347.

[3]Ralph Langner, *To Kill a Centrifuge, A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, (Arlington, Hamburg, Munich: The Langner Group, November 2013), 9, accessed online 26 May 2018, https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

[4]Thomas Rid, "Cyberwar Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (Feb 2012), 19.

[5]Ralph Langner, "To Kill a Centrifuge…, 11.

The end result was physical damage to sensitive and rare centrifuge equipment resulting in extremely long timelines to replace.

The Stuxnet cyberattack was incredibly complicated and required elements of physical action such as espionage and theft in order to succeed.[6] It also required much patience, and a little luck, by relying on an eventual lapse of network security as it needed people to use infected USB sticks to transport the virus.[7] The perpetrators hedged their bets by targeting firms who had need to interact with the Iranian control system.[8] In general, the attack proved how the right combination of factors could result in great physical damage.

This also disproves one of the long-standing tenets of the cyber domain which is that cyber has levelled the playing field. In theory, anyone with an internet connection and the proper skills should be able to do some damage. However, the opposite has been proven so far. The countries who dedicate the most amount of funding and resources for their military enterprise tend to rise to the top.[9] Stuxnet used multiple 0-day viruses, which is a very significant investment.[10] These are the cyber equivalent of using brand new weapons for the first time, except that in the case of cyber once they have been used once their ability to be used effectively again falls exponentially. Stuxnet also relied on theft of digital certifications requiring actual break and entering.[11] There are instances where individuals can get lucky, but on the whole, effective cyber requires resources. Rich countries still have the most resources, from bombs, to

---

[6]David Kushner, "The Real Story of Stuxnet" *Institute of Electrical and Electronics Engineers (IEEE) Spectrum Magazine* online*,* May 2018 Edition, 26 Feb 2013, last accessed 27 May 2018, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[7]*Ibid.*

[8]Thomas Rid, "Cyberwar Will Not Take Place." *Journal of Strategic Studies…*, 19

[9]David J. Betz and Tim Stevens, "Conclusion." *Cyberspace and the State: Toward a Strategy for Cyber-Power,* (Abingdon: Routledge, 2011), 131.

[10]Ryan Naraine, "Stuxnet attackers used 4 Windows zero-day exploits," *ZD Net online*, 14 September 2010, last accessed 26 May 2018, https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/.

[11]*Ibid*.

programmers and coders. For Canada, again, this means appropriately selecting where to apply its limited resources.

The CAF needs to concentrate and invest in defences against potential attacks like Stuxnet which can result in physical damage. The standing up of the Canadian Forces Cyber Ops section and the creation of a Cyber Operator trade are great initial steps. Recognizing that cyber security starts with each individual and includes all elements, including the institution itself, the CAF has made security awareness a part of training at all levels. Ultimately, the more critical an item is, the more measures must be in place to protect it. For example, networked weapon systems must isolate themselves from external influence to the maximum extent possible, specifically maintaining clear of the Internet.

Although the number of confirmed cyber attacks that have resulted in physical damage are rare, there are growing numbers of instances where individuals and groups have made inroads. In 2015 there was a high-profile attack on a Polish commercial air provider which went after administrative style networks using Direct Denial of Service (DDOS) tactics which overwhelm a network with external requests.[12] This had the effect of grinding the airline's operations to a halt although no one was placed in any physical danger. Also, within the aviation industry, it has been confirmed that in 2017 a team led by the Science and Technology Directorate of the U.S. Department of Homeland Security (DHS) demonstrated that it could remotely hack a parked commercial aircraft. DHS acquired a used Boeing 757 that it parked at

[12]Wiktor Szary and Eric Auchard, "Polish airline, hit by cyber attack, says all carriers are at risk," *Reuters* online, 22 June 2015, last accessed 26 May 2018, https://www.reuters.com/article/us-poland-lot-cybercrime/polish-airline-hit-by-cyber-attack-says-all-carriers-are-at-risk-idUSKBN0P21DC20150622.

the airport in Atlantic City, New Jersey, and conducted a "non-cooperative penetration" of systems aboard the aircraft."[13]

The loss of control of physical systems, as indicated by the Stuxnet example and the aircraft hacking, need to be of the most concern for Canada. All networked targeting and weapon control systems need to be protected to the utmost. These are present in ships, submarines, aircraft, land attack systems, and in command and control networks throughout the CAF.

A high-profile demonstration of a cyber attack the next level down, where compromise *could* lead to physical destruction or harm, was Operation Orchard, also know as Operation Outside the Box. The cyber component of this effort directly enabled an attack by Israeli fighter jets on a Syrian nuclear weapon development facility.[14] The incident included many domains (including a strategic-level gamble). Thanks to the combination of cyber warfare as an enabler, and the electronic measures utilized, Syria's air detection systems were spoofed with a fake picture masking Israeli movement and its air defence capability was neutralized.[15] There is also speculation that there was a 'kill switch' embedded in the system's software that the Israelis made use of.[16]

This potential built in switch may have been put in place by employees of the company itself. As Lynn III states: "The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat. Tampering is almost impossible to detect and even

---

[13]Calvin Biesecker, "Cyberattacks on Connected Aircraft Are Happening Right Now," *Aviation Today* online, 13 April 2018, last accessed 27 May 2018, http://www.aviationtoday.com/2018/04/13/cyber-attacks-connected-aircraft-happening-right-now/.

[14]Thomas Rid, "Cyberwar Will Not Take Place." *Journal of Strategic Studies…*, 16

[15]*Ibid*., 17.

[16]Sally Adee, "The Hunt for the Kill Switch," *Institute of Electrical and Electronics Engineers (IEEE) Spectrum Magazine* online, *May* 2008 Edition, 1 May 2008, last accessed 26 May 2018, https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.

harder to eradicate."[17] It makes one give pause and wonder if there are 'kill switches' in Canadian military software laying dormant until required. What is the price that a country would pay a few rogue company engineers to put these in place to have available 'just in case'?

An attack on a US cyber network in 2008 can be examined with a similar lens. In this instance compromise *could* have led to physical harm and destruction. However, in this massive security breach there does not appear to have been any negative kinetic effect that occurred as a result. This infection of the United States' secret network was also accomplished using an infected USB stick.[18] In this case, the system that was compromised housed items ranging from orders and plans, to information on individuals within the organization. It is believed that the virus was never able to link up with its director for instructions on how to proceed or what information to send back once it was in. However, this was a good demonstration of what is required for restorative measures *after* a worm, virus or malware is discovered on a network. It took 14 months for the US to completely restore its classified network in an effort that it dubbed Operation Buckshot Yankee.[19]

The final level of cyber vulnerability that the CAF should be concerned with consists of Information Operations and Influence Activities via networks. As part of the ongoing deployment to Latvia, Canadian troops have been, and continue to be, exposed to a disinformation campaign. They were warned beforehand to expect social media posts that would attempt to detract attention from their mission. The kind of things they ended up seeing (most likely scripted by Russians) included claims that ex-Colonel Russell Williams remains in the

---

[17]William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (Sep/Oct 2010), online article without page numbers, last accessed 26 May 2018, http://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx.

[18]*Ibid.*

[19]Kim Zetter, "The Return of the Worm That Ate the Pentagon," *Wired Magazine* online, 12 September 2011, last accessed 27 May 2018, https://www.wired.com/2011/12/worm-pentagon/.

Canadian Forces, Canadian soldiers reside in luxury apartments, they litter indiscriminately, and they are fixated on buying beer.[20]

The spreading of disinformation can be considered by some as part of the spectrum of cyberwarfare. Russia certainly recognizes this a critical part of cyber activity; they created a cyber army in 2013 dedicated to this pursuit.[21] However, this is not where Canada should prioritize its efforts. This background cyber noise must not obfuscate higher risk cyber defence aspects. Unlike a cyber threat that causes harm to troops and equipment, the use of cyber in this regard is more comparable with low grade harassment such as the Tokyo Rose broadcasts during World War II. Good leadership can nullify negative influence activities, however, it takes money and resources to counter invasive network attacks. A failure in network protection will be what allows battlefield cyber compromise of a professional military, not a meme or insulting post.

It is far from a foregone conclusion that influence activities enabled by the Internet are actually successful. A recent study in the Ukraine concluded that like-minded groups tended to expose themselves to information from other like-minded groups.[22] In other words, although the Internet accommodates extra-community interaction, it doesn't necessarily occur. And it seems the more polarizing the topic, the less cross-cutting between disparate thinkers is likely to occur.[23] It is also improbable, especially through the use of social media, that a person's longstanding views can so easily be swayed by such measures.

---

[20]Tom Blackwell, "Russian fake-news campaign against Canadian troops in Latvia includes propaganda about litter, luxury apartments," *The National Post* online, 17 November 2017, last accessed 26 May 2018 http://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments.

[21]Edwin Armistead and Scott Starsman, "Perception Shaping and Cyber Macht: Russia and Ukraine," *International Conference on Cyber Warfare and Security,* (2015), 15.

[22]Dinissa Duvanova, Alexander Semenov and Alexander Nikolaev, "Do social networks bridge political divides? The analysis of VKontakte social network communication in Ukraine," *Post-Soviet Affairs 31,* Iss. 3, (April 2015), 235.

[23]*Ibid*., 237.

Trying to counter each piece of disinformation or trying to correct all inaccuracies would be a very large undertaking. A single Russian troll with an army of bots at their disposal (to 'like' or trend their message) can produce a lot of data in a day. Trolls are often hired to work together in groups and it is typical that up to 400 of these individuals may be grouped together to use their multiple false identities for the purpose of spreading political influence.[24] They are best described as 'paid propagandists.'[25] They are usually given themes every day about which they have to post. The only avenue to thwart this is to constantly provide a positive counter message that is grounded in truth and facts. Also, sensitization training for Canadian troops going forward is required in order to counter these forms of harassment at the individual level. In the end, the disinformation problem on social media is not the military's to solve. Strong leadership and the encouragement of critical thought are more appropriate than expending any other kind of resource towards the problem.

A final cyber topic to consider is the protection of civilian infrastructure. When the layperson describes what they think a cyberattack could entail, they often talk of infrastructure or industry failure. Specifically, power grids, banking systems, water provision, taxation systems, and air traffic control are routinely expressed as areas of concern, and for good reason.[26] And of course, an additional high-profile area that is considered prone to attack, and a desirable target, is the voting system of countries.

---

[24]Geir Hågen Karlsen, "Tools of Russian Influence: Information and Propaganda," Chapter 9 in *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, Edited by Janne Haaland Matlary and Tormod Heier, (Cham, Switzerland: Palgrave Macmillan, 2016), 190.

[25]Andrei Soldatov and Irina Borogan, The Red Web, (New York: PublicAffairs, 2015), 281.

[26]Michael N. Schmitt, "The Law of Cyber Targeting," *Naval War College Review 68,* Iss. 2, (Spring 2015), 16.

Recently, a 2014 cyber attack in Germany caused metal fabrication industrial equipment to fail.[27] This has been touted as only the second ever incident, after Stuxnet, where an individual or group has maliciously been able to cause actual damage. There are a couple of points of interest regarding this attack. One is that it is strongly believed that the perpetrators had very fulsome inside knowledge of exactly how the plant operates.[28] Also it is likely that for a cyber attack of this magnitude to have occurred, it is consistent with the resources of a state or nation, and not that typically associated with a group or individual. This brings up the confusion as to this particular incident. Why would a state pick a random manufacturing plant in another country to attack? Was it just practice? If so, there was no need to actually execute the final physical damage. There would have been ample evidence that it was possible without having to actually do it. Was it a message? If so, no one understands except to realize the importance of cyber defence.

The motives behind this attack remain a mystery and further prove another important fact regarding cyber attacks. It can be hard to identify, let alone prove, who is behind them. For example, it is believed that the Kremlin makes frequent use of outsourced groups in order to create plausible deniability.[29] When accused of sponsoring the hacking of the Democratic National Committee in the run-up to the recent US election, Putin chooses his words carefully: "…we do not do that at the *government* level."[30]

There is one reason why the military could be expected to be involved with defending these kinds of attacks, whether by being involved with prevention, or by taking revenge action,

---

[27]Kim Zetter, A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever, *Wired Magazine* online, 8 Jan 2015, last accessed 26 May 2018, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

[28]*Ibid*.

[29]Andrei Soldatov and Irina Borogan, The Red Web, (New York: PublicAffairs, 2015), 320.

[30]*Ibid*., 326.

and that has to do with the military's overall responsibility to defend the homeland. Colonel John Warden III explains his concept of a country's 'protective rings' around its center of gravity.[31] According to him, a country's leadership is at the centre, considered Ring 1. Ring 2 consists of important production. Ring 3 consists of infrastructure. Ring 4 is the population itself, and Ring 5 is the military's fielded forces. Warden believes that stealth and precision weapons have created conditions so that forces no longer have to go through all of the outer rings in a serial fashion to strategically reach enemy leadership.[32] He states how rings can now be crossed over, or alternatively how all rings could now be attacked in parallel, something he refers to as a 'hyper' war.[33]

Cyber takes this one step further. Cyber allows an isolated attack at the individual level in a country. It can happen inside any ring, in any particular spot, without having to 'cross over' any of the other rings. A cyber attack is now an attack on someone else's soil. A country can reach out and touch another country without having left its own part of the world, launched an aircraft, sailed a submarine, or fired a missile. Because the military is an actual physical front line of defence for its country, it could, conceivably, be seen as a reasonable cyber front line.

However, it should be a different agency that leads efforts to protect national industry, civilian infrastructure, and the voting process. There is an element of privacy that is expected by people with regards to their online practices. Just as the military is always careful to be behind the scenes or clearly working for another federal, provincial or local authority when operating within a community for disaster relief, it should strive for a similar profile when it comes to the

---

[31]John Warden, "Success in Modern War: A Response to Robert Pape's Bombing to Win," *Security Studies 7,* no. 2, (Winter 1997/1998), 175.

[32]John Warden, "Employing Air Power in the Twenty-First Century," *The Future of Air Power in the Aftermath of the Gulf War,* edited by Richard H. Schultz, Jr. and Robert L. Pfaltzgraff, Jr., (Maxwell AFB, AL: Air University Press, 1992) 78.

[33]*Ibid*., 79.

cyber realm. It also isn't appropriate for a military to be seen as potentially gathering information on the populace for which it serves, whether online or otherwise. The military also doesn't have the expertise or resources for such an endeavour. Homeland cyber protection of non-military assets should remain with organizations such as Public Safety, the RCMP, the Canadian Security Establishment, the Canadian Anti-Fraud Centre, and the Canadian Cyber Incident Response Centre.[34]

In conclusion, cyber is here to stay. Although there have been many advances in the field since its inception, the number of attacks that have actually caused physical damage or injury is very rare. There are a number of reasons, the foremost being that these efforts are complicated, time consuming, expensive, and often require an element of luck. As such, the countries that are well resourced in other aspects of their military industry remain at the forefront in cyber as well; the Internet has not been the great equalizer as expected. Canada, with its limited resources, needs to prepare accordingly for defence of its assets. It needs to prioritize being able to defend against the Stuxnet and Orchard-style events first and foremost. The next priority needs to be network security along the lines of preventing attacks that required Operation Buckshot-levels of effort to clean up. Thirdly, the background noise of Influence Activities via the Internet need to be addressed from a leadership perspective but are not where Canada should prioritize its resources. And finally, the CAF should not be the lead for cyber protection of civilian industry and infrastructure.

[34]Howard Solomon, "Canada's new cyber security strategy will be based on 5 principles," *IT World Canada*, 15 November 2017, last accessed 28 May 2018, https://www.itworldcanada.com/article/398785-2/398785.

BIBLIOGRAPHY

Adee, Sally. "The Hunt for the Kill Switch." *Institute of Electrical and Electronics Engineers (IEEE) Spectrum Online Magazine May 2008 Edition.* 1 May 2008. https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.

Armistead, Edwin, and Scott Starsman. "Perception Shaping and Cyber Macht: Russia and Ukraine." *International Conference on Cyber Warfare and Security,* (2015).

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" In *Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation, 1997.

Betz, David J., and Tim Stevens. "Conclusion." *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon: Routledge, 2011.

Biesecker, Calvin. "Cyberattacks on Connected Aircraft Are Happening Right Now." *Aviation Today* online. 13 April 2018. http://www.aviationtoday.com/2018/04/13/cyber-attacks-connected-aircraft-happening-right-now/.

Blackwell, Tom. "Russian fake-news campaign against Canadian troops in Latvia includes propaganda about litter, luxury apartments." *The National Post* online. 17 November 2017. http://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments.

Dallek, Matthew. "To Understand the Future of Cyber Power, Look to The Past of Air Power." *Huffington Post* online. 3 March 2017; https://www.huffingtonpost.com/entry/cyber-war-technology_us_58dbfab2e4b01ca7b4294347.

Duvanova, Dinissa, Alexander Semenov, and Alexander Nikolaev. "Do social networks bridge political divides? The analysis of VKontakte social network communication in Ukraine." *Post-Soviet Affairs 31,* Iss. 3. April 2015.

Karlsen, Geir Hågen. "Tools of Russian Influence: Information and Propaganda." Chapter 9 in *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, Edited by Janne Haaland Matlary and Tormod Heier. Cham, Switzerland: Palgrave Macmillan. 2016.

Kushner, David. "The Real Story of Stuxnet" *Institute of Electrical and Electronics Engineers (IEEE) Spectrum Magazine* online. May 2018 Edition. 26 Feb 2013. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Langner, Ralph. “To Kill a Centrifuge, A Technical Analysis of What Stuxnet’s Creators Tried to Achieve.” Arlington, Hamburg, Munich: The Langner Group. November 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Lynn, William J. III. "Defending a New Domain." *Foreign Affairs* 89, no. 5. Sep/Oct 2010. http://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx.

Naraine, Ryan. “Stuxnet attackers used 4 Windows zero-day exploits.” *ZD Net online.* 14 September 2010. https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/.

Rid, Thomas. "Cyberwar Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (Feb 2012).

Schmitt, Michael N. “The Law of Cyber Targeting.” *Naval War College Review 68,* Iss. 2. Spring 2015.

Soldatov, Andrei and Irina Borogan. *The Red Web*. New York: PublicAffairs. 2015.

Solomon, Howard. “Canada’s new cyber security strategy will be based on 5 principles.” *IT World Canada.* 15 November 2017. https://www.itworldcanada.com/article/398785-2/398785.

Szary, Wiktor and Eric Auchard. “Polish airline, hit by cyber attack, says all carriers are at risk.” *Reuters* online. 22 June 2015. https://www.reuters.com/article/us-poland-lot-cybercrime/polish-airline-hit-by-cyber-attack-says-all-carriers-are-at-risk-idUSKBN0P21DC20150622.

Warden, John A. "Success in Modern War: A Response to Robert Pape's Bombing to Win." *Security Studies 7,* no. 2. Winter 1997/1998.

Warden, John A. “Employing Air Power in the Twenty-First Century.” In *The Future of Air Power in the Aftermath of the Gulf War,* edited by Richard H. Schultz, Jr. and Robert L. Pfaltzgraff, Jr. Maxwell AFB, AL: Air University Press. 1992.

Zetter, Kim. “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever.” *Wired Magazine* online. 8 Jan 2015. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

Zetter, Kim. “The Return of the Worm That Ate the Pentagon.” *Wired Magazine* online. 12 September 2011. https://www.wired.com/2011/12/worm-pentagon/.