National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

JOINT PREPAREDNESS FOR CYBER WARFARE

LCdr J.P. Karle

JCSP 40

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 40

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 40 – PCEMI 40

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

JOINT PREPAREDNESS FOR CYBER WARFARE

LCdr J.P. Karle

Word Count: 3501

Compte de mots: 3501

JOINT PREPAREDNESS FOR CYBER WARFARE

INTRODUCTION

The World today finds itself at a very interesting cross roads, one similar to that which we faced in the 1950s and 1960s when we entered the Nuclear warfare era, with all the same potential for destruction, fear-mongering, and the desire and need for direction and policy. However, today it is no longer nuclear weapons that pose the significant threat, but that of the ubiquitous computer. The cyber world has so permeated itself on, within, and through every single aspect of our daily lives, it is difficult for us to even see the problem, never mind define and address it. We, particular those in countries such as Canada, the United States of America, the European Union and other first-world nations, those who are the most entrenched in the cyber world, are particularly vulnerable to this new threat. Modern day war is advancing at an unprecedented rate, with technology propelling the super powers to incredible levels of kinetic power and capability, and engagements like the second Gulf War, are seen as the blueprint for current day warfare, where the victor has the technological advantage and dominates each battlespace domain. However, we are failing to appreciate a seemingly innocuous technological development: that of cyberspace. If we do not recognize the potential threat and power that is inherent in cyber domain, then we risk being unprepared for the changing tide of war. While, "the winner always likes to coast on the path of victory,"[1] where we desire to fight the same kind of war which was last victorious, history has shown that enemy forces learn from their own losses, or from the losses of other, and change tactics. A recent example of this

[1]Qiao Laing and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 125.

is the Taliban's changing from open conflict with coalition forces in Afghanistan, to indirect contact using primarily improvised explosive devices (IED). While no one power can directly challenge the US, nor can most countries afford to confront any first world militaries directly, victory in the future will not be decided by the force of arms, but rather by which force embraces and understands the power and potential of the cyber world. This paper will discuss Cyber Warfare in general, discuss the basic capabilities and the threats inherent in it, and propose how a successful country, and therefore its military, will need to address the realities of cyber warfare through offensive and defensive applications. In short, it will demonstrate that without coordination of effort, education, and a clearly articulated vision for our involvement in the cyber world, we will remain significantly at risk from outside attacks.

WHAT IS CYBER WAR?

When it comes to cyber warfare, running a quick search on the internet, or visiting the local library, reveals several contradictions. You will find many sources addressing the subject, but while each source is very similar in content and examples, they all have their own definition of what constitutes cyber warfare. Prominent US government policy makers define it cyber warfare as "actions by a nation-state to penetrate another nation's computer or networks for the purposes of causing damage or disruption."[2] Notable North American academics expand upon this; their definition includes "everything from military conflict to credit card fraud."[3] Yet, NATO defines it as "weapons … and means

[2]Richard A. Clark, *Cyber War*: *The Next Threat to National Security and What to do About it* (New York: Harper Collins Publishers, 2010), 6.

[3]P.W. Singer, and Allen Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014), 120.

… that are by design, use, or intended use capable of causing either injury to, or death of, persons; or damage to, or destruction of objects."[4] This diversity of definition is one of the struggles inherent in the issue surrounding cyber warfare – if one cannot define the problem, it is hard to develop a plan of action to address it. Perhaps looking at a definition for traditional war will better help define a working definition of cyber warfare.

The military theorist Carl Von Clausewitz defined war as an "act of violence to force an opponent to fulfill our will" through means to achieve a defined objective.[5] He, his contemporaries, and most modern theorists of war, would agree that conflict occurs physically between state-actors, in order to enforce the will of one actor over the other, and that this will is political in nature; hence von Clausewitz' often (mis-)quoted line that "war is only a continuation of state policy by other means."[6] But this does not properly encompass terrorist and other extremist organizations that do not have a specific state affiliation. To include non-state actors, current Canadian policy incorporates ideological motivations in addition to politics.[7]

A more inclusive definition, one which is reflective of current conflict and more befitting of the asymmetric and somewhat intangible nature of cyber warfare, might then be: the actions by state and non-state, actors, who have the means and ways to use, or intend to use, force causing injury, death, or destruction, in order to achieve a political or ideological goal. But this still fails to capture the new threat developing in the virtual

---

[4]The International Group of Experts for NATO Cooperative Cyber Defence Centre of Excellence, edited by Michael N. Schmitt, *Tallin Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 118.

[5]Antulio J. Echevarria, *Clausewitz and Contemporary War* (Oxford: Oxford University Press, 2007), 64.

[6]Carl Von Clausewitz, *On War* (Oxford: Oxford University Press, 2008), 9

[7]Department of Justice, "Definition of Terrorism and the Canadian Context," date modified 07 Jan 2015, http://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rr09_6/p3.html#start

world. It has been hard for recent leaders, theorists, and policy makers to see actions occurring in the cyber world as a threat. After all, this is all virtual – practically make believe, right? As will be explored in the next section of this paper, the threats associated with the cyber world are very real, and not only can they have significant consequences, they can directly affect the physical world. In recent realization of this fact, the Canadian Government has officially defined the cyber threat, stating specifically that "[c]yber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information."[8] This definition at least better reflects that cyber has become:

> ... an integral part of all of our lives, because computers are an integral part of all of our lives, even if you don't own a computer. Computers control everything in your car, from your GPS to your airbags. They control your phone. They're the reason you can call 911 and get someone on the other line. They control our nation's entire infrastructure. They're the reason you have electricity, heat, clean water, food. Computers control our military equipment, everything from missile silos to satellites to nuclear defence [sic] networks. All of these things are made possible because of computers, and therefore because of cyber, and when something goes wrong, cyber can make all of these things impossible.[9]

However, Canada has not yet appreciated the enormity and proliferation of the cyber world with regards to the daily functioning as a nation, nor how vulnerable we are as a developed country, or the fact that cyber attacks and effects are not limited to only the cyber world. Attacks initiated in the virtual world are now reaching into the physical world. We see this lack of understanding across the Government of Canada. It is implicit

---

[8]Department of Public Safety, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Canada Communications Group, 2010), 3.

[9]Chris Domas, "The 1s and 0s behind Cyber Warfare," *TedTalk,* Oct 2013 at min 1:17. http://www.ted.com/talks/chris_domas_the_1s_and_0s_behind_cyber_warfare

in the *Canada First Defence Strategy*, where cyber is mentioned only once; we see it again with the Canadian Armed Forces which has a Cyber Directorate but no formal forces-wide direction on cyber policy. It has direction regarding information management, and proper network use, but none concerning the application of cyber towards offensive and defensive operations. This highlights a lack of unity and vision across Canadian departments, and the fact that defence and offence are being addressed haphazardly by many divisions with varying goals and agendas. This lack of cohesion in and of itself is a threat to our cyber security, and a detriment the nation and to our interaction with national allies.

THE CYBER THREAT

As mentioned in the previous section, the problem with current policy and directives is two-fold. First, there is no coordination or unity between and across the civilian, government and military agencies involved in cyber offence, and most significantly defence. Secondly, and reflected in the limited Canadian doctrine, is that the government, while taking the issue seriously, is only addressing half the problem. In *Canada's Cyber Security Strategy*,[10] while the potential, problems, and impact of cyber conflict is clearly articulated, the government only mentions a plan concerning how the government will integrate cyber response in modern military conflict, and how government systems will be protected. There is only the barest mention regarding helping Canadians to be secure online; there is nothing concerning how to protected Canadians and our associated infrastructure from external cyber attacks or from the second order

[10]Department of Public Safety, *Canada's Cyber Security Strategy: For a Stronger and More*

effects of such attacks. When reading several guiding military documents,[11] cyber is mentioned in terms of it being a developing threat; however, there are no examples of said threat, no direction on how to mediate the threat, and no indication as to guiding principles that should be followed in the development and application of cyber defence and offence.

Cyber threats are much more prolific than depicted in modern media. They are also not well understood by current political and military leaders, for two main reasons. First, generationally the leadership did not grow-up within the connected world and does not appreciate the true significance, ubiquity and proliferation that the cyber world has in the every aspect of our lives, and in the functioning of our country. Secondly, the ability for an individual or a group (sanctioned or not) to be able to gain access to the cyber world and cause a quantifiable effect is greater now than at any other time in history, and will likely remain so until we will have figured out how to manage our vulnerabilities.

Today a mediocre hacker (or just a mischievous teenager)[12] can purchase a fully functional computer that is portable,[13] relatively powerful, runs a modern operating system, and only costs $44 CAD.[14] At this price multiple units may be easily purchased and used to commit a single or series of attacks or crimes, and then just thrown away to make it exceptionally difficult to track down the perpetrator. Even more powerful, equally as portable, and better supported, are several octa-core, and soon to be released

---

Prosperous Canada (Ottawa: Canada Communications Group, 2010), 1-8.

[11]Examples include: Lead Mark 2010, CFJP 1.0, CFJP 3.0, CFJP 5.0, and CF Information Operations.

[12]Daniel Cooper,"Teen Arrested for Breaking an Entire school District's Internet." Engaget, last modified 20 May 2015. http://www.engadget.com/2015/05/20/teenager-idaho-ddos/?ncid=rss_truncated

[13]The significance of a computer being portable is that it makes it much harder for authorities to be able to physically and/or virtually trace the originating computer.

[14]Newark Electronics. "Raspberry Pi 2," last accessed 21 May 2015. http://canada.newark.com/raspberry-pi-accessories

deca-core, smart phones. These phones are incredibly powerful machines, far beyond anything system designers could have envisioned just a few years ago, and even beyond the appreciation of many designers of cyber security today. With the exception of the most recent, high-end personal computers, worth close to $5,000 CAD, the smartphone someone may have in their pocket, or tossed in their purse, is more powerful than most every home computer being used at this time. When we consider that there are in excess of 2 billion personal computers, and an equal number of smartphones,[15] one begins to get a view of the enormity of the problem of vulnerability, where every unit is a potential method of attack against our national defence assets.

These vulnerabilities have been recently been exposed on two separate occasions, when both Russian and Chinese agencies have used very simple techniques to flood targeted networks to first prevent any normal user from accessing webpages, and then to ultimately crash company servers. This type of attack is known as a denial of service (DoS);[16] it has typically been seen as bothersome, but not as something meriting concern or retaliation – such as a physical attack on a sovereign nation would merit. However, consider if such an attack were made against Canadian banks and was sustained for weeks or even months. This would have a staggering impact on the country – certainly the populous areas – and our world allies would loose confidence and withdraw. More serious are persistent attacks, where a hacker (or group of hackers) systematically breaches an organization's cyber defences through a focused and specific attack that has

[15]To appreciate how fast these numbers are increasing, in 1995 there we no smartphones, and 10 million computers.

[16]A DoS attack utilizes a botnet (a network of personal computers, working together unknown to their owners) to overwhelm a server, or system of servers, by flooding it with so many requests that it can not respond to any legitimate request and fulfill it designed function. This is a very easy attack to conduct, and very effective in paralyzing any computer network target.

been tailored to the company or system and is normally undetectable, leaving no trace of having occurred. The United States defence contractor, MacDonald-Detweiler, was subjected to one such attack; while it is known that terra bytes of information were stolen or manipulated – including the plans for the then top secret F-35 Advance Joint Tactical Strike Fighter, the exact extent of the compromise has not been determined. It is quite possible (and very likely) that the perpetrators (suspected to be Chinese in origin) left several logic bombs[17] and backdoors behind, to provide opportunities for manipulation and attack in the future. In fact, it was documented that the F-35's on-board maintenance and monitoring system, which in turn integrates with the rest of the aircraft's systems (flight, navigation, and weapons) was hacked and manipulated by an unauthorized user while the aircraft was conducting a test flight. This demonstrates the very real threat that an enemy agent can hack and manipulate military systems, possibly to the point of catastrophic failure.

It sounds like science fiction, the idea of using a computer to control and affect the physical world through the virtual world. However, using a malicious computer program created by the US that specifically targeted a stand alone network controlling several illegal uranium centrifuges caused a physical and catastrophic failure. The program was called STUXNET and it was highly successful; not only did a program in the virtual world (launched by a keystroke across the world) break the centrifuges in the physical world, but it did so in such an innocuous manner, that the operators of the centrifuges thought their actions or faulty equipment was the cause, not an outside

[17]A logic bomb is a small program purposely coded into a system by a programmer, or placed by a hacker, so it is ready to be activated when needed without having to hack in when the security may have been changed. In its simplest form, a logic bomb is basically an eraser, removing all software and files from the computer. Source: *Cyber War,* 92.

agency. It was not until the program was discovered in a vector computer by a separate, private company specializing in malicious computer programs, that the true cause of the destruction was understood.

Even more frightening is a case where non-stealth aircraft conducted an air raid on an enemy position, deep behind enemy lines; they did so unopposed and without being detected. This was possible because the aggressor had hacked the enemy's radar system, causing the computers to appear as if they were operating normally; however, the system did not detect the inbound aircraft. As a result the target was destroyed, none of the aircraft were lost, and the enemy had no idea they were under threat until the ordnance had impacted the target.

CYBER CONFLICT

What was once thought of as impossible, as science fiction, or at best something we would not have to worry about for decades, is happening now. The cyber world, of which the internet is a massive part, is the 'Wild West' of the modern world. It is generally open to anyone, unregulated, and while providing freedom of communication and connecting us around the world like never before, it is also creating vulnerabilities on a scale never before envisioned or predicted.

Most advanced militaries, including Canada's military, have acknowledged that the primary communications exchange and information repositories occur and reside in cyberspace. In light of this, as well as recent data spills and malicious theft of information (Snowden and DeLisle, for example), militaries have put in place strict policies

concerning the access, use and dissemination of data to, from, and across computer networks. However, this is really the extent of the defensive policy; it does not address the fact that a malicious actor can easily access military networks using readily available software, potential backdoors in existing programming (so called zero days),[18] logic bombs, and even hard-wired malicious system in network computers. For example, many intelligence agencies, including those of the US, Canada, and the UK have banned the use of former IBM, now Lenovo, computers on any classified system. Many will recall IBM as a significant computer manufacturer, but many may not realize that the computer production branch of the company was bought by the Chinese and rebranded as Lenovo. These computers, due to being massed produced and sold at very competitive prices were initially the go-to computer for most price-conscious militaries. It was subsequently discovered that spyware and backdoor access had been encoded in the operating system and hardwired into the computer chips themselves.[19] This later process will not be detected by conventional security programs, and allows unfettered access to everything on the computer and the networks attached to it, without the user knowing that the system has been severely compromised. What about the other purpose built systems, embedded in all our modern fighting equipment; where did their chips come from and how were they proven to be clean?

The modern military is dependent upon computer systems; it has been demonstrated that the capability already exists to remotely hijack these systems and not

---

[18]"Zero Days" is the term hackers give previously unknown vulnerabilities, and are highly prized in the community because an unknown vulnerability is nearly guaranteed to be able to by-pass any existing network security and provide free access to the hacker. Source: *Cyber Security and Cyberwar,* 115.

[19]Mathew J. Schwartz, "Intelligence Agencies Banned Lenovo PCs After Chinese Acquisition." *Dark Reading: Information Week*. Last modified 29 June 2013. http://www.darkreading.com/risk-management/intelligence-agencies-banned-lenovo-pcs-after-chinese-acquisition/d/d-id/1110950?

only create false information, but do so in a manner that reassures the user that their system is working correctly and is therefore a reliable and trust worthy agent. These compromised systems can cause physical damage to equipment and loss of life of personnel. In addition to the aforementioned centrifuge attack, this type of process has been used directly to cause an oil pipeline to explode in Russia, and a sewage pipeline to dump its contents into an ecological reserve.[20]

While we have the ability to use cyberspace to attack our enemies, we have done little to defend ourselves from the vulnerabilities highlighted throughout this paper. In spite of this, in recent conflicts limited cyber weapons have been employed; so far, all sides have shown "considerable restraint in … their use … [and] are probably saving their best cyber weapons for when they really need them."[21]

HOW TO FIX THE PROBLEM?

While the examples of true cyber attacks (not just DoS, APT, and other malicious manipulation normally considered hacks and not attacks) have all occurred outside of North America, this should not provide a sense of security; far from it. As highlighted in previous section of this paper, it can be seen how dependant we are on, and therefore exposed by, the use and reliability of the cyber world. We are an 'overconnected' world, where the interconnect elements are "changing so dramatically that the institutions [governing and utilizing the systems] are overwhelmed … and are unable to cope."[22] This

---

[20]Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill Companies, 2003.), 27.

[21]*Cyber War*: *The Next Threat to National Security and What to do About it*, 21.

[22]William Davidow, *Overconnected: The Promise and Threat of the Internet* (New York: Delphinium Book Inc., 2011), 23.

is evident in Canada's own military, where (due to slowly changing in policy and procedures) a newly contracted network has been installed still running an operating system that has been abandoned by the public, and is no longer supported due to significant security vulnerabilities. In this case, it is due to policy that is unable to adapt to the rapidly changing pace of technology, but also because the policy has been developed without a clear vision of what capabilities are need today and in the near future. Aircraft, ships, and long-range weapon systems, are all examples of systems that are controlled by computer programs and hardware, which were developed, generally, with little thought as to how to prevent unauthorized access, use, and corruption. It was never envisioned (and this ties back to the diversity of definitions for, and therefore realization of what is, cyberspace) that these quasi-standalone systems would be directly attacked. While we have developed an arsenal of offensive cyber abilities, we are lagging behind in defence, by failing to holistically govern the development, procurement and implementation/use of computer-based systems.

To help address this lack of defence without being seen as regulating the internet, governments have reached out to the private sector to self-regulate and provide their own methods of detection and defence. The arising issue, however, is that not every organization approaches the problem the same way or with the same effort.[23] The result is national cyber defence that is being lead by individual civilian organizations in an uncoordinated, disparate, and volunteer manner, with no real understanding if it is providing any effect at all. The lack of policy, vision, and minimum security practices are preventing the development of sound cyber practices.

Canada has made steps in the right direction, placing cybersecurity under Public Safety and cyber warfare under the DND. However, neither department is operating with a clear mandate, an understanding of the desired end-state, nor is there coordinating effort between departments. "Cyber is often confused with computer and information security. But … it is not an add-on; nor is it a stand alone [function]; it is a part of the integrated warfighting effort."[24]

CONCLUSION

A significant cyber attack is inevitable: terrorist organizations are quickly realizing the potential of the cyber world, and opposing forces have demonstrated their ability and willingness to use cyber attacks to further national or ideological goals. While the concept of implementing a WoG approach under Public Safety Canada, and working with agencies such as DND, CSIS and the RCMP is a good first start, PS is not the right organization to lead, coordinate and implement a strategic WoG policy, which can define and take action internally and externally for Canada. A specific department needs to be stood-up that is comprised of membership from each of the aforementioned departments, each of which has been *empowered* by their parent organization, to define and implement policy and change. The goal to should be to: define and implement a concise education process; coordinate effort across departments; and establish a clear vision of what we want to accomplish in the cyber world. Without this, we will remain significantly vulnerable to both external and internal attacks. It is certain, "We find ourselves at the

---

[23]*Black Ice: The Invisible Threat of Cyber-Terrorism*, 35.
[24]Robin Laird, "Training for Cyber Operations." *Frontline Defence* Vol 12:2 (2015), 32

peak of evolutionary pyramid, facing what H.G. Wells called the 'inexorable imperative' to adapt or perish."[25]

[25]*Overconnected: The Promise and Threat of the Internet*, 213.

BIBLIOGRAPHY

Bernier, Melanie and Joanne Treurniet. *Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO.* Ottawa: Defence Research and Development Canada, 2010.

Blackmore, Tim. *War X: Human Extensions in Battlespace*. Toronto: University of Toronto Press Inc., 2005.

Canada. Canadian Security Intelligence Services. "Cybersecurity and Critical Infrastructure Protection," last modified 02 May 2014, https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php Reference Type: Web Page.

Canada. Department of Justice. "Definition of Terrorism and the Canadian Context," last modified 07 jan 2015, http://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rr09_6/p3.html#start Reference Type: Web page.

Canada. Department of Public Safety. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.* Ottawa: Canada Communications Group, 2010.

Chris Domas. "The 1s and 0s behind Cyber Warfare," *TedTalk*. Date posted Oct 2013 at min 1:17. http://www.ted.com/talks/chris_domas_the_1s_and_0s_behind_cyber_warfare Reference Type: Online Speech.

Clark, Richard A. *Cyber War: The Next Threat to National Security and What to do About it.* New York: Harper Collins Publishers, 2010.

Clausewitz, Carl Von. *On War.* Oxford: Oxford University Press, 2008.

Cooper, Daniel. "Teen Arrested for Breaking an Entire school District's Internet." *Engaget,* last modified 20 May 2015. http://www.engadget.com/2015/05/20/teenager-idaho-ddos/?ncid=rss_truncated Reference Type: Online Article.

Davidow, William. *Overconnected: The Promise and Threat of the Internet*. New York: Delphinium Book Inc., 2011.

Echevarria, Antulio J. *Clausewitz and Contemporary War.* Oxford: Oxford University Press, 2007.

Fingas, James. "The US Navy Wants to Protect its Drones Against Hacks." *Engaget,* last modified 20 May 2015. http://www.engadget.com/2015/05/20/us-navy-wants-hack-resistant-drones/?ncid=rss_truncated Reference Type: Online Article.

F-Secure Labs: Security Response Division. "Malware Analysis Whitepaper:

Blackenergy and Quedagh: The Convergence of Crimeware and APT attacks" (2015).

Kraska, James. "How the United States Lost the Naval War of 2015." *Orbis Magazine* (Winter, 2010):

Laing, Qiao and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999.

Laird, Robin. "Training for Cyber Operations." *Frontline Defence* Vol 12:2 (2015): 32-34.

NATO. The International Group of Experts for NATO Cooperative Cyber Defence Centre of Excellence, edited by Michael N. Schmitt. *Tallin Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.

Newark Electronics. "Raspberry Pi 2," last accessed 21 May 2015. http://canada.newark.com/raspberry-pi-accessories Reference Type: Web Page.

Rosenblatt, Seth. "Lenovo's Superfish security snafu blows up in its face." *CNet*. Last modified 20 February 2015. http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/ Reference Type: Online Article.

Singer, P.W. and Allen Friedman. *Cybersecurity and Cyberwar*. New York: Oxford University Press, 2014.

Schwartz, Mathew J. "Intelligence Agencies Banned Lenovo PCs After Chinese Acquisition." *Dark Reading : Information Week*. Last modified 29 June 2013. http://www.darkreading.com/risk-management/intelligence-agencies-banned-lenovo-pcs-after-chinese-acquisition/d/d-id/1110950? Reference Type: Online Article.

Verton, Dan. *Black Ice: The Invisible Threat of Cyber-Terrorism*. New York: McGraw-Hill Companies, 2003.

Vigna, Paul and Michael J. Casey. *The Age of Cryptocurrency: How Bitcoin and Digital Money are Changing the Global Economic Order*. New York: St. Martin's Press, 2015.