CICERO FOUNDATION GREAT DEBATE PAPER

No. 15/03

May 2015

CYBER WARFARE:

IS DETERRENCE AN OPTION?

Draft Manuscript: Do Not Cite without Authors' Permission

BRIAN M. MAZANEC, Ph.D

Adjunct Professor
George Mason University
Fairfax, VA, U.S.A.

BRADLEY A. THAYER, Ph.D
Professor of Political Science
University of Iceland

Cicero Foundation Great Debate Paper No. 15/03

Key Words: Deterrence, Cyber Warfare, Cyber Security, Computer Network Attack, Stuxnet, Information Operations, International Norms

Authors' Identifications and Acknowledgement: Brian M. Mazanec is an adjunct professor at George Mason University and is employed by the U.S. government. Bradley A. Thayer is a Professor of Political Science at the University of Iceland.

They are the authors of *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* (New York: Palgrave Macmillan, 2015), and kindly thank Palgrave Macmillan for permission to republish material from their book for this article.

CYBER WARFARE

Is Deterrence an Option?

Brian M. Mazanec and Bradley A. Thayer

INTRODUCTION

As deterrence of attack has a long history in human affairs, dating to pre-history, so too does the interplay between the rise of new technologies and the resultant need to find a countervailing strategy or weapon for deterrence to obtain once again.[i] The endless race between the development of a new weapon, its application, a defensive response to it, and the adjustment of deterrence theory to address or manage the threat, has entered a new chapter with the rise of cyber warfare.[ii] Cyber warfare presents a new and challenging threat to international relations, and the situation is becoming worse as cyber capabilities and attacks are proliferating. This is acknowledged at the highest levels of the United States government. At his confirmation hearing, Secretary of Defense Chuck Hagel expressed his confidence that 'at this time, it appears that the United States has successfully deterred major cyber attacks' but went on to explain that he expects deterring such major attacks to be a continued key challenge for the United States.[iii]

As former Secretary Hagel recognized, deterrence in this area is challenging because deterrence theory was developed for deterrence of kinetic attacks: deterring the application of force by the armies, air forces, and navies of one's

enemies, and in the nuclear era, the enemy's strategic forces. However, with respect to deterrence, cyber warfare is in many respects unlike what has come before—it is not inherently kinetic. Accordingly, deterrence theorists and practitioners must adapt existing concepts and pursue tailored strategies to help achieve deterrence of cyber warfare with the goal that the result will be an increase in strategic stability in cyberspace. Indeed, there is a reasoned assumption among scholars such as Martin Libicki who have highlighted the concern that cyber deterrence may not work as well as nuclear deterrence, and, if this is the case, it illustrates the need for additional focus on this pressing challenge.[iv]

The major question we address in this article is: in light of the challenges of applying deterrence theory to cyber warfare, how can the United States and its allies successfully deter major cyber attacks? Our central argument is that while deterrence theory faces major challenges when applied to cyber warfare due to the unique aspect of cyber technology, investments and efforts in specific areas can help mitigate this challenge. Specifically, we recommend cultivating beneficial norms for strategic stability; continuing efforts in the area of improving cyber forensics and defenses, including regarding lower evidentiary standards for attributing cyber attacks and addressing harboring 'independent' attackers; and developing and communicating a clear declaratory policy and credible options for deterrence-in-kind so as to make escalation unavoidable and costly. The challenges to applying deterrence theory to cyber warfare relate to pronounced uncertainty with respect to, first, awareness and attribution of an attack; and second, the uncertain effects of any attack.

The difficulties surrounding attribution and control of its effects make deterrence of cyber warfare uniquely difficult. In some cases, lack of control makes the application of the weapon both enticing for the attacker but also risky due to blowback onto his own interests, his own society and economy, and those of his allies, and the risk of escalation by the defender, if, indeed, he is able to determine the attacker. Peter Singer of the Brookings Institution and others have identified this lack of attribution as the key factor that prohibits the direct and immediate application of deterrence theory to the cyber realm.[v] If an attack is attributable, then traditional deterrence applies, including the possibility of a kinetic response. If

an attack is not attributable, or the attacker believes it will be falsely attributed, it may be so enticing a weapon as to be irresistible.

This is an old problem—if you could do something bad and get away with it, would you? This issue has been considered in various guises by philosophers and political leaders throughout history. In *Republic*, Plato provides the example of Gyges' Ring, which made its wearer invisible.[vi] Would a man wearing Gyges' Ring be righteous; alas, no, he concluded. The temptation of being able to get away with something malicious without attribution would be too great, and even a moral man would be corrupted by such power. Cyber weapons give a state a Gyges' Ring, and increasingly, we witness the consequences. The implications of this uncertainty illustrate the need to develop a tailored approach to improve the ability to apply deterrence to cyber warfare. The three efforts we identify in this article will help manage these challenges. These solutions are drawn from lessons from fields such as biology as well as prior experiences dealing with threats such as terrorism and nuclear weapons. For example, microbial forensics provides important and useful examples for answering the critical 'who did it?' question. We argue that policy makers can learn from experiences in other areas, such as biological weapons and forensics, and in doing so develop an effective package of responses to improve deterrence of cyber warfare.

OVERVIEW OF CYBER WARFARE

Cyberspace operations are the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace.[vii] Hostile operations can come in the form of Computer Network Exploitation (CNE), like the espionage-style attacks mentioned earlier, as well as true Computer Network Attack (CNA).[viii] CNA is the use of computer networks to disrupt, deny, degrade, or destroy either the information resident in enemy computers and computer networks, or the computers and networks themselves. This understanding of cyber warfare, focused on CNA between state actors—directly or through plausibly-deniable non-state clients—will be the focus of this article rather than more-frequent CNE attacks, which uses computer networks to gather intelligence on an adversary.[ix] However, as might be

expected, there is a blurred line between CNA and CNE activity as CNE can elevate to an actual attack with mere keystrokes. As with other forms of warfare, CNA-style cyber warfare targeting can be countervalue, that is, focused on civilian targets like the United States banking industry, or counterforce, focused on military personnel, forces, and facilities, United States Pacific Command, for example.

CNA-style attacks pose the most serious threat and therefore the deterrence of these attacks is of paramount importance to national security. In 2010, *The Economist* envisioned the most extreme of major CNA-style cyber attacks when it described 'the almost instantaneous failure of the systems that keep the modern world turning. As computer networks collapse, factories and chemical plants explode, satellites spin out of control and the financial and power grids fail.'[x] The targets of such an attack could include hospitals, Supervisory Control and Data Acquisition (SCADA) industrial control systems for chemical or nuclear plants, water filtration systems, transportation systems such as air traffic management systems or subways, banking and financial systems, and the electrical grid itself.[xi]

The United States and its allies must systematically confront this growing and significant threat. While any approach will involve numerous avenues, ranging from export-control regimes to mitigate proliferation of cyber weapons to the development and training of a new cadre of cyber warriors, deterrence must be part of the solution.

DETERRENCE THEORY

Deterrence theory is largely associated with nuclear policy. During the Cold War the United States and Soviet Union adopted a survivable nuclear force to present a 'credible' deterrent that maintained the 'uncertainty' inherent in a strategic balance as understood through the accepted theories of major theorists like Bernard Brodie, Herman Kahn, and Thomas Schelling. Theories of deterrence were largely developed early in the Cold War by academics coming to grips with the intellectual conundrum and novelty of the political and military impact of nuclear weapons, and arguably prevented a world war by allowing policymakers to understand how

nuclear weapons affected traditional tools of statecraft—deterrence and coercion—and the risks associated with nuclear war.

The concept of deterrence is about keeping an opponent from doing something that you do not want him to do by making a threat of unacceptable consequences. In order to work, nuclear deterrence requires a broad range of capabilities, and not just nuclear or other military forces but also economic and diplomatic means, and these capabilities must be directed at the many actors the United States seeks to deter—from rising peer competitors like China, new nuclear states like North Korea, emerging nuclear states like Iran, to al Qaeda and associated movements, and today, cyber attacks.

Keeping someone from doing something you do not want him to do may be brought about by threatening unacceptable punishment if the action is taken, this is called deterrence by punishment (the power to hurt), or by convincing the opponent that his objective will be denied to him, if he attacks, deterrence by denial (the power to deny military victory). Both forms of deterrence may apply in the case of a cyber attack, however two major problems exist.

AWARENESS OF CYBER ATTACK AND ATTRIBUTION

The first major problem of most cyber weapons is the challenge of becoming aware of the attack and properly attributing the attack once it has occurred. These problems are extremely difficult to resolve as a result of the tremendous difficulty in conclusively determining the origin, identity and intent of an actor/attacker operating in this domain, compounded by the fact that defenders generally lack the tools needed to reliability trace an attack back to the actual attacker. As Rid argues, all cyber attacks to date have been examples of sophisticated forms of sabotage, espionage, and subversion and are reliant on this attribution difficulty. Cyberspace is truly global and nearly all action passes through networks and ISPs in multiple countries. Additionally, the hardware used to conduct cyber warfare can be owned by innocent noncombatants, illicitly harnessed for malicious use through the use of computer viruses, as was the case in the 2007 Estonian and 2008 Georgian attacks.

In April 2007, Estonia suffered significant disruptions on their Internet and Web based services that lasted for several weeks and consisted of 128 unique DDOS cyber warfare attacks. At its peak, traffic originating from outside Estonia was 400 times higher than its normal rate and involved approximately 100 million computers from more than 50 countries—highlighting some of the issues associated with the attribution challenge. The attackers executed the attacks using a series of botnets that hijacked innocent bystanders' computers. The Russian attack on Georgia in July 2008 is another example of cyber warfare conducted against a former Soviet state in order to achieve political and military effects while simultaneously maintaining plausible deniability that undermines deterrence. Prior to the military invasion, a large-scale DDOS attack shut down Georgian servers and, as the invasion began, the attacks increased and spread to other targets. The attack was likely organized by the Russian government to support its broader political and military objectives in the crisis, but executed by loosely-affiliated 'independent' hackers that strengthen the government's plausible deniability.

In 2014, another cyber attack occurred during the crisis in Ukraine. This attack involved a weapon known as 'Snake,' which, as discussed earlier, is of suspected Russian origin although, at the time of writing, positive attribution has not been achieved. The Estonian, Georgian, and Ukrainian experiences highlight the challenges associated with uncertainty and attribution in cyberspace. Millions of devices continue to be compromised and used illicitly as part of a various networks— 'botnets'—utilized to conduct cyber attacks. This also provides plausible deniability to state sponsored activity.

While it is a CNE-style attack and not CNA, the Conficker worm, first detected in November 2008, is a major illustration of the challenge of attribution in cyberspace. It is suspected that Conficker is of Ukrainian origin because it did not target Ukrainian IP addresses or computers using Ukrainian-configured keyboards. Of course, a savvy adversary could have programmed that component as part of its deception strategy. Another CNE-style attack highlighting the attribution challenge, this one on a U.S. Department of Defense Solaris computer operating system and known as 'Solar Sunrise,' originally appeared to be coming from Harvard University and then other universities in Utah and Texas. For almost a month, officials did not

know the origin or number of hackers involved and the Deputy Secretary of Defense, John Hamre, informed President Clinton that the attacks were suspected to have been planned by operatives in Iraq in response to the threat of additional U.S. airstrikes. However, highlighting the challenge of attribution in cyberspace, later investigations determined the attack was conducted by two teenagers in California who were merely recreational hackers and not acting on behalf of any nation state.

In all of these attacks—Estonia, Georgia, Conficker, Snake, and Solar Sunrise—the attackers used botnets and routed their attacks through various IP addresses, which are akin to phone numbers or physical locations on the Internet. While it is possible to trace this path of the attack back through the IP addresses to the original source, doing so requires information from the ISPs involved (often obtained by law enforcement through a court order). This can take time and make attribution and 'hot pursuit' in cyberspace impossible. Additionally, this complex process can complicate maintaining the integrity of the 'chain of evidence' and allows foreign ISPs to delay or impede the investigation. The resulting evidence and accusation may become suspect in the proverbial international court of public opinion.

Finally, if quality evidence tracing an attack back to its origin is obtained, it still may not lead to attribution of the attack. Knowing the originating IP address of an attack vector will not necessarily indicate who the attacker was or if they were acting with state support or direction. Sometimes an analysis of the malware itself can provide clues, but these could just as easily be deliberate decoys intended to lead investigators astray and are unlikely to result in firm attribution of a cyber attack. Of course, in some instances tracing of the path of the attack across the Internet is particularly useless—such as when the malware payload is delivered to its target via alternate means, such as via a human delivery with a medium such as a USB drive or direct radio or sonic transmission discussed earlier. This particular challenge is present in the Stuxnet attack, which was an extremely sophisticated computer virus that successfully attacked Iranian industrial control systems associated with their nuclear program.

The challenges of attribution in cyberspace make it very difficult to attribute hostile action in cyberspace to a particular individual, organization, or state and so

make cyber warfare particularly appealing for an adversary that wants to execute an attack anonymously or at least with reasonable deniability. This poses significant challenges for achieving offensive deterrence against cyber attack as an adversary can have some reasonable expectation that it may be impossible to fully attribute the attack and impose reliable costs for the action.

UNCERTAINTY REGARDING CYBER WEAPON EFFECTS

The second major characteristic of cyber weapons that significantly impacts the logic of deterrence is the uncertainty regarding their effects. Due to the potential for IT network evolution as well as IT interdependencies, it is difficult to predict the precise effects of an attack. In cyberspace, the targeted actor is capable of literally flipping a switch and instantly changing the network, or even unplugging it altogether. This factor is a destabilizing force as it rewards immediate hostile action to prevent network modification if cyber reconnaissance-targeting intrusions are later detected.

In essence, it is the opposite of stable deterrence and akin to nuclear crisis instability where nuclear deterrence may fail because it incentivizes a first strike. Defenders may also have unknown automated countermeasures that negate the desired effects of cyber attacks, such as instantaneous network reconfiguration or firewalls. For example, the Stuxnet attack is likely no longer able to continue to attack Iranian nuclear facilities as the zero-day exploits it utilized have been plugged by Iranian officials. In addition to network/target evolution, cyber weapons themselves can also be unpredictable and can evolve. A cyber weapon can adapt—as was seen with the Conficker virus. Conficker included a mechanism that employed a randomizing function to generate a new list of 250 domain names, which were used as command and control rendezvous points, on a daily basis. Thus the virus remained adaptable and stayed ahead of those seeking to shut down or hijack the illicit Conficker-enabled network.

Network interdependencies are another dynamic contributing to the potential for collateral damage that is characteristic of cyber weapons. Because the Internet is made up of hundreds of millions of computers connected through an elaborate and organic interwoven network and it is the backbone of much of the

global economy, there is the potential for significant unintended and collateral impacts from cyber action. This interconnected nature of IT systems has led to real-world collateral damage. For example, the 2007 Israeli cyber attack on Syrian air defense systems as part of Operation Orchard, was believed to have also damaged domestic Israeli cyber networks. Fear of this kind of cyber collateral damage has had a profound effect on military planning.

As another example, in 2003, the United States was planning a massive cyber attack on Iraq in advance of any physical invasion—freezing bank accounts and crippling government systems. Despite possessing the ability to carry out such attacks, the Bush administration canceled the plan out of a concern that the effects would not be contained to Iraq but instead would also have a negative effect on the networks of friends and allies across the region and in Europe. The adverse consequences of such unintended results were powerful deterrents for the United States. Of course, this is not say that other states would be similarly deterred from such actions, especially states that do not have the alliance obligations and responsibilities of the United States.

The uncertain effects cyber weapons coupled with the availability of defenses and the need for secrecy and surprise, reduces their ability to serve as a strategic deterrent in their own right. Available defenses and the potential for network evolution to mitigate the effects of an attack given early warning requires cyber attackers to rely on surprise for much of their effectiveness. To achieve surprise, secrecy is required, reducing the ability of a state to make credible threats without compromising their cyber warfare capabilities. Credible threats regarding specific means of attack or targets invite the threatened state to take protective actions which could blunt the deterrent value of a threat.

Essentially, although cyber weapons have the potential to inflict unacceptable damage against an adversary, they are likely unable to offer states a credible, consistent, and 'assured' capability for doing so. This deficiency significantly undermines their suitability as a deterrent tool and instead they are more likely to support an intelligence, surveillance, and reconnaissance mission, or to be used as a first strike weapon, preemptively, or as force multipliers.

Deterrence offered a solution to other serious threats in the past—most notably nuclear weapons—but due to the pronounced uncertainty surrounding cyber attacks, deterring cyber warfare is particularly difficult. The implications of these challenges illustrate the need to develop a tailored approach to improve the ability to apply deterrence to cyber warfare. Our recommendations focused on cultivating beneficial norms regarding lower evidentiary standards for attributing cyber attacks and addressing harboring 'independent' attackers, continuing to improve cyber forensics and defenses, and developing and communicating a clear declaratory policy and credible options for deterrence-in-kind so as to make escalation unavoidable and costly.

Detailed efforts to develop further specific action plans for implementing each of these recommendations is beyond the scope of this study but merits additional examination. Continuing to work to develop effective deterrence strategies to prevent adversaries from employing these weapons against critical targets is essential to preserving the global economy, U.S. national security, and the coherence of the domain of cyberspace. Future technical and policy research should focus on: first, organizational and technical avenues to improve forensic attribution in cyberspace; second, examining how to develop and strengthen international norms for reduced evidentiary standards for cyber attack; and third, the development of effective declaratory policies to achieve deterrence, which might include cyber deterrence-in-kind or other forms of declaratory deterrent threats that could be leveraged to prevent cyber warfare from occurring or escalating.

Anchored in core principles of deterrence and coercion, nuclear deterrence theory matured rapidly and was immensely helpful during the Cold War when its insights provided policymakers with a framework for understanding the impact of nuclear weapons on international politics. Today, we face circumstances similar to the nascent development of nuclear deterrence theory. Nuclear deterrence theorists wrestled with key questions such as 'how much is enough,' and what nuclear force structure was necessary to deter. Presently, cyber deterrence

theorists grapple with the pronounced uncertainty surrounding cyber attacks. Just as nuclear deterrence theorists resolved their conceptual puzzles, we are confident that cyber deterrence theorists will navigate cyber labyrinths and warrens to solve the problems we have identified. While the difficulties should not be underestimated, if these challenges are met, deterrence of cyber attacks is possible.

We recognize the difficulties of each of these steps. The risks associated with cyber exploitation and attack are often far below the surface, and often esoteric. We understand why businesspeople would not want to incur the costs of securing their systems for a threat that does not seems to affect them, and only adds a another layer of expense. Such an opinion is reasonable and compels a broader educational policy from the government to increase awareness of the threat so that cyber security becomes as natural as the physical security of a business. Weaving business, utilities, local governments together into cyber defense strengthens deterrence. This should be explained to those who doubt the need for another expense or complication.

Of course, despite the roles required of other actors, the principal responsibility lies with the U.S. government. The steps we have suggested will assist the ability of the United States and its allies to deter attack. We recognize that these measures are only steps in the right direction, and will not stop all cyber attacks. This is because the cyber weapon, as with any weapon will be useful to states and other international actors in the right circumstances, or due to the paucity of options they possess.

Deterrence of cyber attacks is not an impossible task but more needs to be done. If we make a historical comparison, it is as though we are in the late 1940s, we know that atomic weapons are different, but we have not created a force structure, mapped out their political and military roles, and their impact on statesmen and international politics. Moreover, the discoveries of fusion weapons are before us, as are crises.

Just as in the early Cold War, statesmen, scholars, and defense analysts have to develop the parameters of the cyber weapon. They need to think through its role, political effects, consequences of use, likelihood of escalation within the cyber realm and its bridge to kinetic weapons. There are a significant number of important and

nettlesome concepts to consider and 'run to ground.' Indeed, despite important contributions to the field, no one has yet written the equivalent of *On Cyber War*, a classic work like Clausewitz's that would capture the logical essence of the cyber weapon and its relationship to politics and strategy. Indeed, even the counterpart of Brodie's *The Absolute Weapon* remains to be written. Equally, just as in the late 1940s, as technology develops, we should expect new developments that make attacks and exploitation more effective. The intellectual constructs of cyber warfare are yet to be defined. The policies are not yet in place. The conscious of vulnerability and the need to address the problem are not present. Thus, the vulnerability of the United States to cyber remains. Because states are often slow to react effectively to threats, it is likely that the United States will suffer additional attacks, some of which may be severe with dramatic and unfortunate effects. Perhaps it is too pessimistic, but our concern is that only then will there be progress on deterrence of cyber attack and development of defenses due to the aftermath of the attack and the concomitant urgency and focus of the U.S. government and its allies.

NOTES

[i] For the considerable evidence regarding warfare in pre-history see Azar Gat, *War in Human Civilization* (Oxford: Oxford UP 2006); and Lawrence H. Keeley, *War Before Civilization: The Myth of the Peaceful Savage* (Oxford: Oxford UP 1996).

[ii] We agree with Adam Liff's definition of cyber warfare as 'a coercive (political) act involving computer network attack that is distinct from cyber espionage, hacking, and crime. Adam P. Liff, 'The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio,' *The Journal of Strategic Studies* 36/1 (Feb. 2013) 134-138, 137. In addition, we concur with Gary McGraw's insights: 'Cyber requires a consequential impact in the physical world, or what military experts call a 'kinetic' effect,' he continues, 'In the end, war is the application of force to achieve a desired end. To qualify as cyber war, the means may be virtual but the impact should be physical.' Gary McGraw, 'Cyber War Is Inevitable (Unless We Build Security In),' *The Journal of Strategic Studies* 36/1 (Feb. 2013) 109-119, 112.

[iii] John Reed, 'Cyber Deterrence is Working, Hagel Tells Senators,' *Foreign Policy* (30 Jan. 2013), <http://killerapps.foreignpolicy.com/posts/2013/01/30/cyber_deterrence_is_working_hagel_tells_senators>.

[iv] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Washington, DC: Rand 2009), xvi

[v] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford UP 2013), 144-148.

[vi] Plato, *Republic*, trans. by Allen Bloom (New York: Basic Books, 1968), 37-38.

[vii] Dennis Murphy, 'What is War? The Utility of Cyberspace Operations in the Contemporary Operational Environment,' Issue Paper Vol. 1-10, *Center for Strategic Leadership*, U.S. Army War College (Feb. 2010), <http://www.carlisle.army.mil/DIME/documents/War%20is%20War%20Issue%20Paper%20Final2.pdf>.

[viii] United States Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (15 May 2011), 93

[ix] United States Government Accountability Office, *GAO-11-695R: Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates* (Washington D.C.: 29 July 2011), 10.

[x] *The Economist*, 'Cyberwar' (1 July 2010), <http://www.economist.com/node/16481504>.

[xi] FireEye, 'World War C: Understanding Nation-State Motives Behind Today's Ad vanced Cyber Attacks' (30 Sep. 2013), 20.

The Cicero Foundation

Independent Pro-EU and Pro-Atlantic think tank

Founded in 1992

Hondertmarck 45D

6211 MB MAASTRICHT

The Netherlands

Tel. +31 43 32 60 828

Tel. +33 1 41 29 09 30

Fax: +33 1 41 29 09 31

Email: info@cicerofoundation.org

Website: www.cicerofoundation.org

Registration No. Chamber of Commerce Maastricht 41078444