Journal of Military and Strategic Studies

VOLUME 14, ISSUE 2, 2012

State of the Art: Attackers and Targets in Cyberspace[1]

John B. Sheldon, Ph.D.

Introduction

The remit of this article is broad, and so the themes explored here are necessarily broad-brush and are viewed from a strategic and policy perspective. The subject under consideration is that of cyber threats – what is it that we confront, and what dangers do they plausibly pose? Anyone even remotely familiar with the topic will know that cyber threats regularly receive extensive media coverage of varying quality, and are increasingly on the agenda of senior policy makers, military commanders, chief executive officers, and political leaders. More recently, cyber threats are becoming more well-known to members of the general public, whose lives are increasingly mediated through and dependent upon cyberspace in some form or another. The specter of criminality, such as theft of financial resources and personal identifying information, stalking, and the unwitting suborning of personal property (computers harnessed by botnets) for other criminal enterprises, is finally receiving the attention it deserves.

In light of the greater attention that cyber threats are receiving, this article argues that there are indeed real cyber threats that could potentially harm, even seriously

[1] The views expressed in this paper are those of the author alone, and do not necessarily reflect the views of the George C. Marshall Institute or The Torridon Group LLC.

ISSN : 1488-559X

harm, core national security interests, but that these threats require extensive, even onerous, preparations and resources and will more likely be accompanied by other, more traditional, forms of hostile action. Other, low-level, threats undoubtedly exist and do have the potential for damage but can be prevented or mitigated by adopting a holistic culture of cyber security, greater resiliency, an evolving offense-defense dynamic, and by sensibly differentiating core interests from transitory and lesser interests in order for the proper institutions and resources be better and more efficiently assigned to counter such threats. Without the ability to differentiate cyber threats, there is a danger that the creeping militarization of all cyber threats can, paradoxically, leave military establishments ill-prepared for the cyber threats that will really matter.

In order to explore and analyze these issues this article takes the following approach: first, working definitions of cyberspace, cyberpower, and strategy are provided; second, a taxonomy of cyber threat actors, generic motivations for cyber threats, and various means of cyber attack is outlined; third, the article briefly discusses the characteristics and attributes of cyberspace that allow cyber threats to take on the specter that they now enjoy; and fourth, a synthesis of all these is combined in to an analysis that seeks to persuade the reader that not all cyber threats – in all three of their elements of actor, motivation, and means – are created equal and therefore will require very different government policy and private sector responses.

Definitions

Like many other disciplines, the field of strategic studies places a premium on definitions even though, in reality, they are always contextually and culturally situated. For example, an American definition of air power may not necessarily resonate with, say, a Ugandan definition, given the vast differences in historical and operational experiences, as well as differences in capability and how the instrument of air power is wielded in order to achieve political objectives set out by the respective polities. Ultimately, however, definitional debates about air power, as well as land- and sea power, tend to revolve around a handful of similar but competing definitions.

But cyberspace, and its consequential product, cyberpower, face different challenges. By 2012, there are at least 18 competing definitions of cyberspace and

several competing definitions of cyberpower being actively used and debated on a worldwide platform.[2] Much of this definitional fruit salad can be explained away by the fact that as strategic phenomena both cyberspace and cyberpower are relatively new when compared to land, sea, air, and space power. However, it is equally plausible to consider the possibility that this dilemma exists because – as many strategists are learning, to their discomfort -- cyberspace is an intangible, fluid, and counterintuitive phenomenon that defies the neat categorizations of the other strategic domains. The strategic effects that can be produced from cyberspace - cyberpower - are somewhat easier to grasp, though, in many cases, they are either exaggerated, under-appreciated, or ignored.

Cyberspace

The term cyberspace was first coined in a 1981 short story by Canadian science fiction writer William Gibson. Defined then as a consensual hallucination that takes place when humans interact with computers, the term has morphed and evolved ever since.[3] The wide array of working definitions attempt to give cyberspace a certain tangibility and uniformity similar to the definitions of land, sea, air, and space power. Such definitions fall under the "inclusive model"[4] of cyberspace in that they emphasize the physical manifestations of cyberspace -- such as computers and networks and other parts of the infrastructure – as well as the code that makes the machines and networks function. Other definitions, by far in the minority, fall under what is known as the "exclusive model"[5] of cyberspace. In this model, the physical element is not mentioned, and instead cyberspace is represented as an informational and virtual place that exists within an infrastructure that is implied. This type of definition emphasizes the previously mentioned cognitive element, where the human being interacts directly with

[2] On the plethora of definitions for cyberspace, see Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Dulles, VA: Potomac Books, 2009), pp. 26-27.
[3] See William Gibson, *Neuromancer* (New York: ACE, 1984), p. 51.
[4] On inclusive and exclusive definitions of cyberspace, see David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (Abingdon, Oxon.: Routledge for the International Institute for Strategic Studies, 2011), pp. 36-37.
[5] Betz and Stevens, ibid.

information created, stored, and transmitted within cyberspace. The major definitions in circulation today (inclusive and exclusive) vary from each other in their specific understanding about what constitutes cyberspace. As a result, some definitions include certain features that may be found in cyberspace, while others omit those same features. By their nature, definitional wars can be tedious to those not directly involved. But, in the case of cyberspace, what is and what is not included in any definition may have serious implications for its strategic application:

> The issue of defining cyberspace is not trivial. What we decide to include or exclude from cyberspace has significant implications for the operations of power, as it determines the purview of cyberspace strategies and the operations of cyber-power.[6]

A good example of this issue can be found among cyberspace definitions that fall within the inclusive model, where some definitions include the naturally-occurring electromagnetic spectrum (EMS) and others do not. The important point to understand is that inclusion or exclusion of the EMS in definitions can determine how cyberspace operations are conducted. This paper, therefore, takes as its working definition of cyberspace the one offered by Dan Kuehl, where cyberspace is:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[7]

Ultimately, while definitions do matter and a kind of winnowing process is likely to occur among the plethora of definitions of cyberspace, one cannot escape the reality that whatever one's preferred definition is, numerous actors are operating in cyberspace creating all kinds of effects every day.

[6] Betz and Stevens, ibid., p. 36.

[7] Kuehl, op.cit., p. 28. Emphasis in the original text.

Cyberpower

If cyberspace can be generally described as a place or domain where information can be created, stored, transmitted, and generally manipulated, then cyberpower can be described as the process of converting information into a strategic effect. This strategic effect ultimately manifests itself in the cognitive processes of human beings, but it can also indirectly manifest itself in the strategic domains of land, sea, air, and space, as well as cyberspace itself.

Strategy

Finally, a working definition of strategy is offered that not only best captures the long-term workings of the dimensions of strategy, but also best exemplifies the symbiotic relationship between strategy and war.

All too often strategy is mistaken for plans or vision when in fact it is neither of these.[8] Strategy, from a national security perspective, provides the bridge between what is politically desired and what is militarily feasible.[9] The strategist must be able to convert the political imperative in to politically relevant military results. As any analysis of NATO military performance in Afghanistan will attest, this is not only extremely difficult to do but finding people capable of doing it is even more difficult.[10] However, strategy is very much wrapped up in war and how it is conducted, even if strategy is invariably done badly. Hence, strategy is defined here as "managing context for *continuing advantage according to policy*."[11]

---

[8] See Harry R. Yarger, *Strategy and the National Security Professional: Strategic Thinking and Strategy Formulation in the 21st Century* (Westport, CT: Praeger, 2008), pp. vii-viii.
[9] See Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), p. 17.
[10] On this point, see Steven Jermy, *Strategy for Action: Using Force Wisely in the 21st Century* (London: Knightstone Publishing, 2011); Jermy, formerly of the Royal Navy, served in Afghanistan and was taken aback at both the lack of strategy guiding operations toward a political objective, and the prevailing attitude that strategy was not needed.
[11] Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (London: Frank Cass, 2005), p. 6.

Cyber Threats

In *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada,* the Canadian government identifies three broad sources of cyber threat to Canadian security and economic interests: cyber espionage and military operations by foreign countries (or their proxies); terrorist use of cyberspace; and cyber criminal activity.[12] These broad threat activities accurately capture the most important threats, but a more detailed taxonomy of cyber threats can be made that identifies not only generic types of threat actors, but also their generic motivations, and also the means of cyber attack that these actors commonly use. As an aside, it should be noted that all threat actors make use of what are commonly referred to as hackers. The popular image of the hacker – a highly intelligent but socially inept young male at odds with mainstream society – is sometimes a fair reflection, but more often than not hackers defy stereotype, and not all hackers are engaged in shadowy, even illegal, activities. All threat actors described below comprise of, and employ, a variety of white-hat (good guys), grey-hat (ambiguous), and black-hat (bad guys) hackers.[13] The following taxonomy provides further granularity on particular threat actors, their generic motivations, and the types of cyber capabilities they commonly use, and does so in approximate order of threat:

- Nation-states: countries are the only actors who possess the human and financial resources to conduct large-scale and destructive cyber operations on a persistent or regular basis. Nation-state cyber activities primarily involve espionage and military/covert operations that require large numbers of specialist personnel and the bureaucracies to manage them, infrastructure ranging from research and development entities able to provide cutting edge technologies and methodologies through to hardware and facilities, financial and human resources, and also the political legitimacy and/or veil of secrecy required for potentially controversial cyber operations. Nation-states are generally motivated by the constant need for information on the intentions and activities of other nation-states, terrorists and criminal organizations, and commercial entities. Hence the prevalence today of espionage via cyber means as all forms of

[12] See *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Government of Canada, 2010), p. 5.
[13] For a more detailed discussion of hackers and their various types, see Betz and Stevens, op.cit., pp. 16-34.

information continues to migrate to cyberspace.[14] Nation-states are also motivated by the timeless triumvirate of fear, honor, and interest, as masterfully articulated by Thucydides in his *History of the Peloponnesian War*.[15] Nation-states develop offensive cyber capabilities out of fear that they will fall behind rivals and adversaries, thus finding themselves at a perceived disadvantage. Nation states also develop offensive cyber capabilities because doing so denotes a certain technical élan and can bolster a nation-state's reputation in national security at home and abroad. Finally, nation-states develop offensive cyber capabilities because it is perceived to be in their interests to be able to act with a certain degree of freedom in a perpetually contested cyberspace. Furthermore, it is their interest because rivals and adversaries who are cyber-dependent to varying degrees are therefore vulnerable to possible cyber attack. Nation-states use the panoply of cyber attack capabilities and methods, ranging from the most sophisticated and precise malware (such as Stuxnet, believed to have been created by a nation-state) and the more blunt method of denial of service attacks, through to sophisticated spear-phishing campaigns targeting leading persons of interest. Nation-states are the most capable and dangerous threat actors in cyberspace.[16]

- Terrorists: terrorist organizations seek to create acts of terror against public targets in order to make political statements, or even in order to try and achieve political objectives (though the latter rarely, if ever, succeeds through the use of terrorism). At present cyberspace is useful to terrorist organizations since it provides a virtual presence for various groups, and is a very useful conduit for funding, recruiting, and even training in terrorist tactics. A number of terrorist groups engage in cyber crime in order to raise money for terrorist operations. Terrorists also use social engineering methods to identify human targets and also use cyberspace to gather intelligence in support of operations. Ultimately,

[14] For a U.S. perspective on this, see Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: The Penguin Press, 2011).
[15] See Robert B. Strassler (ed.), *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War* (New York: Free Press, 1996).
[16] For a recent overview of nation-state cyber warfare activities, see McAfee's *Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare* (Santa Clara, CA: McAfee, 2009).

however, cyberspace is extremely useful to terrorist organizations since it provides that most precious of commodities to such groups – publicity; and in the case of cyberspace, it provides publicity on a global scale.[17] So far, however, there is no evidence to suggest terrorist group involvement in cyber attacks against critical infrastructure, networks, and the information stored on those networks. Yet as a more cyber savvy and technically knowledgeable generation of terrorists emerge, the specter of cyber attacks using cyber capabilities procured 'off-the-shelf,' specially commissioned from rogue hackers or criminal organizations, or even handed to terrorist organizations by better resourced state sponsors. These potential cyber attacks would likely focus on high value and prominent targets, such as key infrastructure, that would generate fear and terror among the public, leave authorities flailing in response, and would generate tremendous publicity for their cause. At present, terrorists generally use social engineering and data mining methods to support their efforts in the physical world, as well as tools commonly used to conduct cyber crime in order to fund operations – such as online credit card fraud. In the near future, however, it is not unreasonable to assume that certain terrorist organizations (though by no means all) will start to use more powerful capabilities to devastating effect.[18]

- Criminal Organizations: criminal organizations – large and small – find a cornucopia of criminal opportunity in cyberspace, as a result of the continuing migration of sensitive personal, financial, and proprietary information to cyberspace. Cyber crime is the latest incarnation of criminal activity that has taken place with the advent of the postal system, the telegraph, and the telephone. Indeed, many of the methods required for cyber crime, such as social engineering, have their antecedents in postal, telegraph, and telephone fraud. Of course, cyber crime is about more than just fraud, it also involves selling personal

[17] The best overview on terrorist use of cyberspace to date can be found in Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: The United States Institute of Peace Press, 2006).

[18] On the possibility of terrorist use of cyberspace becoming more lethal, see J. Piag Charvat, "Cyber Terrorism: A New Dimension in Battlespace," (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, no date), http://www.ccdcoe.org/publications/virtualbattlefield/05_CHARVAT_Cyber%20Terrorism.pdf Accessed July 19, 2012.

identifying information, such as financial information and social security numbers, to other criminal organizations, terrorists, and even governments. It also involves espionage activities where proprietary information is then sold on the black market, and, of course, it mostly involves the theft of money from individuals and institutions. These criminal activities are more often than not ends in themselves, but often the fruits of cyber crime fund other criminal activities in the physical realm, such as the trafficking of drugs, weapons, and people, and can also be used to subvert lawful institutions and buy influence in order to create a more favorable environment for further criminal activity. Ultimately, the motivation for cyber crime is straight-forward – monetary gain.[19] This unending quest for the bottom line has been a surprising wellspring of innovation among certain criminal organizations in terms of cyber crime methods, techniques, and capabilities. While, to date, criminal organizations have not demonstrated the capability to develop sophisticated and precise malware such as Stuxnet, they have developed 'off-the-shelf' capabilities that are adept at creating botnets and generic malware that enable the criminal enterprise, and ironically, have even found a lucrative market for these capabilities.[20]

- Disgruntled Insiders: so far, nation-states and terrorist and criminal organizations rate as perhaps the most dangerous cyber threats to national security and economic interests, but another category of cyber threat exists that is perhaps not as persistent, but can certainly be as damaging, as the cyber threats already outlined. Insider threats can be crippling if carried out, as the incident involving Vitek Boden's malicious attack against the Maroochy Shire sewerage system in Queensland, Australia, demonstrates. Boden, a contractor who helped develop the control systems for the sewerage system had a job application to Maroochy Shire Council rejected, and so used his inside knowledge of the

[19] By far the most comprehensive treatment of cyber crime can be found in Misha Glenny, *DarkMarket: Cyberthieves, Cybercops and You* (New York: Alfred A. Knopf, 2011).
[20] See, for example, *A Good Decade for Cybercrime: McAfee's Look Back at Ten Years of Cybercrime* (Santa Clara, CA: McAfee, 2010); http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf Accessed July 19, 2012; and Col. Stephen W. Korns, USAF, "Cyber Operations: The New Balance," *Joint Force Quarterly*, 54, 3rd Quarter, 2009, pp. 97-102.

sewerage control system to exploit its vulnerabilities and released 800,000 liters of raw sewerage into the local area, causing devastating damage.[21] Insider attacks come in two forms: an actual attack against a system using insider knowledge, or, providing critical information to a third party that enables an attack, or exposes proprietary information. The Maroochy Shire incident is a famous example of the former; and the alleged actions of PFC Bradley Manning of the U.S. Army is perhaps the most famous example of the latter. In the case of PFC Manning, who is still awaiting trial, it is alleged that he downloaded on to CD-Roms gigabytes of classified information from both the Department of Defense and the Department of State, and handed them over to Julian Assange's Wikileaks who subsequently released the classified information to the international media. The potential for damage from insider threats is enormous, though the motivations on the part of the disgruntled insider vary (happy and content employees do not pose a threat, not intentionally at least).[22] Boden, an embittered man, had a long history of disgruntlement with various employers. Manning was known to have had emotional issues, involving a break-up with his girlfriend, had been demoted back to Private – First Class, because of unreliable and erratic behavior, and had voiced critical misgivings about U.S. foreign policy. Yet still Manning was allowed unprecedented access to classified information from two government departments.[23] Other motivations for insiders to turn rogue include blackmail by third parties, greed, moral or ideological discontentment with policies, ethos, and practices of the organization or institution, emotional instability, drug and/or alcohol addiction, or alienation from colleagues and superiors. Means of attack vary, but all insider threats

[21] See Marshall Abrams and Joe Weiss, "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia," 23 July, 2008. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf Accessed 27 April, 2012.

[22] For a U.S. assessment on insider cyber threats, see *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures* (Washington, DC: Department of Homeland Security, April 8, 2008); http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf Accessed July 19, 2012.

[23] On Manning's alleged personal and emotional issues, see Ginger Thompson, "Early Struggles of Soldier Charged in Leak Case," *The New York Times*, August 8, 2010.

exploit vulnerabilities that can only be known to anyone familiar with a system or the inner workings of an organization or institution.

- Hacktivists: Lastly, hacktivists merit a mention in the pantheon of cyber threats, though really their inclusion is done with some reluctance.[24] While some have intimated that the likes of Anonymous and Lulzsec potentially pose a danger to core national security and economic interests,[25] others are less sure.[26] For now groups like Anonymous and Lulzsec engage in nuisance activities such as denial of service attacks or defacement of particular websites, usually in protest of some government or corporate policy. Such groups tend to target 'low-hanging fruit,' which while a nuisance - even at times illegal - is often only done because companies and government institutions are lax in instituting proper cyber security measures. Should such measures be properly in place then in many instances groups like Anonymous would have very little to play with. Politically, when political motivations can be discerned, these groups engage in fringe political protest usually revolving around issues such as transparency or what these groups deem to be hypocritical.[27] What has not happened, however, is an attack by any of these groups against critical systems or infrastructure. Certainly, it might be possible that a hardcore faction of these groups might break away from what is otherwise a series of supercharged cyber pranks to conduct more damaging and serious operations, but it would seem that this has yet to happen. It should also be noted that in many ways the likes of Anonymous and 4Chan are pranking themselves in to irrelevance. The more they expose security flaws in corporate and government cyber presences, the more seriously these entities take their cyber security obligations. Anonymous, Lulzsec, and 4Chan are one-trick

[24] On hacktivism in general, see the landmark work by Tim Jordan and Paul Taylor, *Hacktivism and Cyberwars: Rebels With a Cause?* (Abingdon, Oxon: Routledge, 2004).
[25] See, among others, Siobhan Gorman, "Alert on Hacker Power Play," *The Wall Street Journal*, February 21, 2012.
[26] See, for example, Yochai Benkler, "Hacks of Valor: Why Anonymous is not a Threat to National Security," *ForeignAffairs.com*, April 4, 2012; http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor Accessed July 19, 2012.
[27] On Anonymous, and its genesis and activities, see Parmy Olson, *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency* (New York: Little, Brown, 2012); see also, Cole Stryker, *Epic Win for Anonymous: How 4Chan's Army Conquered the Web* (New York: Overlook Duckworth, 2011).

ponies who move from target to target as victims of their pranks and protests withdraw the low-hanging fruit and institute measures that mitigate and prevent denial of service attacks, and the like.[28]

With the four main threat actors identified and discussed, the article now turns to an overview of the unique characteristics of cyberspace that enable these actors to pose the varying threats they do.

Characteristics of Cyberspace

Nation-states, terrorist groups, criminal organizations, and hacktivists all benefit from the unique characteristics of cyberspace that make the threat they pose real, or in many cases, help inflate the threat they pose in the minds of others. It is worth repeating, at this juncture, the difference between the terms *cyberspace* and *cyberpower*. Cyberspace is the domain in which cyber operations take place; cyberpower is the sum of strategic effects generated by cyber operations in and from cyberspace. These effects can be felt within cyberspace, as well as the other domains of land, sea, air, and space, and can also be cognitively effective with individual human beings. With this in mind, we turn our attention to some of the main characteristics of cyberspace.

- *Cyberspace relies on the electromagnetic spectrum* (EMS). Cyberspace cannot exist without being able to exploit the naturally existing electromagnetic spectrum. Without the EMS, not only would millions of information and communications technologies (ICT) be unable to communicate with each other, but the ICTs themselves would be unable to function. Denying access to the EMS, such as through jamming, can deny threat actors the fruits of cyberspace. Obviously, the reverse is true also.

- *Cyberspace requires man-made objects to exist*. This makes cyberspace unique when compared to the land, sea, air, and space domains. Without integrated circuit

[28] On this issue, see Eric Sterner, "The Paradox of Cyber Protest," *George C. Marshall Institute Policy Outlook* (Arlington, VA: The George C. Marshall Institute, April 2012); http://www.marshall.org/pdf/materials/1087.pdf Accessed July 19, 2012.

boards, semiconductors and microchips, fiber-optics, and other ICTs, there would be no cyberspace capable of hosting the EMS.

- *Cyberspace can be constantly replicated*. As an entity, there is only one air, one sea, one space, and one land. In contrast, there can be as many cyberspaces as one can possibly generate. In the physical realm, there is only one portion of the air, sea, or land that is important: that portion that is being contested. With cyberspace, however, there can be many in existence at any one time—some contested, some not. For the most part, nothing is final in cyberspace.[29] With airpower, enemy aircraft can be destroyed, and there the matter ends. In cyberspace, a jihadist website can be purposefully shut down, only for the same jihadists to start a new website within hours on a different server using a different domain name. Similarly, networks can be quickly repaired and reconstituted, thanks to relatively inexpensive and readily available hardware.[30]

- *The cost of entry into cyberspace is relatively cheap.* The resources and expertise required to enter, exist in, and exploit cyberspace are modest compared to the resources and expertise required for exploiting the land, sea, air, and space. Generating strategic effect in cyberspace does not require a budget of billions, manpower in the thousands, tracts of land, or divisions/fleets/wings/constellations of hardware that cost yet more billions of dollars. Rather, modest financial outlays, a small group of motivated individuals, and access to networked computers that are accessible to a large portion of the world's population can provide entry to the cyber domain.[31] Deep computer expertise is always an advantage but not always necessary. Computer science and programming knowledge need be only modest to generate strategic effect in and from cyberspace. The character of cyberspace is such that the number of actors able to operate in the domain and potentially generate strategic effect is exponential when compared to the land, sea, air, and space domains.

---

[29] See Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), pp. 5-6.
[30] Ibid., pp. 84-85.
[31] See Stephen W. Korns, "Cyber Operations: The New Balance," *Joint Force Quarterly*, No. 54, 3rd Quarter, October 2009, pp. 97-98.

- *For the time being, the offense rather than the defense is dominant in cyberspace*. This is due to a number of reasons. First, network defenses rely on vulnerable protocols and open architectures, and the prevailing network defense philosophy emphasizes threat detection, not fixing vulnerabilities.[32] Second, attacks in cyberspace occur at great speed—for all intents and purposes to a human observer they seem instantaneous—putting defenses under immense pressure, as an attacker has to be successful only once, whereas the defender has to be successful all of the time. Third, and related to the previous reason, range is not an issue in cyberspace as it is in the other domains. Attacks can emerge from literally anywhere in the world.[33] Fourth, attributing attacks is for the most part problematic, thus complicating any possible response.[34] Fifth, and lastly, the overwhelming reliance on cyberspace throughout modern society, not just in the military, presents any attacker with a target-rich environment, again placing great strain on the ability to successfully defend the domain.[35] This all said, it would seem that this dominance of the offense occurs only at the tactical and operational levels. At the strategic level networks demonstrate a remarkable resiliency and are able to recuperate from any damage relatively quickly. Essentially, this means that any victim of a cyber attack is more than likely to live to see another day.

- *Cyberspace consists of four layers, and control of one layer does not mean control of the others*. Cyberspace consists of infrastructure, physical, syntactic, and semantic layers. The infrastructure layer consists of the hardware, cabling, satellites, facilities, and so on. The physical layer consists of the myriad properties of the EMS—electrons, photons, frequencies, and so forth—that animate the infrastructure layer.[36] The syntactic layer consists of the formatting of information and the rules that instruct and control information systems that make up

[32] For a critique of the lack of robust cyber defenses in the United States, see Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Ecco, 2010), pp. 103-149.
[33] See Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, op.cit., pp. 255-256.
[34] See Susan W. Brenner, *Cyberthreats, The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009).
[35] On U.S. dependence upon cyberspace, see Clarke and Knake, op.cit., pp. 170-175.
[36] Martin Libicki refers to the infrastructure layer as the physical layer. I have added the EMS physical layer to Libicki's taxonomy. See Libicki, op.cit., pp. 8-10.

cyberspace. The semantic layer consists of information useful and comprehensible to human users and is essentially the cyber-cognitive nexus. Controlling the infrastructure layer of cyberspace does not necessarily translate into control of the physical, syntactic, and semantic layers. Similarly, semantic control does not require infrastructure control, as evidenced by the prevalence of cyber crime today that effectively exploits the semantic layer. While this proposition is generally true, there are exceptions that depend upon what one is trying to do. If one is trying to destroy and disable a network, then attacking the infrastructure layer alone may well be effective. If, on the other hand, one is trying to spoof an enemy commander into making certain decisions, then control of the infrastructure layer is largely irrelevant, but control of the semantic layer is everything.[37]

- *Cyberpower is ubiquitous*. Land, sea, air, and space power are able to generate strategic effect on each of the other domains, but nothing generates strategic effect in all domains so absolutely and simultaneously as cyberpower. Given the cyber dependencies of the military, economy, and society in a growing number of countries, and given that cyberspace critically enables land, sea, air, and space power—as well as other instruments of power, such as diplomacy, media, and commerce—cyberpower is ubiquitous. Land, sea, air, and space power can return to barracks, ports, airfields, or, in the case of satellites, be tasked on to another target. Cyberpower does not go back to its sender, nor is it expended.

- *Cyberpower is complementary*. Unlike land, sea, and airpower, but in many ways like space power, cyberpower is largely a complementary instrument, especially when used autonomously. It is indirect because the coercive ability of cyberpower is limited and likely to remain so. For example, consider the cyber attack against Estonia in spring 2007. It is often forgotten that the attacks occurred along with violent protests in Estonia and a political warfare campaign allegedly perpetrated by the Russian government against Estonian interests. None of these—the protests, political warfare campaign, Russian threats and diplomatic protests, or the cyber attacks—swayed the Estonian government. This

[37] Ibid.

is even more remarkable given that Estonia is widely regarded as one of the most cyber-dependent countries in the world. It can certainly be argued that the cyber attacks were damaging, disruptive, and a nuisance, but they were not coercive.[38] It is even more evident that the cyber attacks during the short conflict between Russia and Georgia in August 2008 were likewise not coercive. Georgia, especially at the time, was not a particularly cyber-dependent country, and the Russian military campaign was relatively swift and decisive in achieving its objectives against the Georgians. The associated cyber attacks—which have never been publicly attributed to the Russian government but seemed to have been impeccably timed to peak just as Russian forces crossed into South Ossetia and Abkhazia—certainly caused major disruption to Georgian Internet services and several means of communication, but it is implausible to suggest that the Russian military campaign would have been in any way less decisive had the cyber attacks not taken place or had failed.[39] Similarly, for all the press about the damage caused by the Stuxnet worm in recent months,[40] it has plainly not coerced Iranian leaders to abandon their nuclear program.[41] Until such time that cyberpower might prove its coercive ability, it can be said, at best, that it is a complementary instrument.

- *Cyberpower can be stealthy*. One of cyberpower's attractions for many users is the ability to wield it surreptitiously on a global scale without it being attributed to the perpetrator. This ability to stealthily use cyberpower, aided by the inherent difficulties of attributing the identity and motivation of most attackers, makes it a very attractive instrument for governments and other actors.

---

[38] See Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy,* Vol. 27, Issue 3, May 2008, pp. 227-247.

[39] See, for example, Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Vol. 38, no. 4, Winter 2008-09, pp. 60-76.

[40] On Stuxnet, see, among others, Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Washington, DC: Congressional Research Service, 2010); and David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (Washington, DC: Institute for Science and International Security, December 2010); and, more recently, the claims made by David E. Sanger in, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012), pp. 197-203.

[41] See, for example, Daniel Dombey, "US fears faster Iran nuclear arms progress," *Financial Times* (London), 29 December 2010.

Assessing the Cyber Threat

As has been described, cyber threats are comprised of actors, motivation, and capability fuelled by the unique characteristics of cyberspace. To date, however, none of the cyber attacks cited in this paper – Estonia, Georgia, Maroochy Shire, Wikileaks, or Stuxnet – have, by themselves, resulted in permanent damage or coercive effect, despite each attack causing disruption and even physical damage. While the potential damage caused by a possible cyber attack against critical national infrastructure and other core services is rightly of concern, no such attack has occurred resulting in such damage to date. This is not to dismiss the notion that such attacks could not occur in the future, but given the various types, and growing number, of threat actors, the increasingly sophisticated cyber means at their disposal, and the target-rich environment which they might attack, it is noteworthy that such devastating attacks have *not* occurred as yet. This suggests that while there is indeed a theoretical threat, mounting such devastating attacks is extremely difficult and requires onerous resources and assets, such as sustaining a vast intelligence operation to map target sets. Of all the threat actors described above, it is nation-states who are the most likely candidates to mount such attacks due to the vast resources and expertise at their disposal. Yet the absence of a devastating attack to date suggest either restraint on the part of nation-states or a recognition that such attacks are very hard to pull off – or both.

Thomas Rid, in his article "Cyber War Will Not Take Place," is persuasive when he argues that at present cyber threat actors – even nation-states – and their capabilities are only capable of carrying out acts of sabotage, espionage, and subversion.[42] All three are of limited instrumentality and rarely, if ever, produce strategic effects by themselves. Sabotage, such as the Stuxnet attack, is by definition covert and notoriously difficult to attribute, even in the physical realm. Espionage, one of the oldest professions depending upon who one asks, is more often than not an enterprise, much like burglary, that exploits opportunity as much as it is a purposive pursuit of particular information. Finally, subversion is difficult to achieve on a mass scale, even in this information age, and requires other conditions to exist in order to gain traction. This means that cyber threats by themselves are likely to be limited in scope, difficult to

[42] See Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp. 5-32.

achieve, and even if successful, very difficult to sustain over long periods before the victim of an attack is able to mount an effective defense, and even identify those behind the attack and respond.

The real threat lies not in stand-alone cyber attacks, but in cyber attacks accompanied by attacks and other actions in the physical realm. More recently, media attention has focused on cyber attacks made against Iranian oil refineries, causing local authorities to shut the installations down.[43] Such actions are undoubtedly disruptive and vexatious to Iranian authorities and the Iranian economy. However, these attacks pale in comparison to the damage caused by the biting economic sanctions put in place against Iran by the international community.[44] Similarly, a cyber attack coupled with an action in the physical realm is much more likely to have more consequence for its victim than a cyber attack alone. Cyber threats, ultimately, are only meaningful when coupled with other, more traditional, threats.

This does not mean, however, that there is nothing to worry about. The use of cyber capabilities that are deniable by terrorist and/or criminal proxies while their nation-state sponsor conducts a more traditional, even legitimate, action could have devastating consequences. Furthermore, even without the use of proxies, cyber attacks are disruptive and even damaging and can, if unaddressed over time, undermine the legitimacy of lawful authority and government. In order to prevent such a loss of political and economic authority, institutions and other public entities must do better to foster a more holistic culture of cyber security that does not rely solely on technological fixes and specialists, but involves everybody who uses ICTs in their work. Most failures in cyber security are not technical in nature, but human.[45] There is always someone who did not get the memo (or who thought it did not apply to them), is gullible, or under emotional duress, who through negligence, ignorance, or malevolence lets the bad guys in. Only by undertaking a long-term commitment cyber public health through *education*,

---

[43] See Benoit Faucon and Farnaz Fassihi, "Iran Says Virus Has Hit Oil Sector," *The Wall Street Journal*, April 23, 2012.

[44] See Saeed Kamali Dehghan, "Fears that Western sanctions on Iran could cripple local economy," *Guardian.co.uk,* February 1, 2012; http://www.guardian.co.uk/world/2012/feb/02/western-sanctions-iran-economy Accessed June 3, 2012.

[45] See, for example, Johnnie Hernandez, "The human element complicates cybersecurity," *DesfenseSystems.com*, March 2, 2010; http://defensesystems.com/articles/2010/03/11/industry-perspective-1-human-side-of-cybersecurity.aspx Accessed July 19, 2012.

not just rote training, can institutions and other organizations remove low-hanging fruit that can be exploited by malign actors.[46]

Coupled with better cyber public health, greater resiliency and protection of proprietary information is required in order to mitigate the best attempts by cyber threat actors. And lastly, we must stop being afraid of our own shadow and casting cyber threat actors as invincible ten-feet tall giants. Policy makers and legislators must better understand the threat environment and by doing so, better devote appropriate resources to the different levels of threat. This includes the issue of which authority deals with which threat. Anonymous and Lulzsec are not threats to national security, and are most unlikely to be so in the future. The low-level threat posed by them is a matter for law-enforcement, not the military. Greater wariness of unnecessarily militarizing the cyber threat is needed in order to bring much needed perspective and so that scarce resources can be properly allocated to deal with the cyber threats that matter.

[46] This is an emerging concept among cyber security practitioners; for a good overview of the concept and its challenges, see the White Paper issues by the U.S. Department of Homeland Security, *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action* (Washington, DC: Department of Homeland Security, March 23, 2011); http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf Accessed July 19, 2012.