2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures

Jason Rivera
United States Army
Georgetown School of Foreign Service
Washington, D.C., United States
jhr47@georgetown.edu

Forrest Hare
United States Air Force
Johns Hopkins School of
Advanced International Studies (SAIS)
Washington, D.C., United States
fhare@gmu.edu

Abstract: Conducting active cyberdefense requires the acceptance of a proactive framework that acknowledges the lack of predictable symmetries between malicious actors and their capabilities and intent. Unlike physical weapons such as firearms, naval vessels, and piloted aircraft—all of which risk physical exposure when engaged in direct combat—cyberweapons can be deployed (often without their victims' awareness) under the protection of the anonymity inherent in cyberspace. Furthermore, it is difficult in the cyber domain to determine with accuracy what a malicious actor may target and what type of cyberweapon the actor may wield. These aspects imply an advantage for malicious actors in cyberspace that is greater than for those in any other domain, as the malicious cyberactor, under current international constructs and norms, has the ability to choose the time, place, and weapon of engagement. This being said, if defenders are to successfully repel attempted intrusions, then they must conduct an active cyberdefense within a framework that proactively engages threatening actions independent of a requirement to achieve attribution.

This paper proposes that private business, government personnel, and cyberdefenders must develop a threat identification framework that does not depend upon attribution of the malicious actor, i.e., an attribution agnostic cyberdefense construct. Furthermore, upon developing this framework, network defenders must deploy internally based cyberthreat countermeasures that take advantage of defensive network environmental variables and alter the calculus of nefarious individuals in cyberspace. Only by accomplishing these two objectives can the defenders of cyberspace actively combat malicious agents within the virtual realm.

All views and concepts expressed in this paper originate solely with the authors and do not represent the official positions or opinions of the U.S. Army, U.S. Air Force, or U.S. Department of Defense.

Keywords: *active defense, attribution agnostic cyberdefense construct, internally based cyberthreat countermeasures*

1. INTRODUCTION

Thomas Hobbes, in his political text *Leviathan*, postulated that, in the absence of governance, humanity lives within a "state of nature" and that life within this state of nature is nasty, brutish, and short.[1] The text goes on to describe the development of the Social Contract—a societal construct between a ruler and the ruled in which the ruled agree to live under the laws and guidance of the ruler, as long as the ruler provides an environment in which the life, liberty, and property of the ruled are protected.[2] Today, most industrialized nations live under the safety of a social contract and are generally protected, both physically and legally, from those who wish to do harm.

Cyberspace, unlike the physical domain, is arguably still characterized by Hobbes' state of nature. While there are rules and laws that have carried over from the physical domain, they are sparingly enforced within the cyber domain. The porous borders and anonymous nature of cyberspace create an ideal environment for those with criminal intent. Although there have been a variety of collaborative efforts to construct international laws and norms to regulate cyberspace, these efforts amount to little more than an international convention; i.e., no nation or individual is forcefully obligated to abide by the laws and norms of other nations in cyberspace. Furthermore, the prevalence of the attribution problem (the difficultly of positively attributing a nefarious action in cyberspace to a specific actor) is a confounding factor that makes defensive operations increasingly complex within the cyber domain.[3] Cyberspace, therefore, is likely to remain in a state of nature for the near to medium-term future, which implies that cyberdefenders are going to have to develop creative and proactive methods to defend their networks from within.

Given the amorphous nature of cyberspace and this paper's endeavor to develop an attribution agnostic cyberdefense construct, it is imperative to put forth a definition of the nature of cyberspace. Science fiction author William Gibson first defined cyberspace in 1982 as "a consensual hallucination experienced daily by billions of legitimate operators."[4] One could argue that the vast expansion of the domain and rapid advancements in technology have rendered this idea quaint. To confront today's realities more effectively, the White House developed a definition that is used today by the U.S. government:

1 Thomas Hobbes, *Leviathan* (New York: Continuum International Publishing Group, 2005), Vol. XIII, 9.
2 Celeste Friend, "Social Contract Theory," *Internet Encyclopedia of Philosophy*, http://www.iep.utm.edu/soc-cont/ (accessed Oct. 14, 2013).
3 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation), 41.
4 Dani Cavallaro, *Cyberpunk and Cyberculture: Science Fiction and the Work of William Gibson* (London: The Athlone Press, 2000), ix.

> [Cyberspace is] the interdependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries.[5]

The above definitions make an important point very clear: cyberspace is much more than just the Internet; it is, rather, a function of infrastructure and the use of the electromagnetic spectrum, as well as the social interactions that define cyberspace activity.[6]

Based on this characterization of cyberspace, this paper will propose two theoretical shifts in the perception and engagement of cyberthreats. First, it will address the need for cyberdefenders to develop attribution agnostic cyberdefense constructs. By attribution agnostic, this paper specifically refers to the development of security mechanisms that do not rely on attribution to levy deterrent effects, increase threat-actor risk, or deliver punitive measures. It follows that the anonymous nature of the Internet implies that cyberdefenders must stop attempting to achieve attribution and instead focus on gaining a thorough understanding of the organizations they are trying to defend; only then can they engage and counter nefarious tactics that are likely to be used against the defenders. Second, this paper will propose the concept of developing internally based cyberthreat countermeasures; i.e., strategies that are specifically designed and implemented to deter, detect, and defeat network-based threats from within the friendly network's boundaries. These countermeasures must be custom tailored to the specific organization they are designed to defend and designed in such a manner that they cause a quantifiable shift in the malicious actor's calculus, thereby raising the minimum threshold that must be crossed before the actor is willing to engage in malicious online activity. If these countermeasures are successfully implemented, network defenders should be able to deter and defeat cyberthreats without needing to achieve attribution or facing the technical and legal challenges of conducting counteroffensive response measures. This paper will begin by expanding on these two theoretical shifts before it explores some real-world examples of how these theories could be deployed in network environments.

2. CYBER ACTORS, ATTRIBUTION, AND ASSOCIATED CHALLENGES

A. The Attribution-Focused Model

This section begins with the assertion that cybersecurity is inherently different from conventional security. In an effort to deter and defeat adversaries prior to the exposure of critical assets, conventional security in the physical domain is typically attribution focused and outward facing; that is, one must have a target or know what they are going to strike prior to initiating a defensive/offensive response. While there are certain parallels between the two, the cyberspace domain has characteristics that make it difficult to apply an outward-facing security framework. This brings us to the threat spectrum presented in Figure 1 which outlines seven hypothetical actor-centric threats that a commercial or government entity could face against its physical location. The likelihood of a particular actor conducting a threatening action is highest on the right side of the spectrum and lowest on the left. Conversely, the severity of a threatening action

5 The White House, *Comprehensive National Cybersecurity Initiative* (Washington, DC: National Security Presidential Directive, 2008).

6 Forrest Hare, "The Interdependent Nature of National Cyber Security: Motivating Private Action for a Public Good," *George Mason University* (2010), 13.

is highest on the left side of the spectrum and lowest on the right. This model provides a sense of predictability in terms of what threat-actors will and will not do. While it would be possible for a foreign military power to invade and occupy the sovereign territory of another country, this action is least probable. On the other end of the spectrum, delinquents and petty thieves, though a more common threat, are generally limited in terms of the damage they could inflict on a major corporation or government entity and thus can be handled in a predictable manner, given that the proper security mechanisms are in place.

FIGURE 1

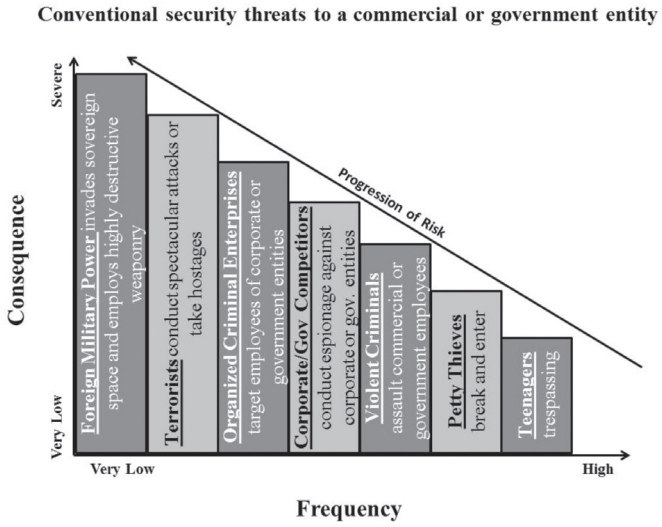
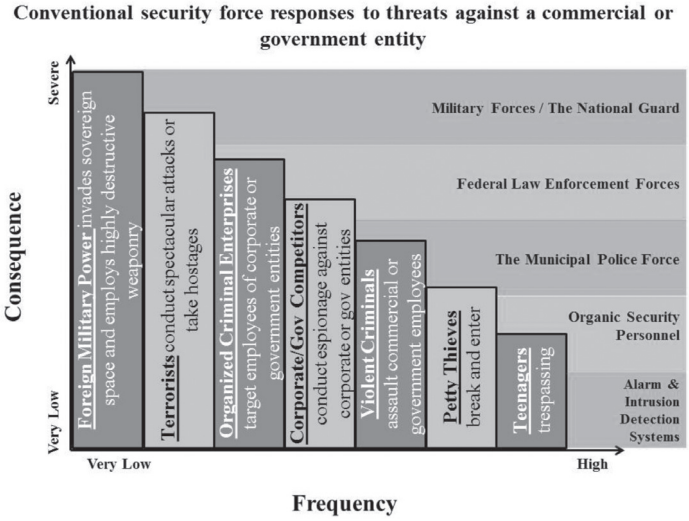


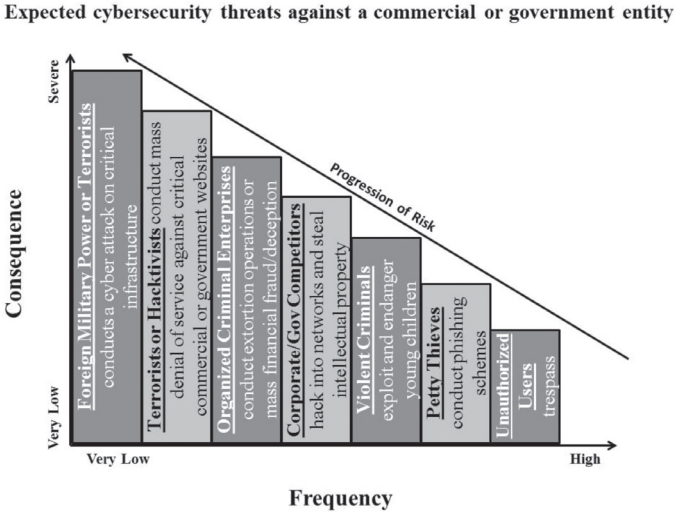
Figure 2 displays conventional responses based off attribution/identification of the nefarious actors. At the highest level of severity, friendly military forces will become involved in order to combat foreign military powers or terrorist threats, whereas low severity threats should be manageable by organic security personnel and/or intrusion-detection systems. Note that there is some level of crossover among the various security response forces, which implies a certain level of necessary cooperation. While there is sometimes friction within this system, this model is regularly adopted and employed by many industrialized nations and private-sector firms worldwide.

FIGURE 2



Naturally, as the Internet has become a more critical component in the day-to-day execution of commercial and government operations, cyberthreats also have become more prolific. In response, cyberdefense professionals have created attribution-specific threat models and defense apparatuses in a manner similar to those of the physical domain, as demonstrated in Figure 3.[7,8] Figure 3 closely resembles Figure 1 in many ways. The actors and their corresponding threats do vary slightly, but the overall threat apparatus remains largely the same.

FIGURE 3

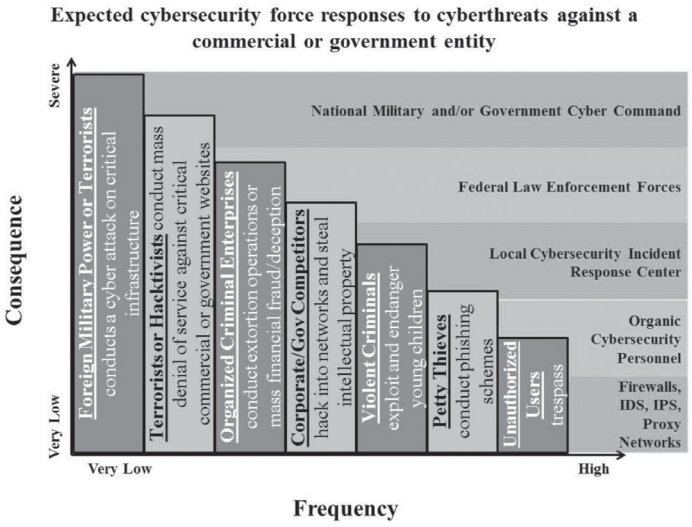


7 The threat-modeling apparatus used in this figure derives its premise from former Director of Cybersecurity Policy at the U.S. Department of Homeland Security, Mr. Andrew W. Cutts.

8 Andrew Cutts, "Warfare and the Continuum of Cyber Risks: A Policy Perspective," *The Department of Homeland Security* (2009), 3, 7.

Figure 4 follows the same security force response logic as Figure 2 and models responses in a similar escalatory manner. In this model, we expect organic cybersecurity personnel, along with various system-hardening measures such as firewalls and intrusion detection/prevention systems, to detect and defeat unauthorized users and/or petty thieves. On the opposite end of the spectrum, host-nation military/government cyber elements are expected to combat a foreign military's cyber capabilities or intrusion by terrorists. Furthermore, as shown in this model, we do not expect the friendly military force to conduct targeted operations against unauthorized users, nor do we expect foreign military powers to conduct phishing schemes or petty trespassing operations. It is at this point that an attribution-focused cybersecurity model becomes flawed, due to the asymmetric capabilities and intent as well as the requirement for attribution of actors operating in cyberspace.

FIGURE 4



B. Defensive Distortions and Critique of the Attribution-Focused Model

Within cyberspace, traditionally less powerful actors, such as unauthorized users in a sensitive network, can sometimes possess highly dangerous capabilities; this is because individual actors in the cyber domain benefit from asymmetric vulnerability relative to larger organizations such as governments or intelligence agencies.[9] Similarly, cyberspace allows foreign military powers, who are traditionally known for targeting adversarial military targets, to bypass national-level defense mechanisms and directly engage lower tier targets. This prevents cyberdefenders from accurately gauging the level of cyberthreat based on the type of aggressing actor, due to asymmetries between threat-actors and their capabilities and intent. Whereas defenders in the physical domain can reasonably assume that petty criminals do not have nuclear weapons and that foreign military powers will not rob the local McDonald's, this same categorical logic does not hold true in cyberspace. Low investment costs and low barriers to entry and exit further amplify asymmetric vulnerabilities, thereby creating defensive distortions.[10] Thus we are presented with two types of defensive distortions in cyberspace:

9 Joseph S. Nye, Jr., "Cyber Power," *Harvard Kennedy School: Belfer Center for Science and International Affairs* (2010), 10.

10 Ibid., p. 13.

1. Military-grade defensive distortion: The ability of government, military, and other powerful entities to wield military-grade cyberweapons and capabilities in order to bypass a nation's national defense apparatus and interface directly with and conduct exploits against private citizens, companies, and other traditionally less defended targets.

2. Unauthorized user-access defensive distortion: The ability for an individual or small group of people to exploit the attribution problem in cyberspace and navigate through the porous portions of the cyber domain in order to conduct attacks, steal information, and/or otherwise levy threats that are typically beyond the capabilities of any one individual or small group of people within the physical domain.

The following are some historical examples of these two defensive distortions:

Unauthorized user access defensive distortions

- In 2012, Anonymous, a non-state-sponsored, loosely connected group comprised of individual hackers, managed to disrupt and degrade the websites of the U.S. Federal Bureau of Investigation, Department of Justice.[11]
- According to a Pentagon report leaked in early 2014, Edward Snowden, a lone actor and former National Security Agency contractor, downloaded 1.7 million classified intelligence files via his access to classified cyberspace networks;[12] this incident is widely considered to be the single largest breach of national security information in U.S. history.
- In 2009, a federal grand jury indicted Albert Gonzalez and two accomplices for conducting a SQL injection attack used in an international operation that compromised 134 million credit cards;[13] in late 2013, experts speculated that a network breach had occurred at Target Corp.'s point-of-sale (POS) terminals, resulting in the exposure and possible compromise of the credit and debit card information of up to 110 million customers.[14]

Military-grade defensive distortions

- Since 2006, a conventional Chinese military force known as the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's 3rd Department is reported to have targeted and compromised private-sector companies throughout the world, including at least 141 companies spanning 20 major industries.[15]

11 MSNBC.com staff and news services, "Anonymous says it takes down FBI, DOJ, entertainment sites," *NBC News Technology*, Jan. 19, 2012, http://www.nbcnews.com/technology/anonymous-says-it-takes-down-fbi-doj-entertainment-sites-117735 (accessed Oct. 15, 2013).

12 Associated Press, "Snowden obtained nearly 2 million classified files in NSA leak—Pentagon report," www.*RT.com*, Jan. 9, 2014, http://rt.com/usa/snowden-downloaded-millions-documents-389/ (accessed Feb. 1, 2014).

13 Taylor Armerding, "The 15 worst data security breaches of the 21st Century," *COS Security and Risk*, Feb. 15, 2012, http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century (accessed Feb. 1, 2014).

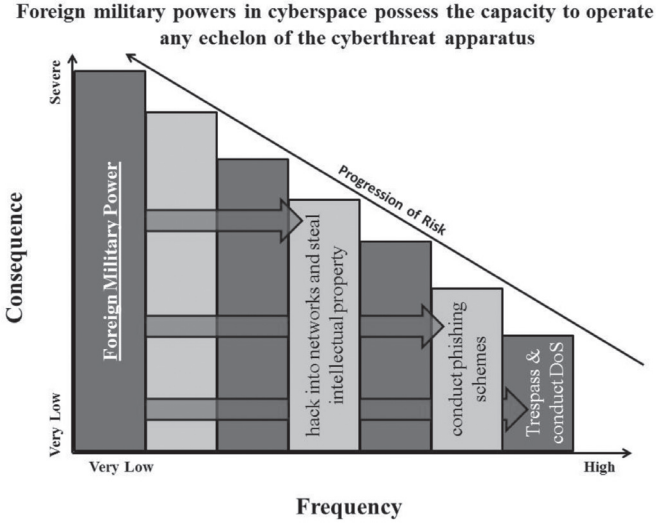
14 Tracy Kitten, "Target Breach: What Happened? Expert Insight on Breach Scenarios, How Banks Must Respond," *Bank Info Security*, Dec. 20, 2013, http://www.bankinfosecurity.com/target-breach-what-happened-a-6312/op-1 (accessed Feb. 1, 2014).

15 Why We Are Exposing APT1, "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant* (2013), 6.

- From 2008 through late 2013, several media sources reported that Israel had gained access to Palestinian phone networks and demonstrated a capacity to send mass text messages to Palestinian citizens. In most cases, these text messages were used to conduct psychological operations against the Palestinian population, including one sent in 2012 that stated, "The next phase is on the way. Stay away from Hamas elements."[16] Another mass message, sent in October 2013, stated that "tunnels that were built by Hamas underground between Gaza and the Israeli-occupied territories cost millions of dollars that were supposed to be spent on the Gaza people."[17]

The above examples demonstrate the difficulties in defending cyberspace, as many malicious cyber actors successfully avoid attribution and often have the ability to circumvent traditional defensive constructs. Note in Figure 5 how a foreign military power is able to conduct cyber operations at the high-frequency end of the threat spectrum. This not only implies that powerful threats have the capacity to threaten entities that are less able to defend themselves, but also that there is a defensive distortion within the traditional national cybersecurity framework. By directly circumventing and therefore not inciting a defensive response from the friendly national military and/or government cyber force, an adversary wielding military-grade cyber capabilities is able to bring an overwhelming capacity to bear against systems that are not adequately hardened, while simultaneously operating safely below the attribution threshold necessary for a national-level response.

FIGURE 5

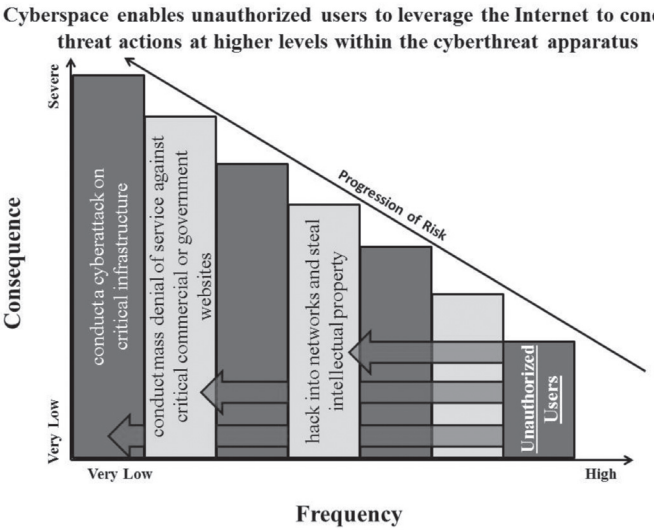


16 Lisa Goldman, "IDF sends text message to Gaza mobile phones: The next phase is on the way," *972 Mag*, Nov. 16, 2012, http://972mag.com/idf-sends-text-message-to-gaza-mobile-phones-the-next-phase-is-on-the-way/60046/ (accessed Feb. 1, 2014).

17 Associated Press, "Israeli text messages warn Gazans not to help Hamas build tunnels," *World Tribute*, Oct. 21, 2013, http://www.worldtribune.com/2013/10/21/israeli-text-messages-warn-gazans-not-to-help-hamas-build-tunnels/ (accessed Feb. 1, 2014).

On the other end of the spectrum, unauthorized users are able to wield capabilities that exceed the expectations of what traditional defensive frameworks ascribe to the individual. Figure 6 demonstrates the unauthorized user's capacity to inflict harm beyond the scope of what was possible prior to the prevalence of the Internet.

FIGURE 6



Consider a worst-case scenario, where the next insider threat is not a disenfranchised intelligence officer like Edward Snowden or Bradley Manning but a disgruntled nuclear engineer with enough computer savvy to cause a regional power crisis—or worse, a nuclear meltdown. In the cyberspace environment, unauthorized users have the ability to apply asymmetric vulnerabilities against traditionally hardened targets. Again, this implies another distortion within the traditional national cybersecurity framework, as the insider threat operates both beyond the locally emplaced defensive measures, often avoids attribution, and interfaces below the enforcement threshold of higher level cybersecurity force response entities.

The asymmetries inherent among threat-actors in cyberspace suggest the need for an attribution agnostic cyberdefense construct that focuses on the individual nature of the organization, its valuable cyberspace equities that are exposed to risk, and the organization's physical and network environment. Let us explore the development of such a construct in pursuit of the objective to implement an active, internally based defense.

3. THE ATTRIBUTION AGNOSTIC CYBERDEFENSE CONSTRUCT

An attribution agnostic cyberdefense construct (AACC) will analyze and depict the unique characteristics of an organization in a manner that enables defenders to deploy catered active defense solutions in the form of internally based cyberthreat countermeasures. Given this objective, defenders must learn to conceptualize their respective organizations and how they relate to cyberspace as a series of analytic components. The United States military community has developed a model that frames cyberspace within the context of three layers, which include the physical layer (both geographic and physical network components), logical network layer, and social layer (both persona and virtual persona components).[18] The AACC proposed in this paper derives its premise from this model and characterizes organizations as they relate to cyberspace via the following five distinct, yet related, components:

1. The Geopolitical Component: All organizations are subject to the constraints associated with their geographic locations, as well as the governing nation-state's laws and policies. This is an important factor in terms of analyzing an organization's capacity to conduct response actions in cyberspace. For example, U.S. law, per the Computer Fraud and Abuse Act, defines accessing a computer without authorization or exceeding authorized access as a criminal offense; therefore outlawing cyberspace response actions by private sector entities.[19] A commercial company in Indonesia, on the other hand, would likely face few to no repercussions for conducting aggressive response actions in cyberspace, as online law enforcement legislation in that country is virtually non-existent.[20]

2. The Physical Infrastructure Component: This component includes the physical aspects of an organization's computer infrastructure, electrical power resources, physical security layout, and public interface functionality. Physical infrastructure may include but is not limited to buildings and office space, physical domain security measures, electrical power connectivity, systems cooling, physical computing technology (hardware, servers, etc.), and communications equipment (satellite communications, VSAT dishes, telephone lines, etc.).

3. The Interface Component: This component encompasses the way an organization employs interface mechanisms to interact with cyberspace. The interface component includes the network gateway and networking identities used by organizational members. Passing through the Internet gateway can be achieved with a laptop, virtual machine thin client, smartphone, fax machine, etc. Once through the gateway, an individual assumes a virtual identity (username, email address, phone number, social media profile, etc.) to exchange information in cyberspace.

4. The Logical Network Component: This component comprises the electrons, bits and bytes, or 1s and 0s flowing to and from computer networked services using the

18 Training and Doctrine Command, "TRADOC Pamphlet 525-7-8: Cyberspace Operations Concept Capability Plan 2016-2028," *Department of the Army* (Fort Eusis, VA: GPO, 2011), 8.

19 18 U.S.C. § 1030: U.S. Code–Section 1030: Fraud and related activity in connection with computers.

20 Farisya Setiadi et al., "An Overview of the Development Indonesia National Cyber Security," *International Journal of Information & Computer Science* (2012),Vol. VI, 108.

Open Systems Interconnection (OSI) or TCP/IP layer models in terms of accurately addressing and directing the flow of information. This component is characterized by the logical connections an organization leverages to interact with cyberspace. An organization's logical network is comprised of switches, routers, various servers, firewall functions, and broadcast domains and is logically mapped via IP addressing and network routing protocol.

5. The Critical Information Component: This component comprises the societal purpose of an organization and is the most critical consideration for developing an effective cyberdefense construct. All computer networks are designed to process information, and information is, in general, processed in one of two ways.
    a. Information exchanged and processed by humans exists in the form of ideas; the most valuable ideas within an organization comprise that organization's intellectual property. Schematics, tradecraft, business strategies, formulas, and plans are some examples of intellectual property.
    b. Information exchanged and processed by machines exists in the form of protocol; the most important protocol within an organization comprises that organization's critical control systems. Electrical power switching, manufacturing processes, financial transaction systems, transportation systems, water/wastewater control systems, and temperature regulation systems are some examples of these critical control systems.

Once an organization is accurately characterized via the AACC, an appropriate internally based cyberthreat countermeasure must be developed in order to actively combat potential cyberthreats. If one thinks of the cyber domain as a fifth domain of human interactivity (the others being land, sea, air, and space), then the development of internally based cyberthreat countermeasures designed to defeat cyberthreats is a logical solution. Consider Germany's first anti-material rifle, known as the "T" Gewehr 13mm anti-tank rifle, which was developed in response to the Allies' introduction of tanks during World War I,[21] or the U.S. military's development of anti-ballistic missile technology in response to the Soviets' Intercontinental Ballistic Missiles.[22] Given historical precedence, it stands to reason that cyberdefenders should facilitate the development of internally based cyberthreat countermeasures designed to defend organizational assets from within friendly networks.

4. INTERNALLY BASED CYBERTHREAT COUNTERMEASURES

The creation of internally based cyberthreat countermeasures (IBCCs) shall be premised upon a key assumption: an adversary with malicious intent sufficiently resourced with time, capabilities, and personnel will inevitably compromise a friendly network. This assertion is reflected in the statements of leading cybersecurity experts and firms. Mandiant, a well-known cybersecurity firm credited with conducting large-scale attribution and exposure of the Chinese

21 Eric G. Berman and Jonah Leff, "Anti-Materiel Rifles," *Small Arms Survey* (2011), No. 7, 1.
22 Mark Hubbs, "Where we began—the NIKE-ZEUS Program," *Space and Missile Defense Command /Army Strategic Command* (2007), 14.

PLA Unit 61398,[23] is one of these cybersecurity firms. According to Mandiant vice president Grady Summers, "We've seen first-hand that a sophisticated attacker can breach any network given enough time and determination."[24]

Of further note, the development of IBCCs views cyberdefense as a function of environmental variables, rather than focusing solely on outward-facing measures. Consider the role environmental factors have played in history's most significant conflicts. What if, during the Battle of Agincourt in the Hundred Years' War, the French had not been canalized by dense woodlands and slowed by thick mud?[25] It is possible that the numerically superior French Army would have won the battle and perhaps even have changed the entire course of the Hundred Years' War. What would have happened during World War II if the English Channel had not separated Nazi Germany from Great Britain? It is probable that the Nazis would have used Blitzkrieg tactics to overrun British defenses, thereby negating Britain's strategic bombing campaign and preventing execution of the Allied Forces' deception plan known as Operation Fortitude,[26] which led to Allies' successful invasion of Normandy in 1944.

Cyberspace, on the other hand, is not constrained by strictly defined environmental variables and is, rather, a function of human creation and ingenuity. In the cyber domain, one can fill the English Channel with elements of danger. In cyberspace, the trees can be made denser and the mud thicker. Cyberdefense professionals are limited only by their own creativity and level of ingenuity, implying that additional attention should be focused on cyberdefense as a function of the virtual environment.

Given this supposition, this paper contends that a successful active defense will be premised on the alteration of defensive environmental variables and must be designed to deter or defeat an adversary from within; that is, such a measure must retain deterrent/defensive capacity even after the network has been compromised. An effective IBCC will have specific qualities that achieve two key functions. First, it will not be reliant upon attribution yet it will deter malicious cyber actors by affecting their cost/benefit calculus in such a manner as to raise the minimum threshold for engagement in nefarious activities. Second, it will be designed to have a negative impact on those who levy cyberthreats, even after the network has been compromised. Let us now explore two hypothetical examples of the development of IBCCs and then discuss the cost/benefit structure, including who will bear the burden of implementing such a system.

A. Example 1: The use of a counter-data strategy by a government-affiliated, private-sector organization operating in a semi-permissive environment

For this scenario, let us consider an IBCC for a corporation within the defense industrial base whose primary business function is the development, design, production, delivery, and maintenance of military weapons systems. Real-world examples of such companies include

23 Why We Are Exposing APT1, "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant* (2013), 2.

24 Mandiant Press Release, "Mandiant® Releases Annual Threat Report on Advanced Targeted Attacks," *Mandiant: A FireEye Company*, 2013 https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks1/ (accessed Feb. 1, 2014).

25 Juliet Barker, *Henry V and the Battle that made England: Agincourt* (New York: Little, Brown and Company, 2005), Ch. 14.

26 Ernest S. Tavares, Jr., "Operation Fortitude: The Closed Loop D-Day Deception Plan," *Air Command and Staff College* (Maxwell Air Force Base, Alabama: GPO, 2001), 1.

Lockheed Martin, Boeing, and Raytheon. In this scenario, the corporation operates within the geopolitical context of a semi-permissive cyberspace environment; that is, private organizations are authorized to conduct reasonable active defense and response actions, but not to the extent that they are violating the U.S. equivalent of the Computer Fraud and Abuse Act.

First, we must depict this organization's AACC:

1. The Geopolitical Component: A semi-permissive environment where the conduct of active defense and limited response actions are within the boundaries of the law.

2. The Physical Infrastructure Component: A highly secure office environment that is unlikely to be physically penetrated by a malicious threat; both onsite physical infrastructure and communications equipment are highly fortified to include redundancy measures and well-protected hardware/server environments.

3. The Interface Component: Most/all members of this organization will likely possess uniquely identifiable network interface personas that differentiate members from others throughout the common population. For example, company president John Doe's email address may be john.doe@CompanyName.com, thereby differentiating him from a less attributable email address such as john.doe@gmail.com.

4. The Logical Network Component: Company network and routing protocol will be restricted from the public, and secure network routing protocol will be implemented. Organization members may have tokens that allow them to tunnel into the corporate network from home, which potentially makes the system vulnerable.

5. The Critical Information Component: This organization's lifeblood is the ability to design, produce, and distribute defense systems for sale to government militaries and private security companies. Therefore, this organization's most critical information component is the intellectual property pertaining to its design and production plans for defense systems.

According to the report, "Commission on the Theft of American Intellectual Property," annual losses due to theft of intellectual property are estimated to be over $300 billion.[27] This report states further that the sectors of the economy affected most prolifically tend to be those that support U.S. national defense programs.[28] Thus, for this situation, an appropriate IBCC is one that deters the theft of intellectual property and causes harm to adversaries who successfully infiltrate friendly networks and steal intellectual property. This of course begs the question, "How does one deter or cause harm against an adversary that they cannot conduct attribution against?" This is why cyberdefense professionals should develop IBCCs based on the premises of the AACC.

An appropriate IBCC for this scenario designed to defend intellectual property is the effective use of counter-data that is carefully seeded within a friendly network via a honeynet, a network

27 The National Bureau of Asian Research, "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research* (Washington, DC: GPO, 2013), 2.

28 Ibid., p. 19.

of resources designed to be compromised.[29] "Counter-data" in this paper refers specifically to one of the following:

1. Custom-designed malware/spyware seeded within a honeynet that, if exfiltrated in an unauthorized manner (i.e., network intrusion), causes direct harm against an adversary by activating a call-back module to inform law enforcement of the adversary's location, wiping the adversary's system, or opening a backdoor into the adversary's system for response actions.

2. Intentionally flawed information seeded within a honeynet that causes indirect harm against an adversary by sowing confusion, misdirection, false intent, and deception.

While a counter-data strategy comprised of custom-designed malware/spyware would have universal application, a counter-data strategy with intentionally flawed information would vary according to the particular specialty of the corporation. A defense industrial base organization working with an intelligence agency, for example, should be defended by a counter-data IBCC containing false and misleading intelligence. Organizations involved with financial institutions should use honeynets that contain counter-data that is relevant yet disadvantageous to a competing financial institution. A weapon developer's counter-data IBCC should contain erroneous blueprints, unrealistic plans, or plans that suggest the pursuit of false strategic military objectives. By using this IBCC, the cyberdefender increases the competing organization's probability of taking a strategic misstep. Facilitating such a method allows the cyberdefender to seize the initiative from those who commit intellectual property infringement by fooling them into believing they have stolen something valuable.

The IBCC described above complements the AACC, as it does not require attribution in order to induce damage against adversaries. By accurately characterizing the five components of the AACC, this countermeasure essentially defends an intellectual property oriented organization in an automated manner. It operates within the geopolitical constraints by conducting automated response actions against adversaries without going as far as to take offensive and autonomous action against intruding networks. It will possess the necessary physical infrastructure and interface components designed to make the honeynet appear as realistic as possible to the potential adversary. Similarly to government intelligence agencies' use of counterintelligence agents, intellectual property oriented organizations should employ counter-data agents in order to deploy and maintain this program. Lastly, the solution will have a logical design (believable IP addresses, appropriately routed networks, etc.) used in such a manner as to fool or at least sufficiently confuse an intruder to the point to where they are either unaware or unsure if they are obtaining intellectual property of value.

B. Example 2: The use of a "white noise" strategy by a private-sector retailer operating in a restrictive environment

For this scenario, let us consider an IBCC for a department store within the commercial retail sector, whose primary business function is the sale of tangible goods such as clothing, food, appliances, electronics, furniture, etc. Well-known real-world examples of such companies include Wal-Mart, Target, McDonald's, and Best Buy; however, we should also consider

29 Matt Walker, *All-In-One Certified Ethical Hacker* (New York: McGraw Hill, 2012), 352.

small "mom-and-pop" type stores. In this scenario, the retailer operates within the geopolitical context of a restrictive cyberspace environment; that is, private organizations are authorized to conduct active defense but not active response actions, nor any activity that would intrude on another network.

The following is this retailer's AACC:

1. The Geopolitical Component: A restrictive environment where active defense is authorized; however, direct response actions are outside the boundaries of law.

2. The Physical Infrastructure Component: An open retail environment designed to facilitate customer service; because priority is given to the sale of retail goods, infrastructure security is not highly prioritized; communications infrastructure is primarily designed to conduct POS transactions.

3. The Interface Component: Likely only upper management will have uniquely identifiable email addresses; lower level employees (sales clerks, warehouse workers, etc.) will likely interface instead with POS machines or personal computers.

4. The Logical Network Component: In the modern era, POS machines may be connected via Wi-Fi, be cloud-based, or be centrally administered in some way or another. POS machines will likely transfer data to a back-office computer or central data-processing point for the purposes of accounting, inventory control, estimating sales trends, etc. IP address data and Internet connectivity will likely be minimally secured.

5. The Critical Information Component: The financial well-being of retailers is based on their ability to purchase goods at wholesale and sell them at a mark-up value in order to turn a profit. Therefore, a retail organization's most critical information component is the financial transaction system that allows them to sell goods to customers and centrally manage data pertaining to POS transactions.

Recent news headlines demonstrate retail POS systems' increased vulnerability to credit card data breach and fraud. According to LexisNexis Risk Solutions, a research-oriented firm, retail merchants paid on average 2.69 cents per dollar in 2012 and 2.79 cents per dollar in 2013 as a result of increased fraudulent use of credit cards via online transactions.[30] In addition to the rising costs of credit card fraud, research suggests that data breaches that lead to credit card fraud are increasing at an alarming rate. According to a Verizon study, over 2,500 large-scale data breaches have occurred over the nine-year period between 2004 and 2013, with 621 of those breaches occurring between 2012 and 2013, for a total of 1.1 billion compromised records.[31] In 2012, approximately 1 in 4 of these data-breach victims suffered identity theft.[32] Online vendors, who suffer the bulk of fraudulent transactions, have implemented a host of fraud-detection technologies, including IP geolocation, device fingerprinting, verification

30 LexisNexis, "2013 LexisNexis True Cost of Fraud Study," *LexisNexis Risk Solutions* (Dayton, OH: LexisNexis, 2013), 6.
31 Verizon Risk Team, "2013 Data Breach Investigations Report," *Verizon* (New York: Verizon, 2013), 4.
32 Ibid. 28, p. 6.

services, browser/malware tracking, rule-based filters, etc.,[33] yet these measures do not address the core problem: how do we effectively limit the breach of data in the first place?

While the online retail industry has managed to implement security measures with varied degrees of success, this does not solve the problem of data breaches; rather, it merely counters a malicious person's capacity to use fraudulent personal data to conduct online transactions. Department stores, restaurants, mom-and-pop shops, and retail stores throughout the world remain vulnerable to data breaches, due to their technical inability or lack of sufficient funds to apply high-level cybersecurity measures. Even if retail stores managed to encrypt data at POS locations, this does not change the fact that a persistent actor who is sufficiently determined can and will intercept personally identifiable information and find ways to crack the encryption. It stands to reason, then, that cyberdefense professionals must seek to drastically alter the threat environment.

Many cybertheorists have conceptualized cyberspace as a sort of environment or terrain that is governed by the laws of physics, including both its logical and physical aspects.[34] Unlike other environments, such as the land, sea, air, and space, the cyberspace environment can easily and quickly be altered by human will. Whereas a ship traveling through a narrow passage or canal is restricted to that particular body of water, human interface via the cyber domain is capable of creating new passages (links and nodes) and new ships (packets of data) at an extremely rapid rate. Given this concept, an appropriate IBCC for the defense of retail POS systems may be the introduction of "white noise" into friendly cyberspace environments.

Consider the breach that took place at Target stores in November-December 2013. Essentially, a group of individuals managed to breach Target's primary information hub, and then distributed code to POS systems and cash registers that allowed them to capture credit card data from customers.[35] Now consider the development of IBCC software that would make it so that, for every legitimate transaction that took place, the software would simultaneously fabricate 1,000 additional transactions. The aim would be that the POS system itself would be unable to differentiate between the legitimate transaction and the fabricated transactions. Each fabricated transaction would be controlled via a random data generator that combined varying sequences of the following:

1. A 16-digit credit card number
   - 9,999,999,999,999,999 possible outcomes
2. A randomly assembled combination of first name, last name, and middle initial
   - Approximately 20,360,011,698 possible outcomes[36,37]
3. An expiration date within the next four years
   - 48 possible outcomes

33 LexisNexis, "2013 LexisNexis True Cost of Fraud Study," *LexisNexis Risk Solutions* (Dayton, OH: LexisNexis, 2013), 30.

34 Gregory Rattray, *Cyberpower and National Security* (Washington, DC: Potomac Books, 2009), 255.

35 Bree Fowler, "Answers to questions about Target data breach," *The Boston Globe*, 2013 http://www.bostonglobe.com/business/2013/12/19/answers-questions-about-target-data-breach/pN7ikzJzFWYhHtsFXHISeL/story.html (accessed Feb. 7, 2014).

36 According to the U.S. Census Bureau, in the year 2000 there were 151,671 unique last names and 5,163 unique first names.

37 U.S. Census Bureau, "Genealogy Data: Frequently Occurring Surnames from Census 2000," *U.S. Census Bureau*, 2014 http://www.census.gov/genealogy/www/data/2000surnames/ (accessed Feb. 7, 2014).

4. A credit card company randomly selected from American Express, Visa, MasterCard, and Discover
    - four possible outcomes
5. A three-digit security code
    - 999 possible outcomes

When all the above factors are considered, there are approximately 3.905e+31 different possible outcomes—an astronomical figure, which implies that the probability of accidentally duplicating a real credit card is virtually zero. All transactions (both real and fabricated) would be transmitted via encrypted channels to a highly secure central processing location. The central processing entity would then cross-reference all transactions with MasterCard, American Express, Visa, and Discover databases in order to process the transactions appropriately. Real transactions would be processed as normal, and fabricated transactions would be sent to and stored in a centralized cybersecurity company database. This storage database would hold on to these fabricated transactions for a predetermined period of time. If, at some point or another, an identity thief attempted to use one of these fabricated credit cards to conduct illegitimate transactions, it would automatically be flagged in the storage database and would cue law enforcement authorities to the location of the transaction or, ideally, the location of the criminals themselves.

C. Costs, Benefits, and Bearing the Burden

The implementation of IBCCs requires expending resources on secondary defense efforts. In addition to maintaining current outward-facing cybersecurity efforts, IBCCs require the allocation of potentially substantial resources to conduct defense and deterrence from within the network. The amount of resources allocated for this effort will be situationally dependent. For example, it would behoove a major firm whose main asset is intellectual property to bear the burden of implementing an IBCC by hiring one or more full-time counter-data strategists to manage their deception program. This individual would be required to have both cybersecurity and traditional counterintelligence-like traits, which suggests that firms will be required to pay a premium for both skillsets. Firms employing the white-noise IBCC, on the other hand, would likely bear the burden of implementing an IBCC by paying a premium on installing and maintaining the defense mechanism, as opposed to paying the salary of a full-time individual. Large computer security firms such as McAfee, Kaspersky, Symantec, and others are capable of implementing such an IBCC today, given currently available technology. Major firms, like Target, would likely be more than willing to bear such costs, whereas small companies would be able to band together to share the maintaining an IBCC. Additional cost-sharing structures could include customers, business partners (such as credit companies), and, potentially, national governments who are responsible for shouldering the costs of national security.

Because the benefits to be gained from implementing IBCCs are not always realized by a private firm directly, there would be a role for national governments to adjust the load-sharing appropriately. However, considering the magnitude of loss that companies regularly face due to data breaches and intellectual property theft, firms that successfully implement IBCCs may be able to limit their losses due to fraudulent activity and enjoy the benefits of long-term loss reduction, in terms of their liability due to identify theft, their reduced losses from intellectual property theft, and lower cost of customer/product remediation measures.

5. CONCLUSION

This paper outlines the need for cyberdefenders to construct frameworks that proactively define an organization's characteristics and conduct environmentally oriented cyberdefense measures. By acknowledging the asymmetries between actors and their capabilities and intent within the cyber domain, cyberdefenders can free themselves from the biases that security professionals have developed as a result of operating within a conventional threat environment. The Internet's history and current events demonstrate that cyberspace yields asymmetric advantages to those who leverage intrusive capabilities. This paper therefore surmises that network defenders must secure friendly networks by using attribution agnostic cyberdefense constructs and designing internally based cyberthreat countermeasures that take advantage of network environmental variables in order to deter and defeat nefarious cyber actors.

The Internet was initially designed to be a collaborative domain characterized by the free sharing of ideas. Unfortunately, the lack of security mechanisms implemented within the initial design has created opportunities for malicious individuals to exploit other people. The framework proposed in this paper, while by no means a comprehensive solution, represents the aggressive mindset that cyberdefenders must develop if they want to combat threats in cyberspace. Like the creation of countermeasures in the physical domain, it is not merely suggested but imperative that network defenders shift to an aggressive mindset and apply energy and resources to create IBCCs within friendly network domains.