Who Shall Defend Us?

Determining National Defense Roles in the Internet Age

By Daniel Ward and Michael R. Grimaila – ISSA member

The modern taxonomy for assigning defensive responsibilities is largely based on geography, scope, and the nature of the threat. When the threat is cyber-based, this taxonomy breaks down.

99 knights of the air // Ride super-high-tech jet fighters
Everyone's a Superhero // Everyone's a Captain Kirk
With orders to identify // To clarify and classify
Scramble in the summer sky // As 99 red balloons go by.

– Nena, 99 Red Balloons

In Nena's 1984 protest song, *99 Red Balloons*, the singer describes a group of fighter pilots sent on a mission "to identify, to clarify and classify" a potential threat. Sadly, they misidentify a bunch of toy balloons as an incursion of enemy forces and end up destroying the world. This song illustrates the importance of accurately understanding the threat environment and using that assessment to determine an appropriate defensive course of action.

As it was in 1984 (and has been for centuries), the modern taxonomy for assigning defensive responsibilities is largely based on geography, scope, and the nature of the threat. Under this model, the U.S. Department of Defense (DOD) protects citizens and allies against *hostile* foreign powers, with the Air Force given responsibility for threats in the air, the Navy responsibility for the sea, and the Army responsibility for the land.

Other types of situations are handled by the Department of Justice (DOJ). Specifically, the Federal Bureau of Investigation handles *domestic* situations (e.g., law enforcement issues) which cross state lines or are deemed sufficiently significant in scope to warrant the FBI's involvement. Smaller-scale crimes and individual criminals are handled by state and local police forces and judicial systems, and of course citizens and businesses are responsible to lock their own doors and secure their own valuables.

A variety of intelligence agencies such as the Central Intelligence Agency (CIA) also have a role in identifying, preventing, and prosecuting certain crimes and conflicts, while the National Guard is uniquely dual-hatted to support both Federal and State objectives, on both sides of our national borders.

The Department of Homeland Security (DHS) has a broad ranging mission, which includes securing "our country against those who seek to disrupt the American way of life… [and] preparation for and response to all hazards and disasters."[1] One common thread for all these agencies and organizations is the need to "iden-

1 Department of Homeland Security Strategic Plan. Retrieved from http://www.dhs.gov/xabout/strategicplan.

tify, clarify and classify" a threat as a first step towards providing security.

This time-honored division of responsibilities relies on observable distinctions between types of threats and hostile entities, between acts of war and merely criminal acts, between espionage and terrorism, between juvenile delinquency and more serious offenses, and between various physical/geographical realms. However, these distinctions are largely meaningless or not observable (or both) in cyberspace. Previously well-established concepts such as "borders" are difficult, perhaps impossible, to define in cyberspace. Thus, the taxonomy of defense and security which previously allowed us to clearly determine roles and responsibilities breaks down rapidly when applied to online information systems. This leaves several vital, practical questions about national security unanswered, the most significant of which is simply "Who shall defend us?"

Accompanying this breakdown in taxonomic clarity is an increase in our national vulnerability. Our critical national infrastructure largely relies on electronic *1s* and *0s* rather than physical resources, and on interconnected systems rather than isolated data stores. The risk, scope, and potential impact of cyber attacks against our infrastructure seems to be growing daily, while our ability to answer basic questions about who owns various defensive missions diminishes, mired in outdated taxonomies and overly complex, ill-understood, unsuitable requirements and regulations.

Estonia 2007 – Neither terror nor destruction

The recent situation in Estonia highlights the confusion between crime and conflict in cyberspace. In a much-discussed incident in 2007, the country of Estonia faced a botnet attack which temporarily crippled its government and communication infrastructure. This situation has often been described as Web War One, but that assessment is not universally accepted. As Hollis points out, some "observers… denied that Estonia's experience qualified as warfare… Although disruptive, the attacks on Estonia had caused neither terror nor destruction."[2] Thus, even the definition of "act of war" is unclear when cyber activity is concerned.

Estonia suspected, but could not prove, that the attacks were sponsored by the Russian government. The Russian government's protestations of innocence were not convincing in many circles, but they could not be disproven. Confusion reigned and was amplified by the difficulties Estonian government leaders faced in trying to communicate with the outside world – difficulties caused and amplified by the attack.

Some observers suggested the Estonian government had the right to invoke *Article 5* from the NATO treaty,[3] asking for defensive military support from the other NATO allies. However, without clear evidence that Estonia was actually experiencing a military attack, much less a definitive identification of the attacker, such a proposal was deemed untenable and unnecessary.

As Estonian defense ministry spokesman Madis Mikko asked, "If a bank or an airport is hit by a missile, it is easy to say that is an act of war. But if the same result is caused by a cyber attack, what do you call that?"[4] Was the botnet attack an act of war or merely a violation of law? Perhaps it was neither. More likely, it was both – indeed, despite refraining from invoking *Article 5*, Estonia seemed to view it as a combination of conflict and crime, "treating the acts as not only war-like, but also launching a criminal investigation."[5] This is further evidence that the traditional taxonomic boundaries are blurred considerably in cyberspace.

But even if the Estonia situation was deemed an act of war and *Article 5* was invoked, it was not clear what kind of military assistance NATO could or should provide. Does a cyber attack merit a kinetic response from a military organization? If so, who should be targeted, and with what weapons? While various opinions have been expressed on this topic, the international community has yet to firmly establish an agreed-upon proportional scale between cyber and kinetic effects. In Estonia in 2007, questions of attribution, jurisdiction, and response had no clear answers. They still do not.

The problem of attribution

This leads to one of the most difficult sticking points in the realm of cyber security: Attribution. Cyber attacks are generally anonymous by their nature, and anyone "can launch attacks from across the globe almost with impunity because of the difficulty of determining the exact origin of the attack or the identity of the attacker."[6]

While an aggressor may chose to claim credit for an attack, it is relatively simple to mask one's identity or appear to be someone else, and as Berkowitz points out, "The greater danger is from hackers who don't want attention."[7] Attacks can appear to come from virtually any computer in any country, regardless of their true origin. This makes it fairly simple for an aggressor to falsely implicate an innocent government, organization, or individual. It also makes it easy for a guilty party to pose as someone or something else.

The problem of attribution is particularly painful because, as discussed in the previous section, identifying the threat source is currently the basis for America's defensive decision-making process. If we cannot identify the attacker, we do not know who has responsibility to defend or the jurisdiction to prosecute. Alliances and international law also take for granted that hostilities will come from attributable

2 Hollis, Duncan B., "Why States Need an International Law for Information Operations," *Lewis And Clark Law Review*, (2007: Vol 11, 1023-XX).

3 Brooks, P., "Flashpoint: The Cyber Challenge," *Armed Forces Journal* (2008).

4 Grant, R., "The Dogs of Web War," Airman Magazine. (January 2008:22-27).

5 Hollis (2007:1026).

6 Umphress, D, "Cyberspace: The New Air and Space?" *Air & Space Power Journal* (Spring 2007).

7 Berkowitz, B, *The New face of War* (New York: The Free Press, 2008:160).

sources, typically with a formal declaration of war. These assumptions, upon which so much of our modern internal and international defensive structure is based, are not appropriate for the wired new world we find ourselves in.

According to the Law of Armed Conflict, attackers must be identifiable. However, as the Estonia situation showed, recognizing an incident as an attack in the first place can be difficult, let alone identifying an attacker who wishes to remain anonymous. The initial events may appear innocent or merely inconvenient, or may get lost in the ubiquitous hum of the attacks already beating on the doors of virtually ever server in the world. A significant attack might initially appear to be "just one more ping among millions of scans,"[8] and the true nature of the incident may not be visible until it is too late to stop it. The identity of the attacker may never be revealed.

In light of this situation, American defensive doctrine needs to establish a way to provide security against cyber threats, regardless of the source's geography, scale, or scope. In cyberspace, it simply does not matter whether the attacker is a foreign government, the mafia, or a 15-year-old hacker. The vulnerabilities and potential impacts are the same. Thus, it is clear that in cyberspace, the defensive decision-making process cannot and should not begin with the question of attribution. Aside from being unanswerable, it is simply the wrong question.

So many cooks

When faced with a cyber threat from an unknown source, someone must take action. The question of defensive responsibility must still be answered – someone must defend us – but cyberspace requires a new basis for forming that answer. Determining jurisdiction or assigning mission areas is no longer a simple question of geography or scope.

Interestingly, despite the difficulties in determining attribution, several government entities have already established broad claims that they are responsible for defending America's portion of cyberspace.

The National Infrastructure Protection Center

The National Infrastructure Protection Center (NIPC) is a joint government and private sector collaborative, located at FBI Headquarters and sponsored by the Department of Justice. It was created in 1998 and true to its origins tends to view cyber security through a law-enforcement lens, using a *"cyberspace is crime scene"* metaphor.

When discussing NIPC's mission, NIPC Director Michael Vatis writes about the need to oppose "criminals [who] use computers and the Internet to steal, defraud, disrupt, destroy, and threaten our data, services, commerce, and national security."[9] This approach assumes jurisdiction over cyber criminals, which is a doubtful assertion in a situation where members of a foreign military are doing the disruption or destruction.

Further supporting the *"cyberspace is crime scene"* metaphor, the FBI's mission includes assessing and responding to "unlawful acts that threaten or target our critical infrastructures," including the information infrastructure. So, along with prosecuting acts that are clearly criminal (such as child pornography), the FBI aims to provide security by preventing computer intrusions and protecting intellectual property.

The use of the phrase "unlawful acts" reveals the FBI's view of cyber threats primarily as unlawful rather than hostile, a matter for law enforcement rather than the military, and predominately domestically-oriented rather than concerned with other nations. At the very least, it assumes there is a distinction between unlawful acts and hostile acts in cyberspace. However, absent a strong attribution capability it is not clear how one might distinguish between the two. A foreign government and an American civilian might both perform the exact same intrusive/hostile act in cyberspace (such as launching a virus or a DDoS attack) and cause a significant amount of damage. Without an ability to identify the instigator, the traditional taxonomy gives us no basis for declaring the act a crime instead of an act of war (or vice versa).

The U.S. military

Naturally, the U.S. military views things differently than the FBI. The DOD, true to its nature, uses a *"cyberspace is battlefield"* metaphor in its assessments of the situation and in determining the actions necessary to ensure security. Military cyber experts talk in terms of threats, attacks, and cyber war, and Umphress goes so far as to claim that when it comes to cyberspace "… we have the front line of a battle at our front door."[10] However, absent a strong authentication capability, the DOD's assertion that hostile acts in cyberspace are war-like is no more justified than the DOJ's assertion that the same acts are criminal. Both agencies assume a dichotomy between digital crime and digital conflict which may not be particularly useful.

In a 2003 article in *SIGNAL Magazine*, White and Sanchez describe a blended mixture of DOJ and DOD responsibilities, explaining that "defense of the nation's cyberspace infrastructure…belongs to several agencies spearheaded by the National Infrastructure Protection Center, Washington D.C. Within the military, responsibility for cyber security belongs to the Defense Department's Joint Task Force, Computer Network Operations, now part of the U.S. Strategic Command."[11] The authors go onto point out that "How either [military] command will work with civilian agencies is an issue under constant scrutiny by national policy makers," indicating that as of 2003, many questions were still unanswered.

8 ibid. p. 161.

9 Vatis, M. (n.d.), "The National Infrastructure Protection Center Overview," retrieved from http://www.calea.org/online/newsletter/No75/The%20National%20Infrastructure%20Protection%20Center.htm.

10 Umphress (2007:5).

11 White G. and Sanchez, J., "Dark screen sheds light on cyberspace security issues," *Signal Magazine Online* (January 2003), retrieved from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=295&zoneid=65.

In 2008, an *Air Force Magazine* article claims that "defending the nation from cyberspace attacks is U.S. Strategic Command's (STRATCOM's) mission – but one of the big challenges is assessing the strategic threat and demarcating lines of response."[12] One might wonder what it means to claim responsibility for something without a well-defined threat or a demarcated line of response. What responsibility are they actually assuming? STRATCOM's ability to accomplish this imprecise mission is likely to be limited in the absence of a well-understood threat or clearly expressed lines of response.

It is worth noting that the mission in question is to defend the nation from "cyber attack," not cyber crime. Just as the FBI's verbiage reflects their crime-oriented perspective, this posture reflects a conflict-oriented point of view, and is consistent with the Department of Defense's prevailing metaphor for cyberspace.

Drilling down even further into the DOD, the U.S. Air Force added cyberspace to its mission statement in 2005, claiming responsibility to fly and fight in that realm. Once again we bump up against the old geographic-based taxonomy of defense, which historically has prevented the military from conducting operational combat activities on U.S. soil. As Grant points out, "Inside the United States, legal precedent and direction limits what the military can do."[13] However, the legal precedent is based on geography, and one might ask whether it makes sense to apply physical geography to cyberspace activities.

This situation begs a number of questions: Is cyberspace inside or outside the U.S. borders? Is there such thing as "America's cyberspace"? When determining jurisdiction, does the physical location of the server or computer matter? Should it? If so, are we talking about the location of the attacking system(s) or the targeted system? What if the attacking system is based in several different countries, none of whom is actually responsible for the attack and many of whom are allies? What if domestic computers are controlled by foreign entities? And even if we answer these questions, it is not clear we will have fully decided whether cyber threats are a matter for the DOD or the DOJ, whether they should be described as conflict or crime.

The National Cyber Security Division

The Department of Homeland Security (DHS) also staked out a piece of the cyber defense mission, creating the National Cyber Security Division (NCSD) in 2003. According to the NCSD website, their mission is to work "collaboratively with public, private and international entities to secure cyberspace and America's cyber assets."[14] This sounds a lot like the claims made by the Air Force, STRATCOM, and the NIPC, with the added role of educating and involving the public. The phrase "America's cyber assets" is particularly interesting, and could theoretically be limited to critical components of the national information infrastructure or expanded to include every server of every bank, grocery store, and university… or even every citizen's personal computer.

Not surprisingly, DHS uses a *"cyberspace is homeland"* metaphor. This is fundamentally different than the DOD or FBI metaphors, and is in line with DHS's understanding of its roles and responsibilities. In a certain sense this might be a more appropriate metaphor than either the battlefield or crime scene metaphors, because it acknowledges the authorized presence of civilians in cyberspace (as opposed to civilians on the battlefield or in a crime scene). However, this metaphor is even more dependent on geographic concepts such as borders and national sovereignty, weakening the propriety of its use in cyberspace.

Industry

In a book titled *The New Face of War*, we find a chapter with the intriguing title "If There Were A Front It Would Be Here."[15] The basic premise of the chapter is that commercial computer security companies are at the vanguard of cybersecurity and would likely be the first to notice a serious cyber attack, if such a thing could be noticed. Thus, rather than viewing law enforcement or military entities as the primary defensive actors, Berkowitz suggests perhaps industry has the lead role.

The chapter introduces a company named Riptech which provides "managed security services"[16] to a wide variety of companies and government agencies. When asked whether Riptech would notify the government if it identified a foreign hacker attacking one of its clients, Riptech officials answered a firm "no way."[17] Riptech made it clear it would leave that decision to its customers, who are described as being "reluctant" to inform the federal government of such an incident. Thus, the entities which are likely to be the prime targets and the first to experience a cyber incident are also the least likely to inform or involve federal authorities. This posture impairs the ability of the DOJ, DOD, or DHS to fulfill their mission of proactively securing cyberspace.

Rather than claim broad responsibility for cyber defense, as the FBI, DOD, and DHS have, industry seems to take a go-it-alone approach, based on a *"cyberspace is marketplace"* metaphor. In this approach, each individual entity is responsible to act as its own first line of defense, and indeed 94% of large organizations in North America have deployed firewalls.[18]

Given the fact that "over 80% of critical infrastructures are controlled by the private sector,"[19] operational responsibility

12 Grant p. 23.

13 ibid. p. 26.

14 Department of Homeland Security overview of National Cybersecurity Division. Retrieved from http://www.dhs.gov/xabout/structure/editorial_0839.shtm.

15 Berkowitz, p. 170-178.

16 ibid. p. 170.

17 ibid. p. 175.

18 White, G., Dietrich, G., Goles, T., "Cyber Security Exercises: Testing An Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events," 37th Hawaii International Conference on System Sciences (2004).

19 Goles, T., White, G. and Dietrich, G., "Dark Screen: An Exercise in Cybersecurity," *MIS Quarterly Executive* (2005, Vol 4 (No 2) 303-318).

for providing cyber security cannot rest solely on government entities. The task must be shared. The interconnected nature of cyberspace, where security is a weakest-link proposition, makes industry's preference for independence and illusion of autonomy an unfortunate position to take.

White hat hackers

Yet another group of contributors to cyber security are the hackers known as *White Hats*. Named after the good guys in cowboy movies, white hat hackers are computer security experts who use their knowledge and skills to help vendors and other enterprises (including government agencies) protect their systems. This unofficial group tends to include highly skilled members, and in fact, "… some of the most advanced techniques for protection are developed by white hats."[20] Government and industry personnel often recruit white hats, tracking them down at conventions such as DEFCON (often described as the largest underground hacking convention in the U.S.).

White hats are generally not concerned with determining whether a threat is foreign or domestic, government-sponsored or individually motivated. Their focus is simply on identifying and fixing vulnerabilities, helping establish and maintain cyber security. They tend to operate with relative autonomy, largely free from traditional opinions of roles and responsibilities. However, government security officials are understandably reluctant to rely on such autonomous, unregulated sources of defensive expertise, since the white hat's availability, capability, and performance are unpredictable.

While the FBI uses a law enforcement metaphor and the DOD uses warlike imagery, White Hats often use a *"cyberspace is the wild west"* metaphor, in which ordinary people are vulnerable and formal protective measures are absent or inadequate. Thus, protecting the citizenry is up to the guy in the white hat, who rides up just in time to stop the villain in the black hat, without regard to where the black hat came from. Given the current state of affairs, this might be the most insightful and appropriate metaphor to guide our understanding and behavior as we attempt to protect our information assets.

Dark Screen

One of the more intriguing, and potentially enlightening, attempts at cyber defense is a joint military/civilian exercise held in September 2002. Named Dark Screen, it involved more than 220 "representatives from government agencies at the local, state, and federal levels; industry; local military bases; and academia."[21] The exercise investigated several key questions about defensive responsibilities in cyberspace, such as how an Air Force intelligence agency might be able to lawfully support local civil authorities who are under attack. Not surprisingly, "the issue of military participation presented more questions than answers."[22]

One of the main conclusions to come out of the Dark Screen exercise is that "communities need new modes of cooperation and collaboration that transcend traditional organizational boundaries."[23] The previous security taxonomy simply does not function in cyberspace, partly because cyberspace is essentially *ageographical*, but also because entities are more interconnected than ever before. This mutual interdependence requires a shared approach to security, and a shared sense of jurisdiction.

Conclusions

In 1984, when a radar indicated "something's out there, floating in the summer sky," we knew what to do. Since the threat was in the air, the Air Force had jurisdiction and would scramble "super-high-tech jet fighters" to get a closer look and engage the targets. But everything is different in the cyberspace environment. "Today, cyber attackers use the speed and global connectivity of the Internet to make national boundaries irrelevant, and sophisticated attackers leave little in the way of electronic evidence that can be used to track or trace them."[24] No longer does geography dictate jurisdiction, and even an independent Cyber Security Agency would need to decide if it were a military organization (i.e., Cyber Force) or a law enforcement entity (i.e., Cyber Police). Instead of dividing responsibility, we need a third way – a way of *joint* responsibility.

We simply cannot rely on the outmoded, geographically-bound defensive taxonomy to determine defensive jurisdiction in cyberspace, however familiar and comfortable it might be. In fact, the very concept of distinct jurisdictions for cyber security needs to be replaced with an appreciation for collective jurisdiction. To effectively provide security in cyberspace, "communities need new modes of cooperation and collaboration that transcend traditional organizational boundaries."[25] The DOD needs to retain its offensive role in cyberspace, and the DOJ should still own the mission of prosecuting criminals, but the task of providing security against incursion and theft is not so easily divided.

The optimal approach to ensuring cyber security is most likely a multi-pronged, loosely-coupled network incorporating law enforcement, intelligence, and military personnel working collaboratively with industry and ordinary citizens from around the globe. This unprecedented need for collaboration introduces a new set of challenges, and highlights the importance of exercises like Dark Screen.

We are all in this together – and that "we" is a broad group indeed, extending well beyond America's physical borders.

20 Hansen, J., Young, S. E., Young, S., Aitel, D., *The hacker's handbook: The strategy behind breaking into and defending networks* (New York: CRC Press, 2003:35).

21 White & Sanchez, 2003.

22 ibid.

23 Goles, et al, p. 316.

24 Lipson, H., "Tracking and Tracing Cyber-attacks: Technical challenges and global policy issues," Carnegie Mellon Special Report CMU/SEI-2002-SR-009 (2002).

25 Goles et al, p. 316.

As White et al point out, "problems in one sector can have a tremendous impact on other sectors as well. What is required are exercises that test not only an individual organization's ability to respond to cyber security events, but also the ability of related external entities, such as cities and states or other industry sector members, to respond in a coordinated manner."[26] Those "related entities" must include American citizens, cities, states, companies, and agencies, but also should extend to our allies around the world.

Current approaches to providing cyber security are often incompatible and incomplete. Worse, they are often independent, as a variety of federal, state, local, and commercial entities try to carve out a portion of the security problem as their own. This independent approach to jurisdictional ownership needs to be reexamined and replaced. Towards this end, we desperately need to regularly host cyber security exercises for a broad coalition of partners. This cooperative approach will foster and enhance the security of our national information infrastructure.

26 White et al, p. 2.

About the Authors

Maj. Dan Ward (USAF) is a developmental engineering officer, currently assigned to the Air Staff's Acquisition Process Office at the Pentagon. Maj. Ward has a BS degree in Electrical Engineering from Clarkson University, an MS degree in Engineering Management from Western New England College, and an MS in Systems Engineering from the Air Force Institute of Technology. Ward is certified Level III in System Planning, Research, Development and Engineering. He can be reached at The.Dan.Ward@gmail.com.

Dr. Michael R. Grimaila, CISM, CISSP, NSA IAM/IEM, is an associate professor and member of the Center for Cyberspace Research at the Air Force Institute of Technology. Dr. Grimaila received a BS and MS degree in Electrical Engineering, and a Ph.D. in Computer Engineering at Texas A&M University. He teaches and conducts research in the areas of information assurance, information warfare, and information operations. He may be reached at michael.grimaila@afit.edu.

Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.