AIR WAR COLLEGE

AIR UNIVERSITY

ACT AND ACTOR ATTRIBUTION IN CYBERSPACE:

A PROPOSED ANALYTIC FRAMEWORK

By

Eric F. Mejia, Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Robert A. Douglas, Col, USAF

14 February 2013

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Colonel Eric F. Mejia is a member of the United States Air Force Judge Advocate General Corps, and is currently assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from Arkansas State University with a Bachelor of Science degree in 1986, and graduated from the University of Arkansas at Little Rock School of Law with a Juris Doctor degree in 1989. He is a Distinguished Graduate of the Air Force's Air Command and Staff College and received his Master's Degree in Military Operational Art and Science in residence in 2004.

Abstract

Cyber attribution continues to vex cyber operators. Often, it is dismissed as impossible to definitively obtain, or worse, unnecessary. Properly analyzed, cyber attribution consists of two components. Actor attribution is concerned with determining who or what entity committed an act of cyber hostility. Act attribution consists of determining the relative severity of a hostile cyber act and whether the act is the equivalent of an armed attack.

Attribution is critically important to government actors because it shapes both the proper response to a hostile cyber act and helps determine the appropriate responding agency. However, despite its highly technical context, cyber attribution is not a science. Instead, it is a subjective analysis similar to the attribution conducted every day by legal practitioners in criminal and civil courts.

This paper proposes a subjective, continuum-based analytic framework for assessing cyber actor and act attribution. Proper application of such a framework helps cyber practitioners assess the proper response and responder for hostile cyber acts, helps define the roles and responsibilities of responding agencies, enhances deterrence, and promotes analytic consistency in an area dominated by ambiguity.

Introduction

Technical Sergeant Pesek rolled out of bed shortly after 6:00 a.m. to get breakfast at the NCO club. He was assigned to the 5th Bomber Group, and had arranged to meet his friends for golf after breakfast. The course in Honolulu was beautiful, and there was no better way to spend a lazy Sunday morning. Waiting for the bus, he admired the beautiful blue sky flecked with distant aircraft. Seeing this many aircraft meant an aircraft carrier was coming into port. Joe wasn't alarmed until the first plane pulled up low over Hickam Air Field with machine guns chattering. The clearly visible rising sun of Imperial Japan on the wings told the story – Japan had attacked Pearl Harbor.[1] The following day, December 8, 1941, America and Japan declared war against each other.

Seventy years later, Air Force Major Shelly Johnson rolled out of bed looking forward to another day of leave in Honolulu. Taking out her smartphone, she tried to scan a check into her account so she would have extra spending money. Despite several attempts, the check failed to deposit into her Bank of America account. Frustrated, she used her tablet to go to the bank's website. However, the home page refused to load. She finished breakfast and tried again, without luck. Irritated, she gave up and got into her car to enjoy her day of leave. A few days later she read the following headline on CNN.com: "Major Banks hit with Biggest Cyberattacks in History."[2] The article explained how several of the largest banks, including Bank of America, had been the subject of a cyber attack. The Islamist group Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the attacks; however, researchers were divided about whether they were responsible. Senator Joe Liberman claimed the attacks were actually conducted by Iran in response to U.S. economic sanctions. The article provided more questions than answers. Major Johnson wondered who actually conducted the attack. Could you even consider this an

attack, and if so, what was attacked, the customers, the individual banks or the U.S. economy? Who would respond, and how?

These two scenarios highlight the critical importance of attribution. In the Pearl Harbor scenario, there was a hostile armed attack, directly attributable to a known state actor. These facts established the proper response, war, and the proper responder, the military. In the second scenario, act and actor attribution were uncertain, and consequently the proper response and responder were equally uncertain. Actor attribution is concerned with determining who is responsible for a hostile cyber act. Act attribution is concerned with the relative severity of the act. Both are necessary to determine the appropriate response to an act of cyber hostility and both help frame which organization should be the primary responder. An analytic framework incorporating both act and actor attribution helps delineate responsibility for hostile cyber acts, and helps determine the appropriate response. This paper examines the definition and importance of cyber attribution and proposes an analytic framework for considering act and actor attribution.

Defining Attribution

The Basic Legal Framework

The legal framework for use of force by states is contained in the Charter of the United Nations. Article 2(4) generally prohibits states from using force against another state: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[3] Two exceptions are recognized. First, Article 42 permits use of force if authorized by the UN Security Council. Second, and more important for our analysis, Article 51 permits use of force in self-defense against an armed attack: "Nothing in

the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations…."[4] These Articles did not originally apply to the conduct of non-state actors. However, international law has developed so that states may use force in self-defense against another state for the acts of non-state actors that are attributed to it[5]. A state may also use defensive force directly against non-state actors if the host state is unable to prevent armed attacks from emanating within its territory.[6] Finally, the use of force is bounded by international law, including the concepts of necessity, proportionality, and distinction. Together, these rules may be summarized as follows:

1. States may generally not use force against other states
2. States may use force against other states if:
    a. Force is authorized by the UN Security Council, or
    b. Force is used in self-defense against an armed attack by:
        i. Another state, or
        ii. A non-state actor if the act can be imputed to a state
3. Force may be used in self-defense directly against non-state actors if the host state is unable to prevent armed attacks by non-state actors
4. Use of force is limited by international law including the law of armed conflict (LOAC)

Determining an appropriate response to a hostile cyber act requires analyzing who the actor is (state, non-state, unknown) and what the act is (armed attack or not an armed attack). In other words, actor and act attribution.

Actor Attribution

Actor attribution is simply determining who should be held responsible for a hostile cyber act. As noted by the 2011 *Department of Defense Strategy for Operating in Cyberspace*,

low barriers to entry for hostile cyber acts, coupled with widespread availably of hacking tools, means that small groups, and even individuals, can impact national security.[7] However, a significant issue from a cyber response perspective is not the identity of the actors, but whether the hostile cyber acts are attributable to a state. This distinction helps determine the appropriate response, responder, and rules for engagement.

Hostile cyber acts can be attributed to a state either directly, or indirectly.[8] The two methods of state attribution are briefly described as follows:

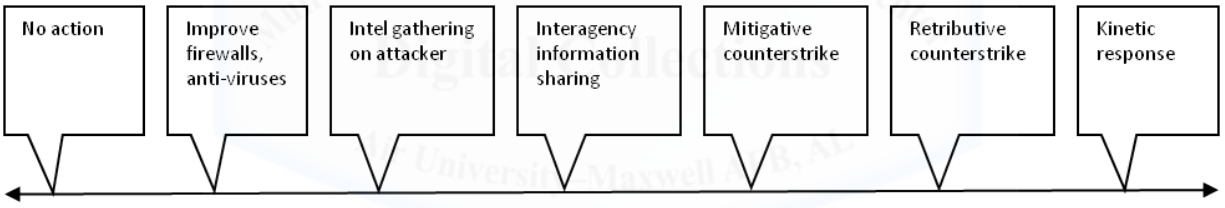
> **Direct Attribution**: States are responsible for the acts or omissions of individuals exercising the state's machinery of power and authority since these actions are attributed to the state even if the acts exceed the authority granted by the state.
>
> **Indirect Attribution**: Acts or omissions of non-state actors are generally not attributable to the state; however, the state may incur responsibility if it fails to exercise due diligence in preventing or reacting to such acts or omissions.[9]

Further, although not universally accepted in international law, it is generally accepted in practice that a state's right to use force in self-defense is also triggered by armed attacks which cannot be attributed to a state. For example, an armed attack may emanate from a state without that state's knowledge of the attack or ability to prevent it. In such circumstances, the armed attack is attributed directly to the attackers and the victim state may defend with force directly against the non-state actors despite their being located in a neutral or even allied state. As recently noted in the *Journal of Conflict and Security Law*, it is the nature of the hostile act that triggers the right to self-defense, not the nature of the actor.[10] This simply comports with common sense. A state should not be required to endure an armed attack by non-state actors when it has the means to defend itself consistent with fundamental LOAC principles. U.S.

attacks against terrorists operating within Pakistan are one concrete application of this concept. Once a state has been subjected to an armed attack, it may forcibly defend itself. The decision of whether to do so or not is a matter of policy, and ultimately the response must satisfy basic LOAC principles including necessity, proportionality and distinction.

Act Attribution

Act Attribution is the process of defining the severity of the hostile cyber act.[11] Hostile cyber acts may range from something as benign as attempting to ping a network computer, to an attack on the U.S. power grid leaving millions without power for months.[12] Similarly, there is a broad range of potential defensive actions that may be taken by the victim state. A simple continuum of potential responses illustrates this:



Supplementing these potential actions is a state's full range of diplomatic and political responses to cyber hostility. However, any response by a victim state must be determined in part by the severity of the hostile act.

A state may passively defend against all hostile actions; however, it may only forcibly retaliate in self-defense against armed attacks. By extension, imminent armed attacks allow states to respond in anticipatory self-defense.[13] International law is silent on whether a cyber attack can be considered an armed attack. However, the United States has taken the position that a cyber attack can be considered an armed attack. The May 2011 *International Strategy for*

Cyberspace states: "Right of Self-Defense: Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."[14] This echoes the language of Article 51 of the UN Charter which states that states have the inherent right to engage in individual or collective self-defense in response to an armed attack.[15] So, clearly the United States has adopted the position that a hostile cyber act may be treated as an armed attack. But, given the range of hostile cyber actions, how do we determine whether a hostile cyber act rises to the level of an armed attack? If the effects of a cyber attack are the equivalent of a traditional armed attack, then states should be permitted to respond accordingly. The leading proponent of this effects-based approach is Michael N. Schmitt. His effects-based analysis offers a method of analyzing hostile cyber acts based on six criteria:

1. Severity: Armed attacks threaten physical injury or destruction of property to a greater degree than other forms of coercion.
2. Immediacy: Armed attacks usually occur with greater immediacy.
3. Directness: Armed attacks have a more direct link to the negative consequences caused.
4. Invasiveness: Armed attacks usually cross into the target state to cause harm.
5. Measurability: The consequences of an armed attack are easier to measure.
6. Presumptive Legitimacy: Because of the general prohibition on the use of armed force between states in international law, an armed attack is presumed illegitimate.[16]

This framework can readily be applied to cyber attacks to determine whether a given hostile act may be considered an armed attack.[17] If so, a forcible response may be appropriate. If not, some lesser form of response may appropriate.

The Importance of Attribution

An assessment of both act and actor attribution is central in determining the appropriate response to a hostile cyber act. The government may respond to a hostile cyber act in a variety of ways including monitoring, improving passive defenses, applying political pressure, employing active defenses, and counterstriking with both cyber and kinetic weapons. Passive defense is defined as "[m]easures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative."[18] Passive defense in the cyber realm includes making systems more difficult to attack through anti-viruses and firewalls, educating users to be more security conscious, and reducing post-attack recovery times through redundancy and backup systems.[19] By contrast, active defense is defined as "[t]he employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[20] In the cyber realm this translates to initiating a cyber attack as a defensive response to a hostile cyber attack.[21] Defensive cyber attacks can be broken down into two types. If the goal is to mitigate harm to a targeted system using only the amount of force necessary to protect the system from further damage, it is considered a mitigative counterstrike.[22] The purpose of a mitigative counterstrike must be to mitigate damage from an immediate threat.[23] If the goal of the counterstrike is to punish the attacker, it is considered a retributive counterstrike.[24] Under international law, only the mitigative counterstrike is truly defensive because its purpose is to defend against an immediate threat.

Actor and act attribution is also critical in determining which governmental entity should take the lead in responding to a hostile cyber act. Several governmental agencies are tasked with cyber operations and responsibilities. As noted by General Keith B. Alexander, commander for United States Cyber Command, these agencies include:

- Department of Defense/Intelligence Community/NSA/Cyber Command: Responsible for detection, prevention, and defense in foreign space, foreign cyber threat intelligence and attribution, security of national security and military systems, and, in extremis, defense of the homeland if the nation comes under cyber attack from a full scope actor.
- Department of Homeland Security: Lead for coordinating the overall national effort to enhance the cybersecurity of U.S. critical infrastructure and ensuring protection of the civilian federal government (.gov) networks and systems.
- Federal Bureau of Investigation (FBI): Responsible for detection, investigation, prevention, and response within the domestic arena under their authorities for law enforcement, domestic intelligence, counterintelligence, and counterterrorism. Importantly, when malicious cyber activity is detected in domestic space, the FBI takes the lead to prevent, investigate, and mitigate it.[25]

The Difficulty of Conclusive Attribution

Both act and actor attribution is difficult to prove to a scientific certainty. Computer networks are not designed to facilitate attribution, and hostile actors exploit this weakness to hide their true identity. For example, on the internet, sender identification information is typically unused during the sending process so its source information can easily be forged. Masking the sender information in this manner is commonly referred to as "spoofing." A hostile cyber actor can also hide their identity and location by employing a system that transforms data in some manner, known as a laundering host. Cyber actors may also employ an attack that is complete in milliseconds, or alternatively, is spread out over months. All of these factors make cyber actor attribution difficult.[26] Even if the technical issue of attribution is overcome, what degree of confidence must be achieved to support a finding that a state is responsible under international

law? Certain? Very Certain? These are subjective political determinations that simply do not lend themselves to precise quantitative analysis.

This same issue exists when trying to assess act attribution. Using the Schmitt model to determine if a hostile cyber act is tantamount to an armed attack requires applying a subjective analysis. How severe is severe? What is the definition of immediate? What constitutes a direct link between a hostile cyber act and the consequences of the act? All of these questions require a subjective, non-scientific assessment.

Fortunately, the legal community has been dealing with the problem of subjective actor and act attribution and has extensively developed the concepts and lexicon related to subjective attribution. This is most evident in the law related to civil and criminal trials. Legal experts refer to these subjective standards as "standards of proof." A few of the more common standards of proof, in order of the degree of certainty, are:

- Scintilla of Evidence: The least amount of evidence possible.
- Preponderance of the Evidence: In a civil trial the issue to be decided is often whether or not one party is negligent, and therefore financially responsible for the losses incurred by the other party. The subjective standard used by courts to assess this question of liability is called the preponderance of the evidence standard. This is simply defined as more probable than not.
- Clear and Convincing Evidence: Creating a firm belief or conviction. It is an intermediate level of proof, being more than a preponderance of the evidence, but less than what is required for proof beyond a reasonable doubt.
- Beyond a Reasonable Doubt: This is the standard used to establish criminal guilt, which is the equivalent of actor attribution, as well as to determine the specific criminal offense

committed, which is the equivalent of act attribution. It means entirely convinced and satisfied to a moral certainty. However, it is less than a scientific certainty.[27]

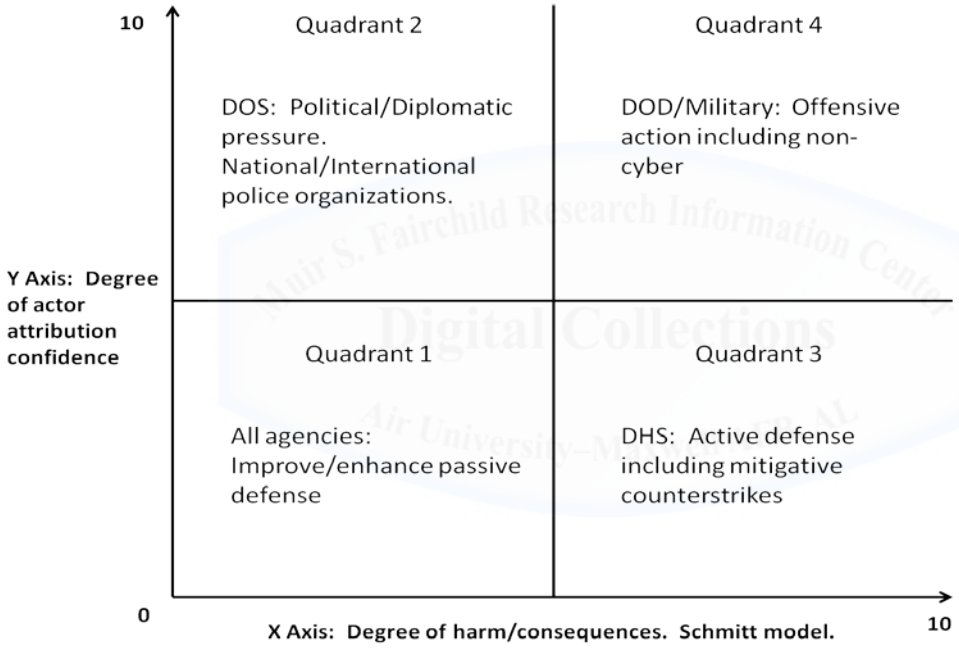
Employing legal subjective criteria is not a new or novel idea. In a 2009 Microsoft white paper the author suggested a similar subjective assessment for cyber attribution:

> "it [is] important to focus on probability of accurate attribution, as opposed to certainty of attribution. In many areas, of course, absolute certainty is seldom achievable. For this reason, a range of different standards have developed (for example, proof beyond a reasonable doubt, a preponderance of the evidence) and individuals and organizations often have to rely upon probabilities when making critical decisions (such as when opting for one medical treatment over another). Of course, the greater the certainty, the easier it may be to choose a course of action, but that does not mean certainty is required before reasonable action can be taken."[28]

While it would be naïve to assume that one could import the whole of court-based attribution concepts to assess cyber attribution, several key points are evident. First, scientific proof is not necessary for attribution. While scientific certainty is the "gold standard" of proof, it is rarely obtainable, and historically has not been necessary to establish attribution. Second, as previously noted, attribution is routinely based on subjective determinations. Third, when using a subjective assessment of attribution, severity of the consequences is linked to the degree of confidence. A court may assess financial responsibility based on a preponderance of the evidence, but it takes a much higher degree of confidence to establish criminal guilt. Finally, although many technical experts may be hesitant or uncomfortable using a subjective assessment, the government, through its legal community, has at its disposal established expertise in subjective attribution.

An Analytic Model for Actor and Act Attribution

Based on the foregoing, the factors that should be included in any proposed analytic model should be based on a subjective assessment of act and actor attribution. An assessment of these factors should indicate who should respond to an act of cyber hostility, and what the upper range of appropriate responses should be. Ideally, the responses would incorporate basic LOAC principles. Combining these basic concepts yields the following proposed analytic model:



Several issues are worth noting. First, the responsive actions in each quadrant represent the upper limits of an appropriate response. For example, the Department of State (DOS) may elect not to apply diplomatic pressure to a state actor for a variety of reasons, even if diplomatic pressure as a result of hostile cyber acts would be justified. Additionally, act and actor attribution is dynamic. Although an act may appear harmless at first, subsequent information may show it to be significantly more harmful than initially believed. Finally, the quadrants do

not reflect sole responsibility for responding to hostile cyber acts. However, the framework does help assign primary or lead responsibility, with other agencies in a supporting role.

Quadrant 1: Low actor attribution confidence, low degree of harm.

In this common scenario, governmental agencies are faced with numerous relatively innocuous yet unauthorized cyber acts. For example, in June 3, 2010, General Alexander, the commander for U.S. Cyber Command, stated that Department of Defense systems are probed by unauthorized cyber actors approximately 250,000 times per hour, or the equivalent of over 6 million times each day.[29] Most cause no damage and do not result in a compromise of data. According to the United States Computer Emergency Readiness Team (US-CERT), in 2009, approximately 73.4% of all reported cyber incidents were categorized as Category 5, Scans, Probes, or Attempted Access. This includes "[a]ny activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service."[30] For these types of acts, passive defense is an appropriate response. The vast majority of Quadrant 1 actions are easily defeated by encryption, firewalls, anti-virus and anti-malware programs, and other purely passive measures.

Quadrant 2: High actor attribution confidence, low degree of harm.

In this scenario, the government is again faced with acts that cause little harm. However, the acts are still unauthorized and may be the harbinger of more serious, and more harmful, future acts. Unlike the scenario in Quadrant 1, the acts can confidently be attributed to an identified actor. Under these circumstances, passive defensive measures alone may be insufficient. However, because the acts are insufficiently harmful to be considered equivalent to an armed attack, offensive strikes and defensive counterstrikes are not necessary or proportional

to the harm being caused. For state actors, in addition to passive defense, employing appropriate diplomatic pressure may be appropriate. This approach is consistent with the May 2011 International Strategy for Cyberspace. This document states that the U.S. will combine diplomacy, defense and development to achieve the national goal of cybersecurity.[31] Diplomatic efforts will be focused on engaging "the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace and the actions necessary, both domestically and as an international community, to build a system of cyberspace stability."[32] Diplomatic efforts to stem the tide of less serious cyber acts are not new. For several years the U.S. has been engaged in diplomatic efforts to dissuade China from continuing cyber espionage against the U.S. government and U.S. corporations. Most recently, U.S. Defense Secretary Leon Panetta spent three days in China addressing the issue of China's cyber activity.[33] This is an appropriate response to state attributed cyber acts which fall short of being an armed attack. As noted by James Lewis, cybersecurity expert with the Center for Strategic and International Studies: "The damage from Chinese cyber espionage is easy to overstate but that doesn't mean we should accept it."[34] To facilitate diplomatic efforts at cybersecurity, a new office within the Department of State was recently created. The Office of the Coordinator for Cyber Issues is tasked with coordinating the State Department's global diplomatic engagement on cyber issues, serving as the DOS liaison to the White House and federal departments and agencies on cyber issues and advising the Secretary and Deputy Secretaries on cyber issues and engagements.[35] If the hostile actor is a non-state affiliated individual or group, the Federal Bureau of Investigation, Department of Justice or analogous international organizations will be primarily responsible for any investigation and prosecution, if appropriate.

Quadrant 3: Low actor attribution confidence, high degree of harm.

In this scenario, the government is faced with a hostile cyber act, capable of causing significant harm. The harm threatened, or caused, may be sufficient to be considered the equivalent of an armed attack. Within the cyber realm, this may involve harming the nation's key resources or critical infrastructure. However, there is insufficient evidence to confidently attribute the act to a specific state or non-state actor. One potential example of this would be unidentified actors using a state's IT infrastructure to conduct an attack without the consent, or even knowledge of that state. Retributive strikes require attribution, which is lacking in this scenario. However, the LOAC still permits action in self-defense. When a state is unable to prevent attacks emanating from inside its borders, or the attackers operate independently of the state, the victim state may still use force in self-defense provided the requirements of necessity, proportionality, and distinction are met.[36] Under these circumstances, active defenses, including mitigative counterstrikes, may be appropriate. The goal of mitigative counterstriking is to "mitigate damage from a current and immediate threat."[37] These active, but purely defensive measures can trace an attack back to its source and immediately interrupt the attack. Further, mitigative counterstrikes are relatively precise. This precision limits the risk of excessive collateral damage. Limiting collateral damage helps satisfy the requirement of proportionality and helps reduce the risk of escalating cyber attacks into full scale kinetic attacks between states.[38] Finally, because of its precision, reduced risk of collateral damage, and purely defensive nature, automated mitigative counterstrikes are less likely to violate international law of armed conflict norms.

Mitigation of cyber attacks is squarely within the purview of the Department of Homeland Security. Homeland Security Presidential Directive 7 establishes the national policy

for identifying and protecting critical U.S. infrastructure, and defines the roles of the various federal and state departments. The Secretary of Homeland Security is responsible for "for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States [and serves as] the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."[39] To fulfill this responsibility DHS created the National Cyber Security Division which is responsible for analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.[40] One of its specified missions is safeguarding and securing cyberspace, and one of its key strategic outcomes in performing this mission is that "[c]yber disruptions or attacks are detected in real-time, consequences are mitigated, and services are restored rapidly."[41]

Quadrant 4: High actor attribution confidence, high degree of harm.

In this scenario, the government is faced with a hostile cyber act tantamount to an armed attack. Further, there is a high degree of actor attribution confidence. Conceptually this is the equivalent of a kinetic attack against the U.S., and therefore a Department of Defense response is appropriate. Further, there is no prohibition against responding with kinetic force against a cyber attack provided the response meets traditional LOAC requirements. This, too, is consistent with the 2011 International Strategy for Cyberspace, which states: "We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense…When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[42]

There is little controversy that the DoD should be the lead agency in this scenario. As noted by the commander of the United States Cyber Command, in extreme situations, it is the role of the DoD to defend "the homeland if the Nation comes under cyber attack from a full scope actor."[43] However, some argue that the DoD should take a more expansive role in cybersecurity, essentially performing DHS's assigned role. Much of this argument is based on the perceived effectiveness of the DoD, or rather the perceived infectiveness of DHS. However, an expanded role for DoD in cybersecurity is the wrong approach. First, it unnecessarily expands the role of the military. The military would undoubtedly perform well at securing transportation hubs, power plants, water treatment facilities, critical manufacturing sites and other critical national infrastructure. However, that is not the mission of the military; the mission of the military is to wage war. Further, effective cyber defense requires a degree of domestic intrusion which should not be conducted by the DoD. As noted by Major General (retired) Charles Dunlap, "The armed forces are the most authoritarian, least democratic, and most powerful institution in American society. The restraint intrinsic to a domestic law enforcement mind-set is not its natural state… If nothing else, the fact that the armed forces unapologetically restrict the rights and privileges of their own members should militate toward avoiding their use in civilian settings where the public properly expects those rights and privileges to flourish."[44]

Conclusion and Recommendations

First, the cyber community must recognize the critical importance of attribution. It is the basis for effective diplomacy, law enforcement and a prerequisite for offensive military counterstrikes under the law of armed conflict. The first fundamental question that must be answered after a hostile act is who committed the act. The second is "how much damage was done?" An accurate assessment of actor and act attribution helps defines both the proper

response to an act of cyber aggression and helps determine the appropriate lead agency to respond to such an act.

Second, because actor and act attribution fundamentally drive cyber defense, efforts to enhance technical attribution should be given priority. Although assessing attribution is subjective, often the evidence used in such an assessment is technical. Attributing a hostile cyber act is a prerequisite to effective deterrence. No hostile actor, whether nation state or rogue individual, will ever be deterred from hostile cyber activity if they can effectively deny responsibility. Further, the international community is unlikely to support military action unless a hostile act, equivalent to an armed attack, can successfully be attributed to an offending party. Because hostile actors will continue to develop new methods to mask their activity, effective deterrence demands that the U.S. continue to enhance its technical attribution capability.

Third, legal expertise is critical in assessing attribution and framing an appropriate response. Although the cyber domain is relatively new, the art of actor and act attribution is ancient. Every criminal prosecution that has ever occurred fundamentally required a subjective determination of guilt (actor attribution) and offense (act attribution). Legal practitioners, although often ignorant of the technical aspects of the cyber domain, are well versed in the art of attribution. Cyber experts may be technically adept, but are often ignorant of the nuances of subjective attribution. Close integration of both legal experts and technical cyber experts is critical to establishing an appropriate cyber policy and appropriate responses to specific hostile cyber acts.

Finally, an analytic framework is an essential tool for cyber practitioners. In a field where significant ambiguity may exist both as to the nature of the act, and the identity of the actor, an analytic construct promotes analytic consistency. Additionally, it helps define roles and

missions for various actors and provides a common framework and understanding of responsibility. An analytic framework also enhances deterrence by providing notice to hostile cyber actors that the consequences they should expect from committing a hostile cyber act are determined, in part, by the severity of the hostile act and that a sufficiently severe hostile act will merit a military response.

Notes

1. "Tech. Sgt Pesek Runs For His Life At Hickam," http://www.pearlharbor.org/eyewitness-accounts.asp (accessed 5 November 2012).

2. David Goldman, "Major Banks Hit with Biggest Cyber Attacks in History," CNN.com, 28 September 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html (accessed 22 January 2013).

3. United Nations, *Charter of the United Nations*, 24 October 1945, Ch. I, Art. 2(4).

4. United Nations, *Charter of the United Nations*, 24 October 1945, Ch. VII, Art. 51.

5. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, Inc., 2012), 53.

6. Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (Summer 2012): 7, available at http://jcsl.oxfordjournals.org/content/17/2/229.full.pdf+html.

7. U.S. Department of Defense, *2011 Department of Defense Strategy for Operating in Cyberspace* (Washington D.C., July 2011), 3.

8. Many commentators use the terms attribution or direct responsibility, and imputed or indirect responsibility. However, since imputed responsibility is functionally the equivalent of attributing the hostile act to the state, the term indirect attribution is used to clarify the discussion.

9. Jan Arno Hessbruegge, "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law," *New York University Journal of International Law and Politics*, 36 (Winter/Spring 2004): 268.

10. "Cyber Attacks, Self-Defence and the Problem of Attribution," 7.

11. Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law & Criminology* 97, no. 2 (2007): 379, (Using the terms "attack" and "attacker" attribution, or "who" and "what" attribution).

12. A ping is a test to see if a system on the Internet is working. "Pinging" a server tests and records the response time of the server. http://www.techterms.com/definition/ping.

13. *Inside Cyber Warfare*, 58.

14. President, *International Strategy for Cyberspace* (Washington D.C., May 2011), 10.

15. *Charter of the United Nations*, Art. 51.

16. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, 37 (1999): 914-915.

17. For an excellent example of an application of the Schmitt analysis see Andrew C. Fultz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate," *Joint Forces Quarterly*, 67, (4th Quarter 2012), 40-48.

18. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 August 2012), 237.

19. William A. Owens, et al, ed., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington D.C.: The National Academies Press, 2009): 13, http://www.nap.edu/catalog.php?record_id=12651.

20. JP 1-02, 2.

21. *Technology, Policy, Law and Ethics*,134.

22. Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," *Harvard Journal of Law and Technology* 25, no. 2 (Spring 2012): 421.

23. Ibid., 421.

24. Ibid., 420.

25. General Keith B. Alexander, Statement before the Senate Committee on Armed Services, 27 March 2012, 12-13, http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf.

26. Statement of Dr. David A. Wheeler, Institute for Defense Analysis, in House, *Planning for the Future of Cyber Attack Attribution, Hearings Before the Committee on Science and Technology, Subcommittee on Technology and Innovation*, 15 July 2010, 3.

27. Black's Law Dictionary (5th ed., 1979), 147.

28. Scott Charney, "Rethinking the Cyber Threat: A Framework and Path Forward," Microsoft White Paper (Redmond, WA: Microsoft Corp., 2009), 9.

29. Gen Keith Alexander, "U.S. Cybersecurity Policy and the Role of U.S. Cybercom," (address to the Center for Strategic and International Studies, Washington D.C., 3 June 2010).

30. United States Computer Emergency Readiness Team, "Quarterly Trends and Analysis Report," (Washington D.C., Department of Homeland Security, 16 June 2009), 2.

31. *International Strategy for Cyberspace*, 11.

32. Ibid.

33. CBS/AP, "China Stonewalls Panetta on Cyber Attacks," CBS News, 20 September 2012, http://www.cbsnews.com/8301-202_162-57516541/china-stonewalls-panetta-on-cyberattacks/ (accessed 24 January 2013).

34. Ibid.

35. U.S. Department of State, Office of the Coordinator for Cyber Issues home page, http://www.state.gov/s/cyberissues/index.htm#.

36. "Cyber Attacks, Self-defence and the Problem of Attribution," 7.

37. "Mitigative Counterstriking," 421.

38. "Inside Cyber Warfare," 72.

39. Homeland Security Presidential Directive 7 (HSPD 7), "Critical Infrastructure Identification, Prioritization and Protection," 17 December 2003, para. 12, available at http://www.dhs.gov/homeland-security-presidential-directive-7#1.

40. HSPD 7, para. 16.

41. U.S. Department of Homeland Security, "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland," February 2010, 54.

42. *International Strategy for Cyberspace*, 13-14.

43. General Keith B. Alexander, Statement before the Senate Committee on Armed Services, 13.

44. Maj Gen (Ret) Charles J. Dunlap, Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 93-94.

Bibliography

Alexander, Gen Keith B. Statement before the Senate Committee on Armed Services, 27 March 2012.

Alexander, Gen Keith B. Statement. "U.S. Cybersecurity Policy and the Role of U.S. Cybercom." Center for Strategic and International Studies, Washington D.C., 3 June 2010.

Black's Law Dictionary (5th ed., 1979).

Brenner, Susan W. "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare." *The Journal of Criminal Law & Criminology* 97, no. 2 (2007).

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, Inc., 2012.

CBS/AP. "China Stonewalls Panetta on Cyber Attacks." *CBS News*, 20 September 2012. http://www.cbsnews.com/8301-202_162-57516541/china-stonewalls-panetta-on-cyberattacks/.

Charney, Scott. "Rethinking the Cyber Threat: A Framework and Path Forward." Microsoft White Paper. Redmond, WA: Microsoft Corp., 2009.

Dunlap, Maj Gen (Ret) Charles, J., Jr. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011).

Fultz, Andrew C. "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate." *Joint Forces Quarterly*, 67 (4th Quarter 2012).

Goldman, David. "Major Banks Hit with Biggest Cyber Attacks in History." *CNN.com*, 28 September 2012. http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

Hessbruegge, Jan Arno. "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law." *New York University Journal of International Law and Politics*, 36 (Winter/Spring 2004).

Kesan, Jay P., and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law and Technology* 25, no. 2 (Spring 2012).

Owens, William A., et al., ed. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington D.C.: The National Academies Press, 2009. http://www.nap.edu/catalog.php?record_id=12651.

Pearl Harbor.org. "Eyewitness Accounts: Hickham Field – Army Air Corps Sergeant." http://www.pearlharbor.org/eyewitness-accounts.asp.

President. Homeland Security Presidential Directive 7 (HSPD 7). "Critical Infrastructure Identification, Prioritization and Protection." 17 December 2003. http://www.dhs.gov/homeland-security-presidential-directive-7#1.

President. *International Strategy for Cyberspace*. May 2011.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law*, 37 (1999).

Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law* 17, no. 2 (Summer 2012). http://jcsl.oxfordjournals.org/content/17/2/229.full.pdf+html.

United Nations. *Charter of the United Nations*, 24 October 1945.

U.S. Computer Emergency Readiness Team. "Quarterly Trends and Analysis Report." Washington D.C.: Department of Homeland Security, 16 June 2009.
U.S. Department of Defense. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 August 2012).
U.S. Department of Defense. *2011 Department of Defense Strategy for Operating in Cyberspace*, July 2011.
U.S. Department of Homeland Security. "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland." February 2010.
U.S. Department of State, Office of the Coordinator for Cyber Issues home page. http://www.state.gov/s/cyberissues/index.htm#.
Wheeler, Dr. David A., Institute for Defense Analysis. Statement before the House Committee on Science and Technology, Subcommittee on Technology and Innovation, 15 July 2010.