Laser-guided bombs line flight deck of aircraft carrier USS *John F. Kennedy* in preparation for air strikes against Iraq during Operation *Desert Storm* (PH2 Lipski)

Determining Hostile Intent in Cyberspace

By Ramberto A. Torruella, Jr.

Okay, bogies have jinked back at me again for the fifth time. They're on my nose now. Inside of 20 miles."

This was the report made by Commander Steven Collins, USN, Radar Intercept Officer (RIO) of Gypsy 207, prior to arming his F-14's radar-guided missiles. Two Libyan MiG-23 Floggers were inbound to the *John F. Kennedy* Carrier Strike Group. Two F-14 Tomcats of VF-32 were assigned to intercept. The Tomcats flew low, lost in the radar clutter kicked up by the sea's surface, maneuvering several times to stay out of the Libyan fighters' engagement envelope. The Americans maintained a constant fire control lock on their opponents. The MiGs matched each American maneuver unerringly, ignoring the radar lock warnings growling in their cockpits. Because the radar on the MiG fighters could not detect the Americans through the clutter, the Libyans relied on guidance from shore-based radar stations for a ground-controlled intercept. The MiGs kept their noses pointed toward the Americans, hoping their radar would burn through the clutter and give them a chance to shoot first. It was clear the Libyans wanted a fight. It was clear they had *hostile intent*.

"13 miles. Fox 1! Fox 1!" the RIO shouted as the missiles left the rails of the Tomcat, initiating an engagement that would end with two MiGs destroyed and two Libyan pilots lost at sea (paraphrased

Commander Ramberto A. Torruella, Jr., USN, is the Joint Staff J8 Models and Analysis Information Technology Support Branch Chief.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Determining Hostile Intent in Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Joint Force Quarterly,260 Fifth Avenue, S.W. (Building 64, Room 2504) Fort Lesley J. McNair,Washinggton,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**8**	

from "Splash Two MiGs," an account of the 1989 Gulf of Sidra Incident).[1]

According to the Joint Chiefs of Staff, *hostile intent* is defined as the threat of imminent use of force against the United States, U.S. forces, or other designated persons or property.[2] It is the indication, the *belief*, a commander has that an adversary is about to attack. That belief provides the groundwork for "anticipatory self-defense," an American legal concept that allows a commander to attack before being attacked.[3]

From the point of view of the American pilots, the Libyan pilots showed hostile intent by flying a vector toward the American Carrier Strike Group, constantly maneuvering to threaten the American interceptors, and ignoring the obvious warning signal of American fire control radar locked onto their aircraft. Libyan actions gave the Americans the *belief* that an attack was imminent. The Americans launched their own missile strike as a result: a clear case of anticipatory self-defense, a preemptive attack that spoils the anticipated attack of an enemy. Interestingly, from the Libyan point of view, the Americans also clearly showed hostile intent by constantly illuminating the Libyan fighters with their fire control radar, the last step the Libyans would detect prior to an American missile attack.

Determining hostile intent is often not this clear, but in this instance, within the physical realm of fighter jets, radars, and missiles, the evidence strongly suggests that both parties demonstrated hostile intent.

This is rarely the case in cyberspace.

Information as a Weapon, Cyberspace as an Abstraction

The cyberspace realm is an abstraction, with components located in a physical space but operations occurring in a nonphysical space, where the terrain is data and information is used as a weapon. This is not new. The ancient Phoenicians pioneered information as an abstraction when they laid the foundation for our alphabet, an abstraction necessary for transmitting concepts via the written word. Medieval Arabs developed our number system, an abstraction necessary to communicate complex calculations. Commanders from Alexander the Great to Napoleon used both of these abstractions to send dispatches in clear text and code—to communicate with subordinates, coordinate actions in real space, and hide their intentions from opponents. Eventually, special signal corps evolved to encrypt, transmit, receive, and handle messages, first at the rate of the written word and the horse, then at the rate of signal flags, telegraphs, and flashing lights. Code breakers ancient and modern fought a silent war to understand enemy signals and gain access to enemy information.

But it was not until the late 20th century, when improvements in communication and computing technology raised the volume and velocity of data flow from dozens of words per minute to 1.5 trillion words per minute, that the information domain gained enough significance to be treated as a warfare area in its own right.[4] An adversary with access to a commander's data flow now possessed a far richer set of information regarding intentions and operations. More importantly, if an adversary could deny the commander necessary information or, better yet, *change* information needed to make a decision, disastrous effects could occur in real space. For instance, what if the Libyans were able to fool the American radars and combat systems into believing their MiGs were farther away or on a different vector? Would confusion have ensued? Would the world be lamenting (or celebrating) a different outcome?

This is not the first time, and probably not the last, that a change in technology caused an abstraction to evolve into a warfighting domain. Consider the concept of the high ground. In the 6th century BCE, the military philosopher Sun Tzu plainly articulated the benefit of operations from the higher ground; a commander has greater visibility over enemy movements and is better situated to defend against attack.[5] It was even axiomatic in ancient times that military possession of higher ground would greatly increase the chance of combat success. During the late 18th century, however, the French Revolutionary Army experimented with a technology that turned that land-based abstraction (*hold the high ground*) into the start of a useful warfighting domain; it started using balloons for aerial reconnaissance of the battlefield.[6] Soon, other countries experimented with using balloons for observation, bombing the enemy, or increasing the range of communications. Most experiments met with modest success; the technology simply was not robust enough to deliver consistent battlefield results.

But once the airplane was invented, everything changed. Aerial reconnaissance became consistent and soon was vital to events on the ground. Artillery spotting was added to the airman's list of vital tasks as well as reconnaissance deep inside of enemy lines. Change occurred again when the first airman aimed a pistol at an enemy observer in another aircraft. An arms race quickly ensued—planes increased in number, specialized in purpose, and carried specially developed weapons meant to shoot down other aircraft. They flew faster and higher and fought for dominance of the air. Commanders now prioritized effects in the air over direct effects on the ground, and air warfare, a new warfighting domain, was born.

Hostile Intent in an Abstract Domain

Cyber warfighters learn from the evolution of other domains, especially with regard to the legal authorities associated with the use of force and armed combat, the Law of Armed Conflict. Just as aviators learned to apply the Law of Armed Conflict in their new domain, so will commanders who operate in the cyber domain.

Cyberspace has its own unique challenges. Attributing a cyber attack is difficult at best because commanders are rarely ever sure of the source of an attack or intrusion, and establishing the forensic evidence needed to be certain is a time-consuming and often imprecise science. Intentions are even harder to discern. For example, does malware beaconing to an Internet protocol address in China indicate an attempt to steal data? Is it a

F-14D Tomcat conducts mission over Persian Gulf region (U.S. Air Force/Rob Tabor)

precursor for establishing a botnet? Is the malware even Chinese? Is placing malware even considered a use of force? Unfortunately, there is little to no international consensus on what constitutes a use of force in cyberspace.[7]

This article discusses the legal authorities to use force in cyberspace. It discusses what constitutes the use of force in cyberspace and how a commander can determine if an opponent intends to use force against the United States or its assets and interests. The article builds on a rubric developed by Michael Schmitt to help identify hostile intentions in cyberspace and, using a spectrum of cyber activity developed by Gary Brown and Owen Tullos, suggests in general what may be appropriate responses to hostile intent. Finally, the article briefly addresses the legal roles, responsibilities, and authorities required for addressing the different types of cyber attacks with an eye to identifying and responding to hostile intent.

Classifying Use of Force in Cyberspace

Article 2, Paragraph 4, of the United Nations (UN) Charter specifically states that "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." Force, in this case, does not mean coercion, but the use of *armed* force as a tool of coercion or persuasion. Matthew Waxman notes that the framers of the UN Charter did not set out to end coercive behaviors in international relations, but to end *war* as a legitimate tool of policy except in the case of self-defense. The prohibition against force is a prohibition against armed attack.[8]

Waxman also notes that when the framers set about to prohibit the use of force, they took an *instruments*-based point of view instead of an *effects*-based point of view of limiting coercion.[9] This means that the framers intentionally sought to limit *how* coercion could be performed in international politics, not limit the *effects* of coercion on a target nation. For instance, armed attacks and kinetic strikes are not authorized, nor are blockades, bombardments, or any other classic use of military power, except in self-defense or as authorized by the UN Security Council for the peace and security of the international community. However, diplomatic isolation and economic coercion are perfectly authorized by the charter. A nation can target an embargo against another nation, but it cannot conduct a naval blockade without the express authorization of the Security Council. Both actions may have the same effect on the targeted nation—severe economic damage as a form of coercive pressure—but the charter explicitly prohibits a blockade and not an embargo.

This creates a difficulty when dealing with potentially hostile actions that occur in cyberspace. By their very definition, cyber actions occur in an abstract realm of data representation, not physical force. So even if a cyber action causes tremendous destruction by overloading an electric grid or shutting down a critical energy pipeline, legally speaking, the cyber action is not necessarily a prohibited use of force.

Andrew Folz notes that several legal frameworks have evolved that address the gap in the way international law views force in cyberspace. Almost all shift away from a strictly instruments-based view. The first is an effects-based approach where the "quantum of damage and not the means of attack" determines if an action in cyberspace is a prohibited use of force.[10] This approach only looks at the damage done as a result of the attack and ignores how an attack was delivered. While this framework is relatively simple to apply, it represents a major break from the way the international community already deals with issues of force by completely setting aside the instruments-based framework. Blockades and embargoes would essentially become the same thing, and the international community would lose major tools in conducting international relations. What is worse, it would lead to a subjective assessment of what constitutes a hostile action in cyberspace. If a quantum-of-damage approach is used, the critical question would be who determines what a sufficient amount of damage is to constitute a prohibitive use of force. Each nation, having different strengths and capabilities in the cyber realm, would draw different conclusions.

Another framework is to consider the "kinetic equivalency"[11] of a cyber action, where an action in cyberspace only constitutes the use of force if the damage caused by the action could also have been caused by kinetic attack.[12] Overloading an electric grid or shutting down an energy pipeline with a cyber action can now be considered a use of force because those effects could also have been accomplished with a missile or bomb. While this test stays more true to the instruments-based view of prohibited coercion, it really does not address all actions in the cyber realm, such as painting false targets in an opponent's radar. No damage was done so there is no kinetic equivalency. Those areas still remain gray.[13]

Duncan Hollis also considers a "target-based" framework, where any attack, cyber or kinetic, on a nation's critical infrastructure should be construed as a prohibited use of force.[14] However, this framework suffers from the same limitations as the quantum-of-damage framework in that each nation will define what is considered critical infrastructure based on the strategic interests of the nation. A cyber attack on gold mining production in the United States may be treated as a routine crime, but South Africa may consider its gold mining infrastructure critical to its national interests and would construe such an attack as a prohibited use of force.

The Schmitt Analytical Framework

One framework that stays true to the instruments-based method of determining what force is prohibited, yet provides an effective metric for determining whether a cyber action constitutes a use of force, is that presented by Professor Michael Schmitt of the Naval War College. After an interview, Andrew Folz noted that Professor Schmitt's framework had bridged the gap between an instruments view of force and effects in cyberspace:

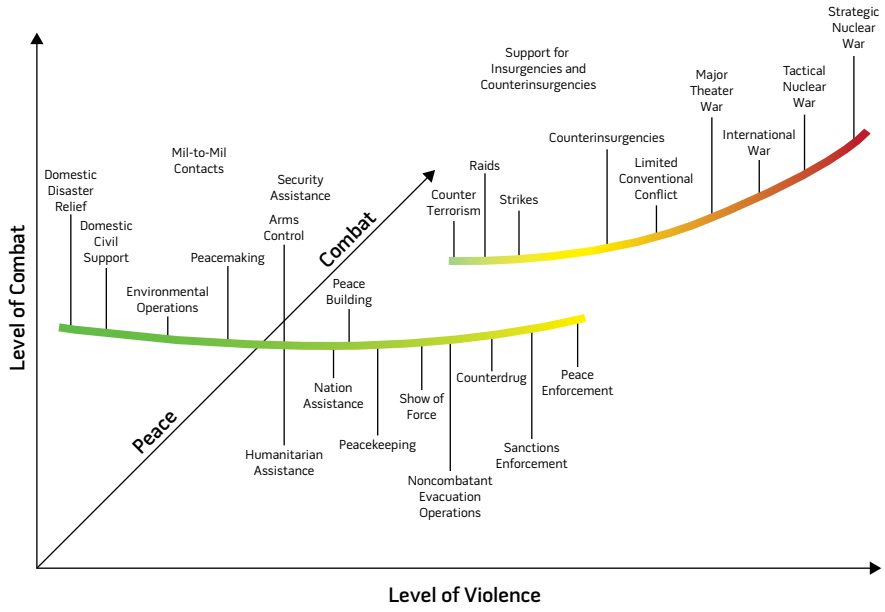
Professor Schmitt recognized that discerning the use-of-force threshold is really about predicting how states will characterize and respond to cyber incidents in light of prevailing international norms. To aid in such predictions, his framework bridges the instrument and consequence-based approaches. In keeping with the Article 2(4) instrument based standard, his model consists of seven factors that represent the major distinctions between permissible (that is, economic and political) and impermissible (armed) instruments of coercion.[15]

Schmitt's framework takes the view that the more closely an action in cyberspace approximates economic or political coercion, the less likely it will be viewed by a nation as an armed attack. Conversely, the more likely an action in cyberspace approximates armed force, the more likely it will be perceived as an armed attack, and hence an illegitimate use of force.[16] Schmitt's seven factors seek to differentiate between what makes armed force inappropriate and what makes economic and political coercion appropriate. Consider, for example, the differences in characteristics of an oil embargo and a blockade.

Schmitt's seven factors are as follows:

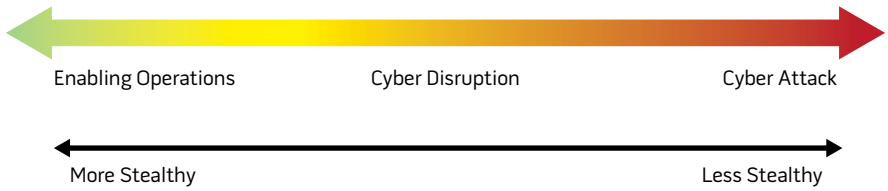
- Severity: Armed attacks threaten physical injury or destruction of property, while economic and political coercion do not. Cyber operations that threaten physical harm are more likely to be viewed as a use of force. This includes such characteristics as scope of the action, duration, and intensity.
- Immediacy: The damage due to an armed attack usually occurs immediately, while damage due to other forms of coercion develops more slowly. This gives the target nation time to respond to the pressure before damage can takes place. Cyber actions whose consequences are immediate, leaving no time for a target nation to respond to pressure or mitigate the consequences, are more likely to be viewed as a use of force.
- Directness: Armed attacks can be linked directly to the damage they cause, and other forms of coercion less so. The more directly a cyber action can be linked to its consequences, the more likely the action will be viewed as a use of force.
- Invasiveness: In an armed attack, the action usually crosses into a target nation's territory; other forms of coercion generally stay beyond the target's borders. So even though armed attacks and economic/political acts may have roughly similar consequences, the armed actions usually are, in the words of Schmitt, "a greater intrusion on the rights of the target state and, therefore, [are]

Figure 1. Spectrum of Conflict



Note: Figure adapted from *Army Vision 2010* (Washington, DC: Headquarters Department of the Army, n.d.), 5, available at <https://rdl.train.army.mil/catalog-ws/view/100.ATSC/CE5F5937-49EC-44EF-83F3-FC25CB0CB942-1274110898250/aledc_ref/army_vision_2010.pdf>.

Figure 2. Spectrum of Cyber Conflict



Source: Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operations," *Small Wars Journal*, December 11, 2012, available at <http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations>.

Table 1. Potential Actions in Cyberspace

Ping map	Change or delete data
Probe	Distributed denial-of-service attack (DDoS)
Implant malware	Email bomb
Erase logs	Influence operations in social media
Email fishing	Disable critical infrastructure
Access networks	Damage critical infrastructure
Access email	Attack financial industry
Steal data	Attack military command and control (C2)

more likely to disrupt international stability." The more a cyber operation violates or impairs the territorial integrity or sovereignty of a state, the more likely it will be viewed as a use of force.

- Measurability: While the consequences of armed attack are usually easy to determine, the actual negative consequences of other forms of coercion are harder to measure. States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable.
- Presumptive legitimacy: In almost every nation, violence is an inappropriate response unless done in self-defense. However, all other forms of coercion are considered lawful unless specifically prohibited by law or treaty. Even actions prohibited by national law, such as espionage, are still considered a legitimate international practice to a certain extent. Cyber actions such as espionage, influence operations, psychological operations, and propaganda, which are legitimately accepted between states, are generally not considered a prohibited use of force.
- Responsibility: The more closely a cyber operation can be tied to a state, the more likely it will be viewed as a use of force.

These factors are not an exhaustive list; they are a starting point for further analysis. Nor should they be treated as anything but a holistic approach to characterizing the use of force in cyberspace. Using the Schmitt framework helps set a metric from which to start characterizing potentially hostile actions in cyberspace.

Spectrums of Physical and Cyber Conflict

Armed conflict is not a bi-stable; it does not exist in a state where a potential adversary's action is either a use of force or it is not. In reality, conflict occurs across a spectrum where it is not always clear if an action should be considered hostile or just plain resistant. Figure 1 illustrates this complexity. In the figure,

Table 2. Example of Completed Schmitt Analysis

Cyber action	Severity	Immediacy	Directness	Invasiveness	Measurability	Presumptive Legitimacy	Responsibility
Ping map	1	1	5	7	7	1	3
Probe	2	1	5	7	7	2	3
Implant malware	3	4	5	7	7	3	3
Erase logs	5	5	5	8	7	6	4
Email fishing	4	4	5	5	5	5	5
Access networks	4	5	6	8	5	6	5
Access email	4	5	6	8	5	6	5
Steal data	6	6	6	9	8	6	6
Change or delete data	7	6	6	9	8	8	6
Distributed denial-of-service attack (DDoS)	7	7	7	9	8	8	7
Email bomb	7	5	6	7	7	6	5
Influence operations in social media	6	7	6	6	7	5	7
Disable critical infrastructure	9	8	8	9	8	8	8
Damage critical infrastructure	9	9	8	9	8	8	8
Attack financial industry	8	9	8	9	8	8	8
Military command and control attack	9	9	9	9	9	9	9

there are two shapes: one to the left that represents the spectrum of peace, the other to the right that represents the spectrum of combat. Both use the same sliding scale with level of effort on the left and level of violence across the bottom. Note the overlap near the center. Actions that occur in that overlap region may have different connotations depending on the strategic situation. Does the commander, for instance, desire de-escalation to maintain the peace, or escalation to maintain pressure in accordance with a UN Security Council directive? Any determination of hostile intent in cyberspace must include an understanding of the strategic situation, especially as it pertains to the spectrum of conflict.

Gary Brown and Owen Tullos suggest a spectrum for cyber activity that is based on the *effects* of actions in cyberspace (see figure 2).[17] They postulate that cyber actions fall into three basic categories: enabling actions, which have little impact on the operations of a nation's information infrastructure but can set the stage for future operations and attacks; cyber disruptions, which may interrupt the flow of information or disrupt the operation of information systems but not cause physical damage or injury; and cyber attack, which may cause physical damage to property or injury to people. Enabling operations tend to be stealthy, and cyber attacks tend to be easily attributable, at least to the point of origin if not the nation responsible.

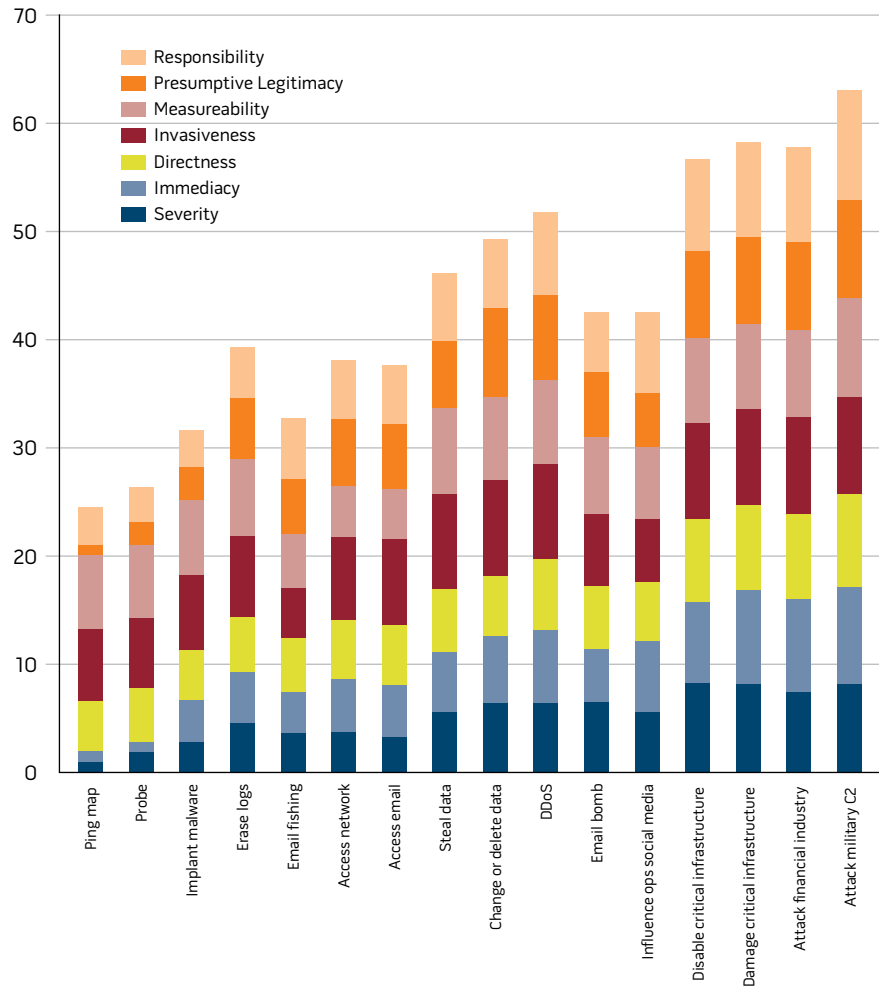
The Brown and Tullos spectrum is meant to be used in concert with Schmitt's framework. Schmitt's framework provides a detailed metric that is excellent for operational-/strategic-level forensic analysis of an attack but may be too complex for use at the tactical level. Brown and Tullos completely abandon the instruments-based metric for determining if use of force is warranted, but the spectrum is helpful, especially when combined with the overall strategic picture, in establishing what immediate actions are appropriate when a cyber action is detected. Taken together—Schmitt for the strategic analysis and understanding the operational landscape, and Brown and Tullos for deploying appropriate countermeasures—we create a solid framework for determining hostile intent in cyberspace.

Determining Hostile Intent in Cyberspace

Establishing that framework starts with understanding the strategic situation. Where is the Nation or joint force operating with regard to the spectrum of conflict (figure 2)? How do partner nations and potential adversaries view the strategic situation? Understanding this landscape helps establish priorities and appropriately weighs factors during the Schmitt analysis.

Conducting the Schmitt Analysis. The analysis begins with a list of potential actions in cyberspace (see table 1). This list of actions is not meant to be specific or exhaustive but strategic and general, similar in manner to how the Standing Rules of Engagement issued by the Chairman of the Joint Chiefs of Staff start out as strategic and general but are modified with more specificity by commanders closer to the conflict. The list should generally and broadly cover the body of

Figure 3. Example of Schmitt Analysis Stack



actions that may occur in cyberspace that have impacts in the theater or area of operations.

Schmitt did not intend for his model to be a quantitative tool but rather to be used as a heuristic. Keeping that in mind, an analyst would use the seven factors to perform a *qualitative* analysis of each action on the list; each action would be evaluated for each Schmitt factor on how close the effects of that action would be to the kinetic effects of an armed attack. For simplicity's sake, analysis would use a scale of 1 to 10—where a 1 means that characteristic is far away from a kinetic effect and a 10 is exactly like a kinetic effect. Once each action is evaluated for each factor (see table 2), the results could then be stacked to give a reasonable comparison of which cyber action is more hostile compared to another.

Determining Response with the Brown-Tullos Spectrum. The Schmitt Analysis Stack (figure 3) gives a good indication of what a commander can consider a hostile act in cyberspace. Figure 4 takes the stack of actions, from least hostile to most hostile, and lays them on the Brown-Tullos Cyber Action Response Spectrum. Using the three general categories in Brown-Tullos (enabling operations, cyber disruption, cyber attack), a commander can develop general responses appropriate to the level of hostility indicated by the action. More importantly, the commander can add or subtract responses, or even move responses up and down the spectrum based on the strategic environment in the theater. For instance, an adversary's access to an unclassified network may be considered enabling operations in a theater at peace, so the response may be to simply monitor and report the covert access. As tensions rise in the area of responsibility, the response may be adjusted to block and report, or even to conduct a counter cyber action against the adversary.

When used in conjunction with one another, the Schmitt Analysis and Brown-Tullos Cyber Action Response Spectrum provide a commander with a flexible tool to determine an appropriate range of responses to a range of cyber actions. Additionally, both can be useful in coordinating cyber responses from different agencies with differing legal authorities. Figure 5 gives an example of how such authorities may be specified. Note that this matrix shows responsibility for action. The Defense Information Systems Agency or the National Security Agency may respond to a ping map or probe on a Department of Defense (DOD) network, but has no legal authority to pursue the perpetrator who resides in the United States; law enforcement would be responsible for that action, and DOD entities would have to coordinate with law enforcement to take action.

Conclusion

Use of force is not simply in the eye of the beholder; there is a rugged, tested framework that is reflected in the United Nations Charter that governs what is acceptable coercion and what is prohibited use of force. Staying as close to that framework as possible when determining hostile intent in cyberspace means we stay close to the use-of-force lessons and applications of the past six decades. An evolutionary development of the legal basis is more appropriate than a revolutionary development.

Some issues of concern remain: even though it is useful for evaluating the strategic/operational cyber landscape, the Schmitt framework was never meant for real-time battlefield analysis. The analytical framework presented is meant to give the commander a *feel* for how hostile a cyber action is and help plan appropriate responses ahead of time. The analysis is also not meant to be static but dynamic, based on continuous analysis of the cyber landscape. New tools, techniques,

vulnerabilities, and mitigations must be continuously taken into account with the strategic situation to accurately stack all the factors and give a commander the right situational awareness. Additionally, the Brown-Tullos spectrum starts out as an effects-based spectrum and only takes into account the instruments of force after Schmitt has been applied. Both must be used together, therefore, one for the strategic/operational analysis, the other to communicate immediate actions at the tactical level.

The real test for any method of determining hostile intent is how it works operationally—that is, how easily it can be employed on the battlefield. The cyber battlefield is not physical; it is abstract, but its effects have real consequences in the physical world. The results of tests can be quickly seen and applied, and the method improved in a short period of time. JFQ

Figure 4. Example of Brown-Tullos Cyber Action Response Spectrum

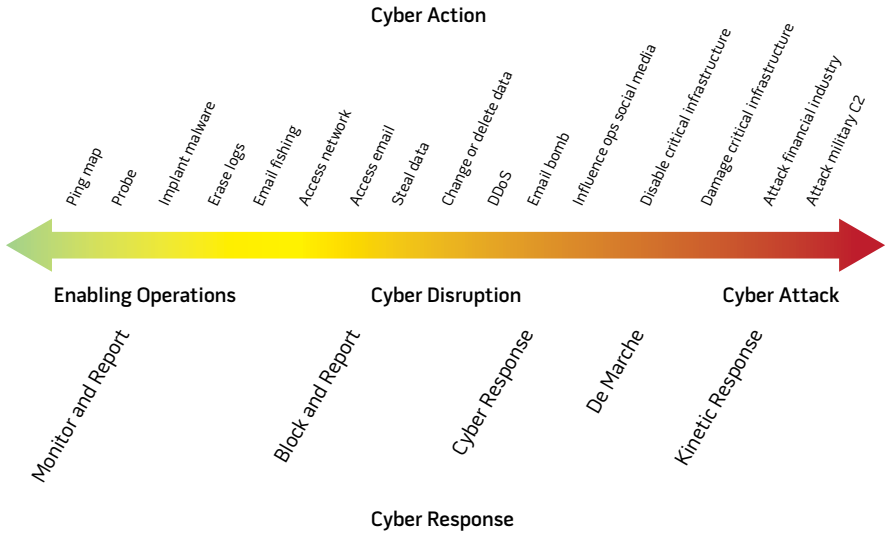
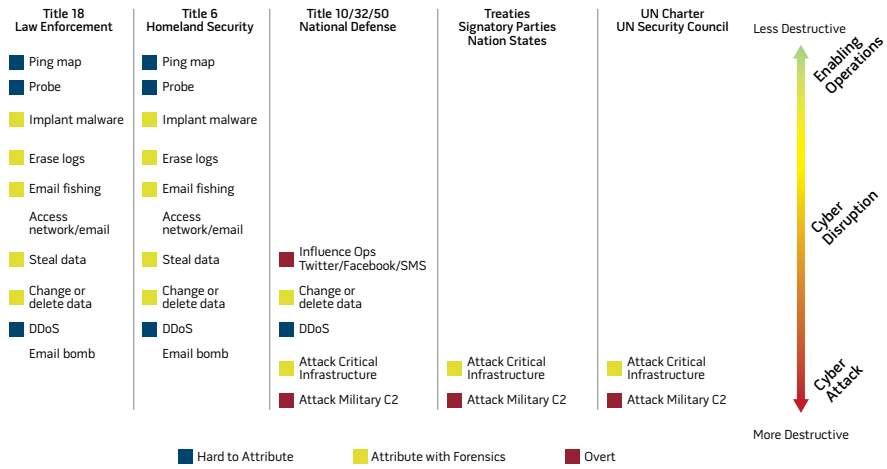


Figure 5. Responsibility for Threats in Cyberspace



Notes

[1] "Splash Two MiGs," *Fly.Historicwings.Com*, January 4, 2013, available at <http://fly.historicwings.com/2013/01/splash-two-migs>.

[2] Chairman of the Joint Chiefs of Staff Instruction 3121.01B, "Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces," Washington, DC, June 13, 2005.

[3] International and Operational Law Department, *Operational Law Handbook* (Charlottesville, VA: U.S. Army Judge Advocate General's Legal Center and School, 2012).

[4] Jude E. Franklin, "CCRTS C2 Plenary Panel," June 30, 2006, available at <www.dodccrp.org/events/2006_CCRTS/html/presentations/1_Panel.pdf>.

[5] Sun Tzu, *The Art of War*, ed. James Clavell, trans. Samuel B. Griffin (New York: Delacorte Press, 1989).

[6] "The Hot Air Balloon," *Century-of-flight.net*, available at <www.century-of-flight.net/new%20site/frames/balloons_frame.htm>.

[7] Andrew C. Folz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate," *Joint Force Quarterly* 67 (4th Quarter 2012), 40–48.

[8] Matthew C. Waxman, "Cyber Attacks and the Use of Force: Back to the Future of Article 2(4)," *The Yale Journal of International Law* 36, no. 42 (2011), 421–459.

[9] Ibid.

[10] Folz, 40–48.

[11] Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis and Clark Law Review* 11, no. 4 (2007), 1023–1061.

[12] Folz, 40–48.

[13] Ibid.

[14] Hollis, 1023–1061.

[15] Folz, 40–48.

[16] Ibid.

[17] Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operations," *Small Wars Journal*, December 11, 2012, available at <http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations>.