SMALL WARS JOURNAL

On the Spectrum of Cyberspace Operations

*By **Gary D. Brown** and **Owen W. Tullos***
Journal Article | *Dec 11 2012 - 4:30am*

As cyberspace operations continue to evolve, they raise some unique questions regarding the nature of conflict and how it should be discussed and regulated. The lack of legal rules governing cyber operations, for example, is commonly lamented by authors and journalists. It makes a good story, but it isn't necessarily true. While lawyers and policymakers wring their hands and fail to make decisions about cyber, practitioners have spent the past decade applying *existing* law and policy to operations and state practice. As evidenced by the actions of the U.S., **Japan**, Iran, China, and **at least 30** other states, countries have been moving to include cyber warfare in their **military planning and organization**.

National practice in the cyber warfare era arguably dates back to 1982 with the **explosion of a Soviet pipeline** said to have been caused by a CIA-planted logic bomb. Even if that spy narrative is merely fanciful musing, **Moonlight Maze and Titan Rain**, unauthorized penetrations of unclassified government computer networks, started the clock a few years later. Thirty years of on-going practice couldn't have occurred in a logical vacuum; some standards of practice have emerged. While the body of law is still developing, these years of cyber activity serve to illuminate much about cyber practice.

When evaluating potential cyber activities, US policymakers have tended to view cyber operations as strictly delineated: offense or defense; espionage or military operations. Reality defies such stark categorization; determining when one type of cyber operation ends and another begins is challenging. Rather than establishing strict categories into which cyber activities are sorted, it may be best to view cyber operations along a spectrum; a proposal for a spectrum of cyber activities is set out later in the paper.

Before discussing the cyber spectrum, let's determine what the term "cyber operation" means. Although there isn't complete agreement within the U.S. government – much less internationally – on a standard meaning, cyberspace operations might be defined as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." This broad definition, similar to one the Vice Chairman of the Joint Chiefs proposed in 2010 that was not widely embraced, encompasses the full array of military and other national cyber operations possible within cyberspace and ranges from gaining access to a computer system through conducting espionage to executing a cyber attack (Joint Terminology for Cyberspace Operations," Vice Chairman of the Joint Chiefs of Staff memo, undated.)

Although only a discrete portion of cyber operations are equivalent to a kinetic attack, the Department of Defense includes in its current definition of "Computer Network Attack" (CNA) nearly every imaginable cyber military activity. DoD's definition of CNA is **"actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."** While this definition might create the appearance that all cyberspace operations are basically the same in the level of damage and scale of effect, that is decidedly not the case.

This codification of what constitutes an attack in cyberspace was DoD's first crack at the problem and, with the exception of the additional phrase "through the use of computer networks", has remained unchanged since its **debut in 1998**. The U.S. military has been struggling to understand the **implications to operations** of this broad definition ever since. With little actual practice available to inform decisions, definitions and other important policy and doctrine choices were made based on analogy and supposition.

So, if DoD proposals regarding cyber doctrine often seem backwards, it's because they *are*. Typically, military doctrine develops as a result of experience gained in military operations. That is, militaries conduct operations, and those parts of strategy and tactics that work best are **preserved as doctrine**. DoD did not even stand up a joint cyber unit until 2005 with Joint Functional Component Command-Network Warfare. It's easy to see why its understanding of cyber operations in 1998, when DoD originally issued its definitions, was incomplete. Further, there is little recent experience in

developing doctrine for new areas. Airpower rose to prominence over 60 years ago, and space has not yet begun to play a significant direct role in military operations, so cyber is the first really new method of warfare to come along in half a century. During this nascent phase, developers of cyber doctrine may wish to emulate the adaptability demonstrated by the United States Air Force during the evolution of airpower.

Throughout its relatively brief history, the Air Force has been notorious for a lack of formal doctrine. One reason the Air Force has tended to eschew doctrine is that, through the latter half of the 20th Century, airpower tactics and techniques were developing and changing so quickly that written doctrine couldn't possibly keep up. Imagine if, in mid-century, formal doctrine froze air operations where they were then – strategic bombing of population centers will win the war! The bomber will always get through! There would have been no impetus to develop stealth technology, precision guided munitions or remotely piloted vehicles.

Similarly, cyber thinking should evolve with the times and not be anchored to stale or outdated doctrine. As some of the fog surrounding cyber operations has cleared, it's now possible to develop a better framework and lexicon for thinking about and discussing cyber. A critical requirement for new policy is that it allow us to differentiate real attacks via cyberspace from lesser actions, because the nature of the action will determine the nature of the appropriate response.

It's important to distinguish between international legal analysis and domestic legal considerations. While cyber operations must satisfy both international and domestic law, the elements of analysis differ. An action may be permissible under international law, but face domestic legal or policy restrictions. Although domestic concerns may ultimately control U.S. cyber operations, this article primarily focuses on international legal principles. Understanding the parameters of international law can help shape national policy and inform the development of domestic legislation.

Perhaps the most striking difference between domestic and international law is the way they develop. Rather than resulting from a legislative process, most international law relevant to hostilities is customary, having developed from national activities that have been observed and studied. As new technologies provide new options for military actions, the law continues to distinguish them based on their scope and effect. In this analysis, forceful acts of violence that risk death and destruction are categorized differently than are acts causing mere inconvenience or economic loss. Because cyber operations have mostly been carried out in secret and not publicly acknowledged, cyber has had little effect on international law development. Only in the (so far) rare instances when the *effects* of a cyber operation are observed does cyber contribute to the customary law conversation. For this reason, it's the effects of cyber operations that must control the analysis under international law.

The other possible way to characterize cyber operations is by intent, but this is ultimately an unsatisfactory solution. Sorting operations by intent would require the nation on the receiving end of the action to have enough accurate information to discern the "why" behind an adversary's action in a timely fashion. In cyberspace, where many actions from multiple origins may occur within milliseconds, this is simply not a workable standard. One illustration of just how fast things happen in cyberspace is that it takes an Internet packet around one-fifth of a second to **travel around the globe**. If the effects of a cyber action make it look like an attack, the victim may well deem it an attack, even if the actor's intent was to engage in espionage. Once again, it's the effects of cyber operations that must drive evaluation of it under international law.

Finally, it's important to note that the spectrum detailed below doesn't distinguish between possible actors who might undertake cyber operations. A state's reaction to a hostile cyber event could depend partly on whether the event was the result of criminal behavior, nonstate actors, government sanction activity, etc. This is an interesting question, but it's beyond the scope of this paper.

The Spectrum of Cyber Operations

Potential cyber operations range from virtually undetectable to merely annoying to destructive. Operations may be designed to gain access to a system for a variety of motivations, which could be to facilitate future criminal, espionage or military activities. These access operations can go **unnoticed for months** or may never be noticed. Operations can go much further, as well, adversely affecting the functionality of a computer system or even destroying a system or component. These disruptive or destructive operations tend to be noticed, of course, although the source of the problem may not always be apparent.

So, cyber operations can be divided into these broad categories: access, disruption and attack. While it is possible to describe actions that fit neatly in each category, many operations fall somewhere between the labels, in the margins between these general categories. This makes the use of a spectrum, rather than a listing, particularly useful.

As noted earlier, cyber espionage is sometimes treated as a separate category distinguished by the intent of an operation. In the U.S., such separate treatment may be partly grounded in the domestic covert action statute, which creates special requirements for activities defined as covert. US law defines covert activities as **"activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."** International law provides no such distinction between classes of activity based on intent. Instead, **effects** generally determine how actions are characterized and consequently where an action falls on the suggested spectrum.

The easiest activities to characterize are those near either end of the spectrum. The simpler green and red areas are discussed here first, with the middle – and most vexing – issues addressed last.

Access Operations

Access operations enable other cyber activities by providing entry to an adversary computer system. Whether the ultimate operation will be intelligence collection, disruption or attack, the actor must have some access into the system before undertaking a cyber activity. Cyber operators may gain access by installing software programs, defeating security measures, injecting malicious code or other exploitation of a system's vulnerabilities. To maintain an access, additional actions are typically required to account for changes in software applications, security measures or hardware updates. Access operations include actions to maintain an access previously gained as well as activities that could be characterized as reconnaissance. The act of gaining or maintaining access, by itself, does not generally affect the system's function or the flow of information.

Access operations will generally fall near the left end of the spectrum, but analysis may move them more to the right as the effects they have on the victim system become more pronounced. For example, port scanning and network mapping fall on the extreme left. Access operations that modify log files and registry entries to conceal access register farther to the right, but still fall short of being disruption operations because they have limited effects. Even in the case of more intrusive access operations, interference with the victim system is temporary and limited. For example, the operation may force a system to reboot or modify electronic log files to prevent system administrators from discovering who gained access to the system. The limited effects of access operations don't typically rise to the level of a disruption operation because they do not deprive the user access to information or prevent normal functioning of the system.

In 2008, unknown actors used a flash drive virus to penetrate a classified DoD network. In what came to be known as **Operation Buckshot Yankee**, adversaries loaded malicious code on portable flash drives. When inserted into a universal serial bus (USB) port on a desktop computer connected to the Internet, the malware loaded itself onto the host hard drive and beaconed back to its originator. When unsuspecting users inserted the infected flash drives to transfer data between secure and non-secure systems, the access gained enabled follow-on activities on both systems. Operations like this can be designed to facilitate espionage or the destruction of a system, or anything in between. For this reason, it's clearest to analyze the process of gaining access separately from the ultimate operation.

Another instance of an access operation disclosed publicly is Operation Aurora. Aurora gained and maintained access into Google's network for many months. **Access into Google's systems** opened a portal to a treasure trove of information at companies that were doing business with Google. Public reporting indicated the accesses were used only for industrial espionage, which Google said originated in China. We have little detail on that espionage, or anything else that might have been done after the access was acquired, so our analysis here is limited to the access operation itself. Regardless of the goal of any access operation, it may be analyzed distinctly from whatever other cyber operation follows. However damaging Aurora might have been in leading to a loss of confidence in Google's systems, it apparently did not interrupt the flow of information on host systems, and so it registers near the left end of the cyber spectrum.

The 2009 **GhostNet** investigation discovered unauthorized accesses into the government systems of more than 100 countries. A **command system** traced to its origin in China could turn on an infected computer's microphone and video

recording systems in order to capture new information, or could be used merely to exfiltrate data from the computer system, depending on the controller's desire.

As illustrated through the above examples, various methods are available to gain and maintain access to systems. GhostNet used spear phishing to infect machines. Spear phishing is highly targeted email or other messages that appear official enough that they may deceive many people into believing they are legitimate. Spear phishing may appear to originate from someone with whom the recipient corresponds regularly; replying with sensitive information or clicking on a proffered link allows the sender access into a victim's computer to steal information, download malware, or otherwise control the victim's system (Harry Newton, *Newton's Telecom Dictionary, 23d Ed.* New York: Flatiron Publishing, 2007). Buckshot Yankee, on the other hand, installed malware from a flash drive.

It's not just the method of infection that differs from malware to malware. All malware takes up some hard drive space or uses system memory. Generally, it's only a small percentage of a system's capacity, but if enough malicious code targeted a system, it could use enough system resources to affect the operation of the computer. Some malware requires the host machine to restart in order to be fully installed, just as many legitimate programs do. For this reason, part of the malicious code might be a command to force the host machine to reboot. Arguably, the forced reboot of the host machine to enable access begins the transition from mere access to cyber disruption, because rebooting "disrupts" the function of the computer for a brief period. It's difficult to define exactly where the change occurs, because operations differ from each other in subtle ways. At some point, however, the negative effect on a system becomes so great that the nature of an operation changes from a mere access operation to a disruptive or aggressive one. It's the difficulty in defining this point precisely that makes a spectrum the most useful way to discuss harmful activities that can occur in cyberspace.

Cyber Attack

C*yber attack* falls on the right of the spectrum and moves farther to the right depending on the severity of the attack. In contrast to the way the term "computer network attack" is used by DoD, "cyber attack" as used here means cyber activity that has effects in the real world beyond the cyber system itself. Mere degradation or denial of a system, for example, are not cyber attacks. The definition of cyber attack used here is *actions in cyberspace whose foreseeable results include damage or destruction of property, or death or injury to persons*.

To date, the best real-world example of a cyber attack is **Stuxnet**, an operation reportedly carried out by Israel and the US to **slow Iran's development of nuclear weapons**. Reports of Stuxnet estimate 1,000 Iranian centrifuges were damaged beyond repair when stealthy malware caused machines to spin at certain high and low ranges. The result of the Stuxnet activity – destruction of equipment – would make it a **cyber attack** under the cyber spectrum proposed here. Stuxnet falls in the red category, and illustrates how physical destruction may occur via cyberspace and constitute a use of force – an attack equivalent to one conducted using traditional means of warfare.

A **tragic accident** that occurred in Russia in 2009 provides a hypothetical example of what a cyber attack at the far right end of the spectrum could look like. A damaged turbine at the Sayano-Shushenskaya hydroelectric power plant had been shut down for maintenance. A computer operator at a control facility, located far from the dam, seeking to correct for a loss in available power, brought the damaged turbine back on line. The operator's electronically delivered command for increased activity caused the damaged turbine to spin out of control, killing 75 people and causing over $1 billion damage. While the official investigation of the dam failure blamed poor management and technical flaws, this tragedy demonstrates how wrongdoers might theoretically take control of a computer system and cause horrific damage by manipulating it.

Had the event at Sayano-Shushenskaya been caused by malicious cyber actors, it would have crossed the line to attack. Like Stuxnet, it would have served as an example of the kind of physical effects that define a genuine attack. Aligning the meaning of "attack" in the cyber context with the way the term is used in other domains allows for a more precise analysis of cyber activities under international law. Specifically, it would leave the operating space in the middle of the spectrum, the disruptive activities, to be analyzed separately.

Cyber Disruption

Most actions DoD would currently define as computer network attack fall into the category of "cyber disruption" on the spectrum. Cyber disruption includes actions that *interrupt the flow of information or the function of information systems without causing physical damage or injury*. The greater the effect, the farther it moves along the spectrum, from green to red. It's important to note, however, that merely because a cyber action is a disruption rather than an attack doesn't mean it is permissible or lawful. Sub-attack actions may still run afoul of other laws or standards, such as specific international agreements.

In general, however, there seems to be little in the international regime to prohibit cyber disruption activities. International law is a permissive regime; actions are not unlawful unless they violate a specific prohibition. The clearest standard for cyber actions that don't constitute a cyber attack, or "use of force" in international law is the non-intervention principle – and it isn't all that specific. The non-intervention principle prohibits coercive or dictatorial actions that deprive a nation of the ability to control governmental matters such as economic, political, military or cultural activities (Robert Jennings & Arthur Watts (ed.), *Oppenheim's International Law*, Vol. 1, 9th ed. 1992). Actions that don't cross this threshold may be considered generally permissible under international law.

Applying the considerations set out above, some cyber disruptions would constitute wrongful interventions, but others wouldn't. Examples of cyber disruptions that would violate the non-intervention principle include disturbing the ability of a government to communicate with its population, as occurred in Estonia (2007) and Georgia (2008) – both are discussed below – or advocating for the overthrow of a government by hacking an official electronic messaging system, for example. Other cyber disruptions that don't interfere with a nation's ability freely to decide on sovereign matters may raise policy considerations, but don't cross the threshold of illegality. If an operation is not a use of force and doesn't violate the intervention restriction, then it is generally permissible under customary international law.

The following factors may be useful to consider when determining whether a cyber disruption violates the non-intervention principle:

1. Does the activity directly affect government activities? For example, is it interfering with a government web site or government-owned computer system?

2. How subtle and discrete is the activity? Is the national government or a significant portion of the population likely to be aware of it? For example, does the activity noticeably alter the functionality of a website or computer system with a high number of users?

3. Has the nation specifically acted in the subject area being adversely affected? For example, has the government publicly indicated support for the affected group, position or information?

4. Is the activity likely to affect the nation's economy adversely in a measurable way? For example, will it prevent access to a significant number of commercial web sites?

The answers to these four question can help determine whether a cyber activity violates the non-intervention principle, or is simply an unneighborly action that disrupts cyber activities in a way that doesn't run afoul of any existing international law.

Operation Cupcake (2010) is one of the few government cyber actions that has been reported, and it serves as an example of cyber disruption that doesn't constitute an unlawful intervention. When the terrorist organization Al Qaeda in the Arabian Peninsula (AQAP) released *Inspire* magazine online, the British government replaced the bomb-making instructions in the online publication with cupcake recipes; the substitution lasted a few days. Analyzing the UK's action against this terrorist organization reveals no international law violation. The posting of cupcake recipes was not a threat or use of force, nor did the action interfere with any nation's political, military or economic governance. In fact, as no nation claimed responsibility for the content of the newsletter, the only sovereign claim at stake would be that of the nation hosting the server and other infrastructure that allowed the newsletter to exist on the Internet. A quick review of the four questions set out above makes it clear that, wherever the content was hosted, no sovereign claim was at stake.

While the action undertaken in Operation Cupcake clearly disrupted AQAP's flow of information, the UK's actions did not violate international law. On the spectrum, Operation Cupcake would fall in the transition area from green to yellow; the action rose above mere access into disruption, but fell far short of an intervention or cyber attack.

The Operation Aurora events, discussed above, didn't meet the definition of cyber attack because no physical damage or injury occurred. The disruption activities persisted over a long period of time and may have caused significant economic loss, so it was more serious than Operation Cupcake, whose effects endured only briefly. However, Aurora's impact was on private companies, and did not interfere with any government's ability to govern political, economic or military activities, so the actions didn't violate the non-intervention principle.

Another disruption event occurred on July 4, 2009, when cyber operations were conducted against the United States and South Korea. Those **Independence Day actions** attempted to jam traffic on over two dozen government and commercial systems, including financial networks. The effects lasted only few hours to a few days, and standard cyber security means could readily counter many of them. The scope and effects of the operation were minimal, but it's not difficult to imagine an operation targeting government networks or a nation's stock exchange that would constitute a wrongful intervention.

The well-known cyber incidents in Estonia and Georgia merit individual discussion. During 2007 in **Estonia**, cyber actions shut down the Government's ability to communicate and froze the financial sector for about a month. The motivation for the actions was the Estonian government's decision to move a memorial statue of a Soviet soldier in Tallinn to a less prominent location in the city. The activities were coercive in that they were imposed against Estonia's will and the Government was not able to stop the effects. Estonia heavily relied on cyberspace for communications and commerce, and experienced significant disruption of its communication and economic systems. The Estonia incident probably violated the non-intervention principle, and therefore merits a position farther to the right on the spectrum.

In 2008, cyber disruption of Georgian web and telecommunications began just as Russia commenced military operations in the **Republic of Georgia**. The disruptive activities prevented many government computer-based activities in the early days of the Russo-Georgian conflict. Georgia's civilian communications, financial systems and media were also degraded by the cyber operations. The unilateral, coercive actions preventing the Georgian government from communicating during a period of national crisis may provide another example of a wrongful intervention, but the significance of these cyber events was lost in the fray of the shooting war that followed.

A lesser-known example of cyber disruption is the **GhostNet** set of activities. GhostNet, discussed earlier, was reportedly based in China, and affected government systems around the world. Here, we focus on its effect on Canadian computer networks. It penetrated systems in Canada's Finance Department and Treasury Board so pervasively that the Government took the systems off-line for nearly a month. As the Canadian action demonstrates, certain access or espionage activities may be so damaging to the system's trustworthiness or reliability, they can effectively render the system useless. This is especially true in the case of systems vital to national security or welfare. When unauthorized people gain deep or persistent access to sensitive information, the situation effectively forces a government to choose between shutting down a system or suffering exposure to unacceptable risk. For example, if the Canadian Government had been unable to carry out essential economic tasks without the Department of Finance's systems, the disruption might have qualified as an unlawful intervention, because the actions could have formed the basis for follow-on coercive demands.

In January 2012, **Israel** observed two denial of service activities, one affecting the Tel Aviv Stock Exchange and the other El Al Airline websites. Israel chose to take the systems off-line for the few hours that the disruption continued. This case illustrates how even relatively low-level cyber activity can force a nation to choose between risking damage to the integrity of a cyber system or taking it off-line. This could be classified as coercion. Shutting down a nation's control of a stock exchange or transportation under some circumstances would potentially cross the threshold of unlawful intervention.

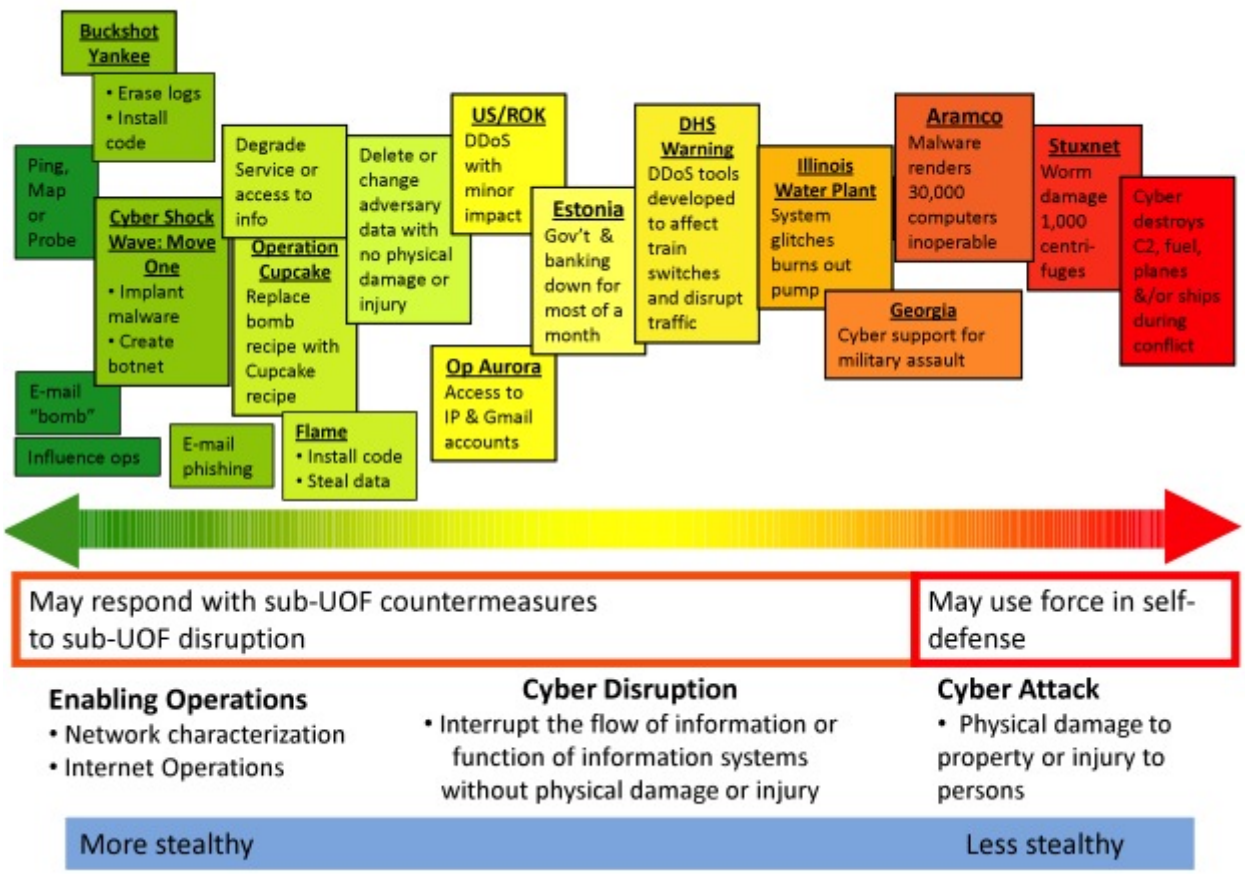
A final example of cyber disruption gets very close to the line of cyber attack, if Secretary of Defense Leon Panetta's **statement** about it is accurate. According to the Secretary, the **Shamoon virus**, named after a word found in the malware code, had a near-destructive effect on thousands of computers used by the Saudi Arabian national oil company, Aramco. Secretary Panetta said Shamoon "replaced crucial systems files with an image of a burning U.S. flag [and] overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless and had to be replaced. It virtually destroyed 30,000 computers." Although at the time of writing, it was unclear exactly what happened to the Aramco computers, other than the Secretary of Defense statement, reports generally indicated it wasn't operating system data that was overwritten, so the computers might still have been operable. The hard drives appear to have been replaced to ensure no malware remained to reinfect Aramco's network. The following discussion, and Figure 2, treat Shamoon as if it were the more serious case, as that makes for a more interesting discussion.

If a major energy supplier has thousands of computers rendered inoperable, it might well be considered a cyber attack. Here, it is labeled a disruption because it appeared to be a software effect, even using Secretary Panetta's assertions, rather than a destruction of hardware. In addition, there was no associated oil spill or other catastrophic physical event, which would change the analysis.

Cyber disruption is factually distinguishable from actions that cause death and destruction. Currently, most reported contentious cyber activity falls below the use of force and fits into the category of disruption. Lumping fundamentally different actions into an over-inclusive category like "computer network attack" as DoD has done created a Gordian Knot that has paralyzed policy and doctrine development. It simply isn't possible to create appropriate rules when the starting point is that all negative cyber activities are treated the same, whether it's shutting down a website or completely destroying a computer system.

This flawed framework helps explain why, 30 years after the dawn of aggressive cyber activity, **Congress**, the **Department of Defense** and the **Department of Homeland Security** are debating over who is responsible for defending the nation in cyber. It may also explain why DoD collocated its cyber "war-fighting" command with the nation's largest intelligence agency. There simply is a high level of confusion among US government policymakers regarding the nature

of cyber aggression and how to deal with it. To the extent the cyber spectrum can help demystify cyber operations, it has served its purpose.



Beyond helping the US sort out its policy confusion, distinguishing disruption from attack offers an additional benefit: it matches a proportionate potential remedy with the offending action. When faced with a use of force or armed attack, a necessary and proportionate response in self-defense may include a use of force or attack using cyber techniques or more traditional means. However, when faced with cyber disruption that causes no physical damage or injury, the proportionate response is more properly limited to sub-use of force actions.

Conclusion

Now that many nations and non-state actors possess the technical capability to cause disruption, destruction, and even harm people through cyberspace, it's time to more carefully explain the place of such cyber actions in international relations and law. Clarity in defining how victims will and should view cyber actions is essential to avoid tragic miscalculation that could lead to overreaction or an unnecessary and dangerous escalation of international tensions. It is incumbent on the U.S., as the most important player on the international cyber stage, to lead the drive to a workable conceptual model. DoD can do its part by espousing definitive doctrine that treats cyber attacks the same as attacks through air, land, sea and space, while carving out cyber activities that are merely disruptive, so that a rational set of rules can be crafted to govern these actions.

The spectrum of cyber operations proposed here is meant to aid operators and policymakers as they analyze cyber operations. Not all cyber operations are created equal, and the law and policy should reflect that. A spectrum may not provide all the answers, but it does offer a more coherent framework around which US government cyber professionals can organize their thinking.

Rating:

Your rating: None

About the Authors

Gary D. Brown

Colonel Gary D. Brown, USAF, has been the Staff Judge Advocate at U.S. Cyber Command since its inception in May 2010. He holds a J.D. and an LL.M. in International Law, and is a Nebraska attorney.

Owen W. Tullos

Lieutenant Colonel Owen W. Tullos, USAF, was the Deputy Staff Judge Advocate for Operations Law at U.S. Cyber Command, Ft. Meade, Maryland until July 2012. He holds a J.D. and an LL.M. with a dual specialty in International Law and Operations Law. He is a member of the South Dakota bar.

Available online at : http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations

Links:
{1} http://smallwarsjournal.com/author/gary-d-brown-0
{2} http://smallwarsjournal.com/author/owen-w-tullos
{3} http://news.discovery.com/tech/japan-vigilante-virus-120104.html
{4} http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf
{5} http://www.hsgac.senate.gov/download/?id=5252c88e-05ce-447a-8f8e-f785dfac7cc2
{6} http://www.economist.com/node/16478792?story_id=16478792&fsrc=rss
{7} http://www.fas.org/sgp/crs/natsec/RL31787.pdf
{8} http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf
{9} http://www.c4i.org/jp3_13.pdf
{10} http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html
{11} http://www.au.af.mil/au/awc/awcgate/readings/drew1.htm
{12} http://www.internettrafficreport.com/
{13} http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
{14} http://www.gpo.gov/fdsys/pkg/USCODE-1994-title50/pdf/USCODE-1994-title50-chap15-subchapIII-sec413b.pdf
{15} http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/
{16} http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
{17} http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html
{18} http://www.nytimes.com/2009/03/29/technology/29spy.html
{19} http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html
{20} http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all
{21} http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?ref=stuxnet
{22} http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html
{23} http://www.popularmechanics.com/technology/engineering/gonzo/4344681
{24} http://abcnews.go.com/US/operation-cupcake-mojito-varietyfoils-al-qaeda/story?id=13761903
{25} http://www.nytimes.com/2009/07/09/technology/09cyber.html
{26} http://www.ccdcoe.org/publications/books/legalconsiderations.pdf
{27} http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf
{28} http://www.theregister.co.uk/2011/02/17/canada_cyber_espionage/
{29} http://www.nytimes.com/2012/01/17/world/middleeast/cyber-attacks-temporarily-cripple-2-israeli-web-sites.html?_r=0
{30} http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5136
{31} http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?ref=nicoleperlroth&_r=0
{32} http://www.wired.com/threatlevel/2012/02/cybersecurity-act-of-2012/
{33} http://www.dhs.gov/news/2012/09/19/written-testimony-secretary-napolitano-senate-committee-homeland-security-and
{34} http://smallwarsjournal.com/jrnl/art/why-your-intuition-about-cyber-warfare-is-probably-wrong