A Review of Frequently Used Cyber Analogies

Kandice McKee, NSCI
July 22, 2011

Introduction

Analogies are useful insofar as they help to explain a new or difficult subject. When it comes to cyberspace, something that is quite abstract and yet very real, there are numerous analogies that assist in describing what type of environment cyberspace is and its complicated security situation.

The current cybersecurity crisis can be described several ways with numerous metaphors. Many compare the current crisis with the lawlessness to that of the Wild West and the out-dated tactics and race to security with the Cold War. When treated as a distressed ecosystem, the work of both national and international agencies to eradicate many infectious diseases serves as a model as how poor health can be corrected with proper resources and execution. Before these issues are discussed, what cyberspace actually is must be identified.

According the U.S. Department of Defense, cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] Other global domains that cyberspace is often compared to include the seas, airspace and outer space.

As expressed by Shawn Brimley in the *Washington Quarterly*, the addition of cyberspace to the list of global commons "…helps to communicate to key U.S. international allies and partners that the United States views peace and security within these domains as a common global good – something that all nations can benefit from equally."[2] Adding cyberspace to the short list of global domains could also potentially help create the much-needed decisions in the relatively new and incredibly invasive realm.

The Global Domains

The seas

Out of all the global commons, the seas were the first to be explored, battled on and used for commerce. Unlike cyberspace, the seas are tangible and naturally exist. And while powerful countries have been attempting to regulate the seas for centuries, the cyberspace world has existed for just a few decades.

When it comes to the "ownership" of these waters, much of the seas are considered to fall into the global domain, just as cyberspace. What doesn't fall into the global domain includes territorial waters, which is commonly 12 nautical miles off a coast, as well as the contiguous zone and the resources found within a 200-mile extension into the seas.

These modern definitions and "rules," along with several others, are found within numerous agreements – the 1958 Geneva Convention on the High Seas, the Geneva Convention on the Continental Shelf, and the United Nations Convention on the Law of the Sea Convention, which was signed in 1982 but went unratified by many until 1994. The League of Nations attempted to pass the first treaty in 1930 regarding the laws of the seas, though it failed and the seas went unlegislated until the Geneva Convention in 1958.

According to an article presented at the 2010 Conference on Cyber Conflict Law and Policy, the similarities between the seas and cyberspace are summarized into just a few sentences:

> "Both are expansive domains in which humans can operate using specially designed and developed technologies. Neither is wholly contained within the sovereign territory of a single nation or small group of nations, and many nations profit from more or less

1 Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 17 October 2008, p. 141, available at http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(10-08).pdf
2 "Promoting Security in Global Commons," Shawn Brimley, The Washington Quarterly Vol. 33, Number 3, p. 4, available at http://www.twq.com/10july/docs/10jul_Brimley.pdf (herein after Brimley)

> simultaneous access to and free transit across these domains. Both require human investment of scarce resources to realize their potential, and both share analogous risks from property appropriation to criminal activity to warfare."

The same authors also summarize the differences between the two entities in another few sentences:

> "On the other hand, cyberspace, unlike the ocean, is mostly manmade, and requires near-continuous human attention and support to remain functional. The seas have more-or-less well-defined boundaries related to topographically defined jurisdictions in physical space, while cyberspace has only weak connectivity to physical space. And the technologies for using and exploiting cyberspace are evolving more rapidly today than those we use to take advantage of the oceans and the treasures beneath them."[3]

While the capability for warfare in both domains is mentioned as a likeness between the seas and cyberspace, the authors neglect to list among the contrasts of the two environments the near anonymity that is often used in cyberspace by both state and non-state actors in both warfare and common circumstances, while on the seas, and in other global domains, it is nearly impossible to hide one's identity. The issue of identity is one that the authors of the international sea treaties didn't need to focus on, and, therefore, such treaties will do little to help in the construction of such provisions within international cybersecurity treaties or agreements.

The Airspace

Airspace is another area that is considered a global commons. Like both the seas and cyberspace, there are areas that are under state control while there are other areas that remain uncontrolled by any single authority. Like the seas, airspace is divided into categories. Nation-states have control over Air Defense Identification Zones and Special Use Airspace within their respective territories while international conventions regulate the airspace used for commerce and travel among the general public (airspace zones A through E).[4]

While it took centuries for the international community to develop and ratify sea treaties, the timeframe for controlling airspace was much shorter. The first airplane, built and flown by Orville and Wilbur Wright, took off in 1903. After development and use in the aircraft industry increased, the global community responded. The first convention that addressed the need to regulate airplanes was held in 1910 and a commission was created in 1919. The U.S. played by its own rules and neglected to sign and obey international conventions and provisions until international air traffic grew to be so large that the U.S. was no longer isolated from the air congestion that the European countries had been experiencing. In 1944 – just more than four decades after the first plane took flight – the U.S. and 51 other countries signed the International Civil Aviation Convention, which became effective in 1947. Currently, like much of the seas, a United Nations Agency manages global air traffic control.

To summarize the similarities between cyberspace and airspace, a Cooperative Cyber Defence Centre of Excellence article states:

> "Both the atmosphere and cyberspace are extensive domains within which humans, using appropriate technology, can operate. Both are international in scope and use, with some areas within existing national jurisdictions and some areas outside of any national jurisdiction. Both have traffic flows that need to be controlled to facilitate transiting the domain."

---

3 "Cybersecurity Regulation: Using analogies to develop frameworks for regulation," Julie J.C.H. Ryan, Daniel J. Ryan, Eneken Tikk, International Cyber Security Legal and Policy Proceedings, NATO Cooperative Cyber Defence Centre of Excellence, available at http://www.ccdcoe.org/publications/legalproceedings/Ryan_Ryan_Tikk_Cybersecurity%20Regulation.pdf (hereinafter "Cybersecurity Regulation: Using analogies to develop frameworks for regulation")
4 Ibid.

The article goes on to summarize the differences in the two environments, where they acknowledge the anonymity of cyberspace:

> "While airspace is tightly connected to national jurisdictions and traffic is under the control of a specific jurisdiction when above a national jurisdiction, traffic in cyberspace is much less subject to such controls. Air traffic is tightly monitored and directed by the Air Traffic Control system; packets in cyberspace take unpredictable paths dictated by network routing protocols that can change dynamically in response to loading in ways that are not controlled or controllable by either the user or the nations the traffic paths traverse. Both planes and passengers are identified and tracked when they use airspace, but authentication and attribution of users of cyberspace is often impossible."[5]

In the U.S., the defense of both airspace and much of cyberspace is the Air Force's responsibility. However, as Nancy Brown acknowledged in High Frontier, the two realms, when used in warfare, are very different. "Just as Cyber is a force-multiplier, so too, can it be a problem multiplier. As an example, when we destroy an opponent's anti-aircraft gun, we have limited his ability to fire projectiles at our aircraft. If we destroy an opponent's computer, we have not significantly limited his ability to fire attacks at our network," she wrote.[6]

This doesn't mean the framework that is presented in airspace treaties, regulations, etc cannot be translated over into cyberspace, though. NATO has stated that like airspace traffic, there are different types of cyberspace traffic, and each should be treated differently when regulated. The "national security emergency vehicles and 'cyber tanks'" have been left without internationally cooperative regulation while the "'cargo flights' (business uses of the Internet) and some charter flights (e.g. personal data protection, consumer rights) have been heavily regulated."[7]

The Outer Space

Like both the seas and airspace, outer space naturally exists while cyberspace is in virtual existence. But unlike the seas and airspace, and like cyberspace, outer space is difficult to define, especially by territorial lines. While cyberspace components must physically exist within a territory, the Internet has made the world smaller by allowing cyberspace users quick access to information that may cross over numerous territories; satellites belong to a nation or private entity – not the world, though they orbit over several territories while in space. As Ryan, Ryan and Tikk wrote: "If nations were allowed to exercise sovereign control over the use of outer space in the same way they exercise sovereign control of air traffic in the skies above their territories, it might be practically impossible to explore and use space at all. The same may apply to cyberspace."[8]

Despite the differences in territorial sovereignty between sea, airspace and outer space regulations, the same international organization that "regulates" much of the seas and airspace also oversees a lot of outer space use. In response to the space race of the Cold War, the U.N. adopted in 1963 nine legal principles pertaining to outer space use and exploration. Since then, the U.N. has adopted numerous other resolutions and treaties to enhance the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space – the combination of all outer space regulations is collectively known as the United Nations Treaties and Principles in Outer Space. There have also been "multilateral and bilateral agreements and treaties" signed.[9]

Though outer space would continue to exist without technology and cyberspace wouldn't, our use of outer

5 "Cybersecurity Regulation: Using analogies to develop frameworks for regulation"
6 "Difficulties Encountered as We Evolve the Cyber Landscape for the Military," VADM Nancy E. Brown, High Frontier Vol. 5, Number 3, p. 6, available at http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf (hereinafter Brown)
7 "Cybersecurity Regulation: Using analogies to develop frameworks for regulation"
8 Ibid.
9 Ibid.

space is also dependent on technology. The seas and airspace were being exploited prior to modern technological advances; outer space was merely gazed upon and cyberspace an imaginary place prior to such advances. Thus, there are regulations that currently exist that have considered modern technology.

THE CONNECTIONS BETWEEN GLOBAL DOMAINS

Prior to cyberspace and use of airspace, the seas were the means of international commerce and wars. After centuries of lawlessness on the seas, much of the international community recognized the need for regulations. The fact that an area, which was used in the same way modern cyberspace is, had been left unregulated for so long and has been tamed after international efforts should signal optimism that something can be done with cyberspace.

Like the seas and airspace, there is a range of uses and users of the cyberspace domain. Sea and airspace treaties and agreements have accounted for these differences, and cyberspace agreements must as well. Attacks on civilians in air and sea are forbidden, and when they do occur, they are often considered acts of war. Such "international laws of war" are lined out in several international treaties, all predating the existence of cyberspace. However, Neil Rowe of the Naval Postgraduate School writes that international cyberwar attacks may still be "illegal or unethical" as malicious attacks and can be considered a weapon of mass destruction, if used in such a manner.[10] To modernize the 19th and 20th century international laws of war, provisions must be added, and new treaties must be signed, to accommodate for 21st century weapons.

Because outer space must still be regulated to ensure the safety of its exploration, and such international treaties must do so without considering territorial lines, these provisions could be translated and changed, as needed, to fit the much-needed cyberspace national and international regulation. However, the "differences mean that, while a framework of principles, agreements and treaties may well serve to regulate behavior in cyberspace, they may not be the same principles, agreements and treaties that have evolved to control behavior in outer space."[11]

THE MODERN WILD WEST

Before any of the modern day treaties for any of the global commons had even been imagined, the U.S. wrestled with the lawlessness of the Wild West. The riches of the newly acquired western part of the U.S. put prospective entrepreneurs into a frenzy and new technologies were developed to handle the vast size of the U.S. As written in 1998 by Andrew Morriss: "Today a new gold rush is beginning."[12] By now, the gold rush is here and flourishing. There are some organizations and companies that exist solely because of cyberspace – Ebay, Google, Craigslist, Netflix, etc. Like the old West once was, cyberspace is a relatively new environment with few regulations or laws. "I liken the hackers to the gunslingers and the town to the millions of unprotected computers, and so I ask where is the sheriff? We do need a sheriff," said Dr. John Savage.[13] Dr. Joe St. Sauver from University of Oregon agrees – "Since no one else will accept responsibility for cleaning up and securing infested systems, the time has come for the government to do so," he presented during a 2007 counter e-crime summit.[14]

---

10 "Ethics of cyberwar attacks," Neil C. Rowe, U.S. Naval Postgraduate School, available at http://faculty.nps.edu/ncrowe/attackethics.htm
11 "Cybersecurity Regulation: Using analogies to develop frameworks for regulation"
12 "The Wild West Meets Cyberspace," Andrew P. Morriss, The Freeman Ideas on Liberty, Vol. 48, Issue 7, July 1998, available at http://www.thefreemanonline.org/featured/the-wild-west-meets-cyberspace/
13 "Cyberspace – Taming the Wild West," remarks in Washington D.C., March 23, 2010, available at http://www.state.gov/g/stas/series/154216.htm
14 "We Need a Cyber CDC or a Cyber World Health Organization," Dr. Joe St. Sauver, University of Oregon, available at http://www.uoregon.edu/~joe/ecrime-summit/ (hereinafter Dr. Joe St. Sauver)

While President Barack Obama has created a "cyber czar" position, many, including the National Cyberspace Security Institute, don't believe the position carries enough weight to really act as the "sheriff" Dr. Savage references.

THE COLD WAR TACTIC

Deterrence is only useful when repercussions exist and are known. Such was the case during the Cold War when both sides relied on Mutual Assured Destruction via their robust stockpiles of nuclear weapons. This concept, though, is most often void in potential cyber warfare. As the U.S. remains more developed than many of its adversaries, the U.S. is susceptible to more offensive cyber warfare attacks. "This skews the familiar Cold War concept of 'mutually assured destruction' pretty fundamentally," according to Gary McGraw.[15]

Dr. Martin Libicki outlines another eight difficulties in utilizing deterrence within cyberspace. One of these acknowledges the current difficulty in assigning blame that wasn't present during the Cold War. "For nuclear and massed conventional attacks the source is usually immediately obvious. This is not true in cyberspace," he wrote. Not only is "the source" not immediately known, the attack itself, along with damage, could potentially go undetected for a considerable period of time; it is impossible to counter an attack that remains hidden. If an attack receives no retaliation, the tactic of deterrence is going to fail.[16] While successful during the Cold War, cyberspace deterrence is currently a difficult tactic to both define and use.

THE PUBLIC HEALTH

The U.S. created the Communicable Disease Center in 1946 primarily to combat malaria. With significant growth in mission and objectives over the ensuing years, the center has since gone on to become the modern-day Centers for Disease Control and Prevention. According to its website, "Today, CDC is the nation's premier health promotion, prevention, and preparedness agency and a global leader in public health."[17] During the same time period, in 1948, the UN created its World Health Organization. The WHO has essentially many of the same goals as the CDC but on a global scale.[18]

Many professionals in both the private and public sectors agree that the U.S. needs a "Cyber CDC" and the international community a "World Cyber Health Organization." In a paper published by the Department of Homeland Security, the authors state the government must translate to the cyber world its response to "mass scale acute emergencies" as well as its approach to "correcting chronic health problems." To create such policies, the "cyber public health" entity would need to survey its users. "Public health services conduct population health surveillance and react to threats to the overall health of communities" – the same must be done to promote cyber health.[19] So as to protect users privacy, Dr. St. Sauver recommends that such data be collected and reported "in aggregate only."[20] The DHS paper outlines possible functions of the "cyber equivalent of a CDC" to include: data aggregation, data dissemination, cyber threat analysis, intervention analysis and recommendations, and coordination of preventative actions.[21]

---

15 "Software [In]Security: Cyber War – Hype or Consequences?", Gary McGraw, Informit.com, June 17, 2010, available at http://www.informit.com/articles/article.aspx?p=1597476
16 "Deterrence in Cyberspace," Dr. Martin C. Libicki, High Frontier Vol. 5, Number 3, p. 16-20, available at http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf
17 "Our History," The Centers for Disease Control and Prevention, available at http://cdc.gov/about/history/ourstory.htm
18 "History of WHO," The World Health Organization, available at http://www.who.int/about/history/en/index.html
19 "Enabling Distributed Security in Cyberspace," The Department of Homeland Security, March 23, 2011, available at http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf (hereinafter "Enabling Distributed Security in Cyberspace")
20 Dr. Joe St. Sauver
21 "Enabling Distributed Security in Cyberspace"

While the influenza virus will often pass without long-term consequences, there are vaccines available to limit the number of infections. Some diseases and infections have been nearly eradicated with the help of vaccines and work of the CDC and WHO. While there are treatments available for some illnesses that vaccines can shield against, the purpose of the vaccines are to prevent the illnesses from ever occurring. The same must be done with cyberspace policy – there must be reactive measures in place for when outbreaks occur, but more importantly, there should be proactive, preventative measures in place so that the reactive plans are used less frequently.

Such proactive and preventative measures are comparable to the body's autoimmune system, according to the DHS. Automated Courses of Action "allows the speed of response to approach the speed of attack, rather than relying on human responses to attacks that are occurring at machine speed." Letting systems automatically correct security issues means brainpower can be conserved for larger and more complex issues. Like the body's immune system, "automated defenses could be effective at the earliest, least costly stage of the lifecycle as well as at the later stages of an attack when malicious code and other attack elements propagate at machine speed." Also like a healthy immune system, infected systems could potentially work through attacks by utilizing information that hasn't become infected – in essence, the infected portions of a system could be quarantined until the ACOA has had time to cure the infection.[22]

THE FUTURE FOR CYBERSECURITY

As Brown wrote in High Frontier: "The cyber world is both separate from the domains of sea, air, space, and land, and ubiquitous throughout them. What this means is that cyberspace reaches across services, cultures, nations, and ideologies. While the US is the dominant player in the land domain, unchallenged in the air, and has few near-peers on the oceans, the same is not true in a place where anyone with a computer can make their message heard and a concerted online social group may have a larger following than any elected official."[23]

Deterrence worked during the Cold War; mutually assured destruction was not something any leader or group dared to test. However, MAD doesn't apply to cyberspace – the U.S. doesn't even have national legislation that is written specifically for cybersecurity. While the U.S. has signed and ratified an international treaty pertaining to cybersecurity, it has yet to do what is necessary to become the world leader in cybersecurity.

The U.S. hasn't done enough as a nation to flex its muscles in the cybersecurity realm to deter attackers. The U.S. has assigned much of cyberspace and its implications to the military. In the near term, it is probably a good thing for such an established community to take 'ownership' of cyberspace, but over the long-term, the U.S. really needs a bon-a-fide cyber community to represent a broader range of stakeholders. Dr. St. Sauver believes for the U.S. to actively pursue appropriate cyber hygiene, "a new cabinet level federal agency" must be created and maintained.[24]

A clear strategy, whether it be one of deterrence or not, for cybersecurity offenses and defenses, as well as an expert and focused cyber community to execute such strategies, is necessary to limit the number of attacks and amount of damage done. Part of that strategy must include prescriptions on how to achieve good cyber health at all levels. In an outline provided by the DHS, a healthy cyber ecosystem considers not only how machines will react to cyber attacks, but also how users interact with machines. "Just as healthy individuals are essential to healthy communities, healthy participants are essential to a healthy cyber ecosystem. Cyber ecosystem participants include persons (both individuals and entities), devices,

22 Ibid.
23 Brown
24 Dr. Joe St. Sauver

and processes."[25] A complete national strategy must seek to promote a healthy cyber ecosystem as part of its plan to achieve thorough cybersecurity.

There have been few international efforts to regulate cyberspace, in comparison to other global commons. This may be due to the "newness" of cyberspace – after all, the seas have existed longer than man, and both airspace and outer space use have decades more experience than cyberspace. However, cyberspace, like the other domains, will need to develop its own identity as it matures. The quickness that outer space treaties and agreements came to be, especially during the height of the Cold War and the fact that "there is still no accepted legal definition of 'outer space,'"[26] demonstrates that the international community can come together for the common good in a reasonable amount of time. The same must happen with cyberspace.

While outer space treaties and agreements could be quickly formed, signed and ratified, the abstract environment and rapidly changing technology that is core to cyberspace may be partly to blame for slow international, and national, regulatory progress. However, the severity of a "Wild West" environment in cyberspace is one that must be rapidly tamed. "It is very much within the realm of the possible that the next battle we fight will not be on land, sea, air, or space—but on the networks," Brown wrote.[27]

All the past treaties pertaining to the global commons were written with the agreeance among recognized, territorial states. The Cold War was primarily fought by two key states. However, the past treaties and Cold War did not account for non-state actors. "Non-state actors, ranging from pirates off Somalia to cyber 'hacktivists' to the growing number of commercial players that own and operate satellites, further complicate this landscape" of the global commons, according to Brimley.[28] This is an issue that any future cybersecurity regulation or treaties must address.

In the abstract world of cyberspace, many analogies have been presented in hopes of both explaining what the domain of cyberspace represents as well as how it is and should be regulated. While "no analogy is perfect … regulations may be inconsistent, or even contradictory when developed in isolation."[29] Whether cyberspace is looked upon more as a domain for war or as an elaborate ecosystem with countless possibilities will directly influence how the realm is handled and regulated. "The real question for policymakers is this: Are we more concerned about foreign actors injuring our critical infrastructure or the constant drum of computer hacking and data breaches that has been prevalent over the past several months? It is a question not easily answered, as evidenced by how slowly Congress has acted in moving cybersecurity legislation."[30] If the analogies presented are dissected for their worth and those parts collaborated on, the modern-day Wild West may soon find itself tamed. If not, the U.S. will "run the risk of losing a battle without a shot being fired."[31]

25 "Enabling Distributed Security in Cyberspace"
26 "Cybersecurity Regulation: Using analogies to develop frameworks for regulation"
27 Brown
28 Brimley
29 "Cybersecurity Regulation: Using analogies to develop frameworks for regulation"
30 "War or Ecological Disaster? The Search for a Cyber Analogy," Jessica Herrera-Flanigan, NextGov.com, July 12, 2011, available at http://cybersecurityreport.nextgov.com/2011/07/war_or_ecological_disaster_the_search_for_a_cyber_analogy.php
31 Brown