Establishing Cyberspace Sovereignty

Kris E. Barcomb, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA

Dennis J. Krill, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA

Robert F. Mills, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA

Michael A. Saville, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA

ABSTRACT

International norms governing appropriate conduct in cyberspace are immature, leaving politicians, diplomats, and military authorities to grapple with the challenges of defending against and executing hostilities in cyberspace. Cyberspace is unlike the traditional physical domains where actions occur at specific geographic places and times. Rules governing conduct in the traditional domains emerged over centuries and share a common understanding of sovereignty that helps establish and justify the use of force. In cyberspace, sovereignty is a more abstract notion because the geographic boundaries are often difficult to define as data and applications increasingly reside in a virtual, global "cloud." This paper proposes a construct for establishing sovereignty in cyberspace by studying similarities between space and cyberspace. The characteristics of the space domain challenged traditional notions of sovereignty based on geography. As nations deployed space-based capabilities, the concept of sovereignty needed to mature to deal with the physical realities of space. Sovereignty is defined, and general requirements for claiming sovereignty are presented. The evolution of sovereignty in space is then discussed, followed by a construct for how sovereignty could be defined in cyberspace. The paper also reviews U.S. civil policy and military doctrine and discusses how these documents offer insights into the U.S. approach to asserting its claims within these domains. It concludes by examining an emerging trend where nations not only seek to establish sovereign claims over the architectural aspects of cyberspace, but also the information that flows over it.

Keywords: *Critical Infrastructure, Cyberspace, Information, Sovereignty, Space*

1. INTRODUCTION

Cyberspace exists within the realm of electronic data where activity happens at "network speed" through a vast array of interwoven networks, computers, and repositories spanning the globe. International norms governing appropriate conduct in this new domain are still developing, leaving politicians, diplomats, lawyers, and military authorities to grapple with the challenges of defending against and executing hostilities in cyberspace. Cyberspace is

DOI: 10.4018/ijcwt.2012070103

unlike the traditional physical domains where actions occur at specific geographic places and times. Rules governing conduct in these traditional domains emerged over centuries through diplomacy and conflict. They also share a common understanding of sovereignty that helps establish and justify the use of force. In cyberspace, sovereignty is a more abstract notion because geographic boundaries in air, land and sea are difficult to define as data and applications increasingly reside in a global, virtual "cloud."

Like cyberspace, the space domain is also relatively new, and its characteristics challenged traditional notions of sovereignty based on geography. Technological advancements outpaced the development of a legal framework for establishing internationally accepted practices in the domain, and the international community's understanding of sovereignty needed to mature to deal with the physical realities of space. Studying the emergence of space as a domain in its own right will help national leaders establish a concept of sovereignty in cyberspace. Once nations generally agree on the aspects of cyberspace where sovereignty might apply, they can then develop and employ means to protect those claims.

2. SOVEREIGNTY

Sovereignty is a complex concept in political science. The Stanford Encyclopedia of Philosophy (2010) defines sovereignty as the "supreme authority within a territory." Generally, a nation has sovereignty when it meets two conditions. First, it must have "formal" or "technical" sovereignty in the sense of formal recognition of sovereignty by other governments. This is known as *de jure* sovereignty. Second, it must have both practical control and jurisdiction over a territory. This is known as *de facto* sovereignty. (Colangelo, 2009, p. 626) To claim *de facto* sovereignty, a nation must be able to control the territory it claims and protect it from outside influence. The point at which a nation can claim *de facto* sovereignty is also a useful demarcation for delineating the difference between an "environment" and a "domain". For example, space did not become a domain until nations began to assert their presence within it; prior to that point, space was simply an environment.

Sovereignty's historical relationship to geographic territory complicates applying sovereignty to both space and cyberspace. The international community generally acknowledges geographic boundaries in the air, land, and maritime domains, but boundaries do not always apply directly to space and cyberspace. Fortunately, laws and customs governing both *de jure* and *de facto* sovereignty in space have successfully been developed over the last half century. Understanding the historical development of sovereignty in space is useful as nations attempt to define sovereignty within cyberspace.

2.1. The Evolution of Sovereignty in Space

In light of the unique challenges of establishing military norms in cyberspace, the United States military has turned toward the space domain to draw parallels. We can see this in the structural similarity between joint space and cyberspace doctrine discussed later in this article. It is also reflected in the way that U.S. services have aligned their space and cyberspace forces. U.S. Air Force cyberspace forces are subordinate to Air Force Space Command, U.S. Fleet Cyber Command is responsible for space and cyberspace operations supporting maritime forces, and Army Cyber Command grew out of the Army Space and Missile Defense Command.

As the prospect of man-made satellites transitioned from science fiction to reality, the international community struggled to determine whether or not geographic sovereignty should be extended into space. Long-accepted notions of sovereignty dictated that a nation had a right of self-defense against any action below, on, or above the geographic areas it claimed. In 1957, the Soviet Union launched Sputnik, which orbited the globe without regard for the territories over which it passed. After the launch, the Soviets reversed their previously held position that the sovereignty of a state extended to unlimited altitude and instead advocated that no state could claim sovereignty in space. (Reinhardt, 2005) This opened the door to U.S. space advocates who, prior to the launch of Sputnik, were concerned that a U.S. satellite launch could be considered an act of aggression. Donald Quarles, then Deputy Secretary of Defense stated, "the Russians have done us a good turn, unintentionally, in establishing the concept of freedom of international space." (Terrill, 1999, p. 29) Furthermore, other nations were largely silent concerning Sputnik's overflight of their territory. These events set a precedent for customary space law allowing for the free flight of satellites in space. (Terrill, 1999, p. 30)

In May of 1960, the Soviet Union shot down Francis Gary Powers' U-2 aircraft which was flying within the recognized boundaries of the Soviet Union. (Department of State, 1960) The Soviets thus exercised their *de facto* sovereignty by defending their airspace. Around that same time, the U.S. was close to launching a satellite capable of collecting intelligence similar to that provided by the U-2. The Corona imagery reconnaissance satellite, cloaked under the "Discoverer" program, provided the U.S. with a new means of assessing the strength of the Soviet nuclear program. (Ruffner, 1995, p. xiv) President Eisenhower ended the contentious U-2 overflights of the Soviet Union in favor of gathering similar data from space. The international precedent for satellite overflight established by Sputnik helped safeguard the Corona program. The first successful Corona launch occurred in August, less than four months after Powers was shot down. (Ruffner, 1995, p. xi)

In 1967, 10 years after the launch of Sputnik, international diplomatic efforts culminated in a basic framework for international space law called the Outer Space Treaty. Among other things, the treaty barred participants from placing nuclear weapons in space. (United Nations, 1967, Article IV) It also stated, "outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation or by any other means." (United Nations, 1967, Article II) However, the state launching an object into space retained jurisdiction and control over that object. (United Nations, 1967, Article VII) The Outer Space Treaty effectively established space as a *global commons*, similar to the high seas, where no country can make territorial claims, and any nation with appropriate technological capability can use its resources.

Beginning with the Strategic Arms Limitation Talks in 1969 and continuing beyond the end of the Cold War with the New Strategic Arms Reduction Treaty in 2010, the United States and Soviet Union negotiated agreements and treaties to maintain the balance of nuclear power between the two nations. They established that both parties would use "national technical means of verification" (i.e., reconnaissance satellites) and that each party would not interfere with the other's means. These statements codified the critical relationship between national technical means and national security. In light of the dependency between space assets and treaty verification, and the growing reliance on other space-based capabilities, the most recent U.S. National Space Policy claims the U.S. has an "inherent right of self-defense" of space assets. (United States of America, June 2010, p. 3) The document further clarifies that the U.S. will *deter* others from interference and attack, *defend* against hostile action and, if deterrence fails, *defeat* efforts to attack U.S. and allied space systems. The National Space Policy serves as a statement of the *de facto* sovereignty of the U.S. over its space assets.

The International Telecommunications Union also plays a role in space sovereignty. That organization is responsible to the United Nations (UN) for allocating geostationary orbital slots to nations and for managing satellite communication frequencies. (International Telecommunication Union, 2011) These functions play an important role in determining *de jure* sovereignty over space assets. Intentional intrusions into another nation's assigned orbits or interference with its satellite frequency allocations could be considered a hostile action on the international stage.

2.2. Cyberspace Sovereignty

Those engaged in defining international law as it pertains to cyberspace can learn from the historical development of space law and policy. Decades passed before the modern, generally-accepted notion of sovereignty emerged in the space domain. Likewise, nations must also decide which cyberspace assets are so important that it is willing to *deter*, *defend*, or if necessary *defeat* efforts to attack them. Each of these identified assets must be clearly traceable to national security objectives, just as national technical means were explicitly linked to nuclear treaty verification.

The following sections outline potential methods for evaluating sovereignty in cyberspace using U.S. policy and doctrine as the primary references. This is a critical step in laying the foundation for establishing control within the domain. Violations in any of these areas could provide a basis for taking action. For example, under normal circumstances in the United States, an aggressor who is a U.S. citizen would be subject to national law, with law enforcement agencies being responsible for enforcement and prosecution. Responses to aggressive actions from outside the nation would be dealt with using various instruments of national power, as deemed appropriate by national leadership.

2.2.1. Defining Critical Elements of Cyberspace

Within the United States, many organizations are engaged in identifying "critical infrastructure," which include cyberspace elements. The primary organization tasked with this responsibility is the Department of Homeland Security (DHS), but coordination when deciding what constitutes critical infrastructure spans Congress, the State Department, Department of Defense (DoD), law enforcement, and the intelligence community. The Patriot Act of 2001 defined critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." (United States of America, 2001, Sec. 1016 (e))

In 2009, DHS authored the National Infrastructure Protection Plan (NIPP), which identified the 18 sectors of critical infrastructure and key resources (CIKR) shown in Table 1. (Department of Homeland Security, 2009, p. 3) This list has grown from only 13 sectors originally identified in 2002. (Department of Homeland Security, 2002, p. 30) Interestingly, the NIPP does not explicitly identify space systems as critical infrastructure, although

Table 1. 18 critical infrastructure and key resource sectors

18 Critical Infrastructure and Key Resource Sectors		
Agriculture and Food	Banking and Finance	Chemical
Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services
Energy	Government Facilities	Healthcare and Public Health
Information Technology	National Monuments and Icons	Nuclear Reactors, Materials and Waste
Postal and Shipping	Transportation Systems	Water

it does reference communications satellites under the telecommunications category and describes space-based position, navigation and timing services as "components of multiple CIKR sectors." DHS states that cyber elements span all of these sectors. When describing the relationship between U.S. critical infrastructure and cyberspace, The *National Strategy to Secure Cyberspace* even goes so far as to declare that "Cyberspace is their nervous system—the control system of our country." (Department of Homeland Security, 2003, p. 1)

The *National Strategy to Secure Cyberspace* lays out three strategic objectives for securing cyberspace: (1) prevent cyber attacks against U.S. critical infrastructures; (2) reduce national vulnerabilities to cyber attack; and (3) minimize the damage and recovery time. (Department of Homeland Security, 2003, pp. 13-15) These three functions are analogous to the National Space Policy's *deter*, *defend*, and *defeat*, although the tone is much more focused on *deterrence* and *defense*, than on *defeat*. In fact, the word "defeat" is found only once in the *National Strategy to Secure Cyberspace* and refers to defeating a certain class of attack through a defensive versus offensive action. (Department of Homeland Security, 2003, p. 31)

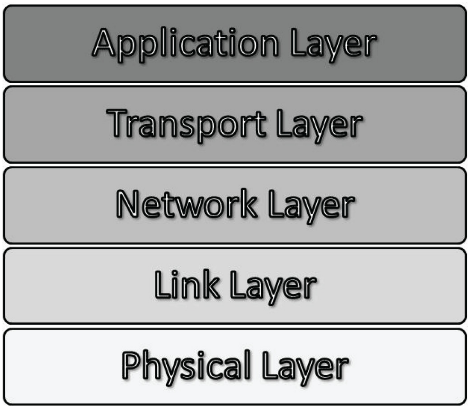
To date, the U.S. has not faced an attack in cyberspace sufficiently damaging to elicit a military response. In fact, an action of this magnitude has not occurred even internationally, although many hostile cyberspace actions, such as those conducted against Georgia and Estonia, have sparked intense debate over what responses are acceptable.˒ (Tikk, 2008; Evron, 2008) Given that the cyberspace domain exists to facilitate the flow of information, most "cyber attacks" either destroy, disrupt, or intercept that flow and typically fall under the categories of crime or espionage. By customary international law, neither of those activities is generally considered an acceptable justification for going to war. Loss of life or physical property of sufficient magnitude to meet the criteria for *jus ad bellum* has not occurred as a direct consequence of an attack generated in cyberspace. Unless significant progress can be made under peaceful circumstances, the issue will likely go unresolved until a sufficiently significant event forces the international community to deal with its ramifications under emergency conditions.

2.2.2. Recommendations for Establishing Sovereignty in Cyberspace

Nations need to have a clear understanding of what they consider critical elements of cyberspace before they can begin to assert sovereign claims within the domain. To this end, the 18 CIKR identified by the U.S. are a good first step, but the United States should continue to refine the list so that its scope is more precise. The current areas established by DHS cover an extremely wide variety of subjects. The diversity and breadth of those subjects make their prioritization extremely difficult. Eventually, if not already, it will be hard to find an example of what is *not* considered critical, and the U.S. will be no better off for having gone through the process. Just as space-based, national technical means were identified as critical to national security, critical infrastructure components must be identified according to their relationship to national security objectives. This is a foundational step for asserting sovereign claims in cyberspace. The next step is to make those claims with respect to the inner workings of this domain. Cyberspace is composed of many technical layers and understanding how each contributes to the overall whole is critical for setting sound policy.

One way to approach cyberspace sovereignty is to consider it holistically according to all of the layers shown in Figure 1. The depiction, commonly known as the Internet Protocol (IP) stack, illustrates the different layers of functionality required to support operations in cyberspace. Each layer has unique responsibilities for facilitating the flow of electronic information and most have international governing bodies overseeing their management. Having at least a basic understanding of the purpose and

Figure 1. Internet protocol stack (Kurose & Ross, 2009, p. 51)



the management structure for all aspects of the Internet Protocol Stack will help policy makers make better decisions concerning sovereignty in cyberspace.

The *physical layer* consists of the actual hardware, such as computer systems, network links, and the electromagnetic spectrum that provide the foundation of cyberspace. A physical attack on that infrastructure could be considered a "use of force" according to customary understandings of warfare, such as those found in Articles 2(4) and 51 of the UN Charter. Such an act would allow nations to act in "self-defense" to protect their sovereign territory. (United Nations, 1945)

Many devices now connect to cyberspace via wireless radio frequency (RF) links. Most nations tend to view the RF spectrum as a national resource that drives economic activity and commerce. As such, they monitor and regulate RF activity at local and national levels, and willful violation of national laws and regulations may result in criminal action. The International Telecommunication Union (ITU) constitution recognizes "the *sovereign right* of each State to regulate its telecommunication" (emphasis added), but also provides a global framework in which nations can cooperate and provide "efficient telecommunication services." (International Telecommunication Union, 2012) Thus, cyberspace attacks in or through the RF spectrum could potentially be viewed as violating a nation's sovereign right to use and manage its spectrum, as well as violating international conventions.

The physical layer presents difficulties for those who have attempted to label cyberspace as a "global commons" similar to space and international waters. (Department of Defense, 2005, p. 1) (Atlantic Council, 2010, p. 1). This interpretation stems from the perception that cyberspace is free, open and global. Unlike cyberspace, though, space and the high seas are natural domains that existed prior to their discovery and use, and humanity played no part in their creation. The physical layer of cyberspace presents a challenge to any notion of cyberspace as a global commons because every piece of infrastructure exists in some specific geographic location and is owned, operated and maintained by some entity, whether government, military or private sector. Treating cyberspace as a global commons fails to recognize that the underlying physical resources remain subject to private property rights (Kanuck, 2010, p.1579) and policy makers must account for this when defining cyberspace sovereignty.

The *link layer* provides a bridge between the physical hardware and the network. Every hardware device connected to the Internet has a unique Media Access Control (MAC) address. The Institute of Electrical and Electronics

Engineers (IEEE) manages the distribution of MAC addresses to hardware manufacturers by assigning them a 24-bit Organizationally Unique Identifier (OUI). Each hardware interface produced by that manufacturer will contain the OUI along with an additional 24-bit address that serves to identify the individual device uniquely. (Institute of Electrical and Electronics Engineers, 2011) These device identifiers provide a means of distinguishing one component from another on a local area network and could be used to delineate spheres of control in cyberspace akin to sovereign territory.

The *network layer* is the first layer that represents cyberspace subdivisions completely independently of the physical world. It serves to logically group and separate the realm of cyberspace. This layer is responsible for routing information from one node to another through all of the intermediary nodes along the way. Typically, it manages this according to the Internet Protocol (IP) address of the sender and receiver of the information. The Internet Assigned Numbers Authority is the international body responsible for the global coordination and assignment of IP addresses. (Internet Assigned Numbers Authority, 2011)

Both the assigned MAC and IP addresses of the link and network layers of the protocol stack could provide a basis for establishing internationally-recognized (*de jure*) sovereignty. Since international governing bodies manage these addresses, the global community might consider intentional actions taken to manipulate or infringe upon them as hostile. Anyone attempting to illegally impersonate an assigned IP address by falsifying his own network information or denying legitimate services intended for the address would be committing a criminal act. Any damage or loss associated with either of these activities could provide a basis for seeking restitution either on the national stage through law enforcement or on the international stage by exercising various instruments of national power, depending on the nature and effects of the attack.

The *transport layer* provides a means to logically link end systems together. For example, the Transmission Control Protocol establishes a logical connection between two processes for data transfer. This connection only exists as long as the two machines require it. During that period, though, the connection could be thought of as being owned by those two machines and no one else should be able to interfere with or duplicate it. The transport layer also allows systems to define ports that tie data connections to programs at the application layer. These ports act like doorways that allow information systems to access data or services on host machines.

No internationally-recognized agency allocates ports or connections to physical systems or organizations. Therefore, it would be difficult to claim any form of *de jure* sovereignty at this layer. Yet, these connections while transient in nature are essentially the property of the two connected systems for the duration of the connection. Any intentional attempt to hijack or circumvent those connections could be considered a hostile action.

Finally, the *application layer* provides a series of protocols by which systems exchange semantic information. Popular examples include Hypertext Transfer Protocol, Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP). DNS and SMTP are the most relevant to sovereignty. DNS automatically binds organizational names in a human-readable form to IP addresses. DNS makes using the web more efficient by freeing users from having to remember numeric IP addresses. For example, it is easier to remember "www.google.com" than 206.111.10.27, although one could use either to get to the same web page. The Internet Corporation for Assigned Names and Numbers (ICANN) is the internationally-recognized organization that manages the association of domain names to IP addresses. In executing this role, ICANN's efforts could provide a basis for establishing *de jure* sovereignty at the application layer. Intentionally corrupting the automatic translation from domain names to IP addresses performed by DNS servers would violate the victim's recognized identity. DNS also manages the name assignments associated with e-mail servers operating over SMTP, which is the protocol responsible for handling e-mail. An organization's e-mail address is a form of identification. Intentionally tampering with or impersonating an e-mail address by spoofing SMTP would also violate the identity of the victim.

In conjunction with identifying the sovereign aspects of cyberspace, nations asserting sovereignty must also develop and employ capabilities to patrol and protect those sovereign claims against the hostile actions from others. The first step is to organize, train, and equip cyberspace forces and then employ them to establish and maintain superiority in the domain. *Superiority* is the degree of dominance of one force over another which permits the conduct of operations by the former at a given time and place without prohibitive interference by the opposing force. (Department of Defense, 2010, p. 30) *Control* is the mechanism by which nations employ their instruments of power to establish and maintain superiority and protect their sovereign claims. The following sections provide an overview of U.S. joint doctrine covering space and cyberspace control. These topics are important for understanding how the U.S. asserts and exercises a form of *de facto* sovereignty in the space and cyberspace domains from a military perspective.

3. SPACE AND CYBERSPACE CONTROL

U.S. doctrine defines "Space Control" as one of five mission areas for space operations. Space control supports U.S. efforts to gain space superiority by "defeat[ing] adversary efforts that interfere with or attack U.S. or allied space systems and negat[ing] adversary space capabilities." Joint Publication 3-14: *Space Operations* establishes that the space control mission area consists of both offensive space control (OSC) and defensive space control (DSC). (Department of Defense, 2013, p. xi) The previous edition of this publication also included space situational awareness (SSA) under the umbrella of space control, but SSA has now been elevated to its own unique mission area. (Department of Defense, 2009, p. II-5) Since situational awareness is still a foundational component of the ability to control a domain, we will consider all three functions, OSC, DSC and SSA in the following discussion of space control.

OSC consists of measures taken to prevent an adversary's hostile use of U.S. or third party space capabilities or offensive operations to negate an adversary's space capabilities used to interfere with or attack the U.S. or the space systems of its allies. Joint doctrine clarifies that the adversary can include either state or non-state actors. (Department of Defense, 2013, p. xi) It also states that OSC is not limited to military options alone. Preventing an adversary's hostile use of space capabilities can include diplomatic, informational, military, and economic measures, as appropriate. (Department of Defense, 2013, p. II-8)

DSC covers both active and passive activities conducted to protect friendly space capabilities from attack, interference, or unintentional hazards. It includes all of the capabilities necessary to detect and characterize an attack, the ability to attribute an attack to an adversary, the ability to defeat the attack, and the ability to operate through or deter an attack. (Department of Defense, 2013, p. xi).

Lastly, SSA provides the foundation for accomplishing all other space control tasks. It underpins OSC and DSC by characterizing, as completely as necessary, the space capabilities operating within the terrestrial environment and the space domain. Contributors to SSA include space surveillance, environmental monitoring, and various intelligence sources to provide insight into adversary use of space capabilities and their threats to U.S. space capabilities. (Department of Defense, 2013, p. II-1)

U.S. military doctrine for cyberspace activity emerged with a similar structure to U.S. space doctrine. Originally covered under the umbrella of "Information Operations", it also consists of an offensive, defensive and intelligence gathering triad. The foundational doctrine for Information Operations established that the U.S. would achieve cyberspace superiority through Computer Network Operations (CNO) consisting of three mission areas: Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE). (Department of Defense, 2006, p. II-5) U.S. doctrine is still evolving, and new terminology is emerging as the DOD revises cyberspace doctrine. Regardless of what terminology the U.S. chooses to use, the core concepts of offense, defense and situational awareness are still foundational to a framework for approaching control in the domain.

CNA are "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." CND uses computer networks "to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks." CND actions protect DOD systems from both external and internal threats, and are a necessary function in all military operations. Finally, CNE is the set of network-based operations and intelligence collection capabilities conducted to gather data from target or adversary automated information systems or networks. (Department of Defense, 2006, p. II-5)

Having the ability to both patrol and protect assets within space and cyberspace is a critical component of *de facto* sovereignty over those assets. SSA and CNE capabilities provide a means to patrol the space and cyberspace domains, respectively. Protection has both offensive and defensive facets. The offensive capabilities in both domains serve to deter adversaries from taking hostile actions against critical assets. Defensive operations help protect assets when attacks occur. It is not enough to simply have strong perimeter defenses—*de facto* sovereignty requires the ability to actively seek out and identify undesirable activities within sovereign cyberspace assets, and then take appropriate action to nullify or mitigate those activities.

4. INFORMATION SOVEREIGNTY

The preceding discussion dealt with cyberspace sovereignty from an architectural perspective. Its purpose was to help provide insight into questions about how nations can protect what they believe to be their portions of the domain. An emerging trend is for nations to exert claims of sovereignty at the semantic layer that rides above the architectural layers described in Figure 1. One could describe these assertions as *Information Sovereignty*. Many organizations, such as Freedom House, the Open Net Initiative and the Global Network Initiative, have been actively documenting how nations are attempting to control the flow of information to and from their citizens. Over concerns that information technology may foster political unrest, "many authoritarian states have taken various measures to filter, monitor, or otherwise obstruct free speech online. These tactics were particularly evident over the past year in countries such as Saudi Arabia, Ethiopia, Uzbekistan, and China, where the authorities imposed further restrictions following the political uprisings in Egypt and Tunisia, in which social media played a key role." (Freedom House, 2012, p. 1)

In response to political censorship and restrictions on free speech by authoritarian regimes, the United States has begun taking a proactive role in promoting universal freedoms online. The 2010 National Security Strategy (NSS) extols the extraordinary potential of cyberspace in promoting information freedom. It also ties this value to a belief that individuals will be able to form a more capable and peaceful democratic government when freedom to communicate is allowed to flourish. In the section titled *Marshalling New Technologies and Promoting the Right to Access Information*, the NSS declares, "[information technologies] have fueled people-powered political movements, made it possible to shine a spotlight on human rights abuses nearly instantaneously, and increased avenues for free speech and unrestricted communication around the world.

We support the dissemination and use of these technologies to facilitate freedom of expression, expand access to information, increase governmental transparency and accountability, and counter restrictions on their use." (United States of America, May 2010, p. 39)

Another key component of U.S. policy toward information sovereignty is contained in the section of the NSS titled *Promote Democracy and Human Rights Abroad*. It states, "The United States supports the expansion of democracy and human rights abroad because governments that respect these values are more just, peaceful, and legitimate. We also do so because their success abroad fosters an environment that supports America's national interests. Political systems that protect universal rights are ultimately more stable, successful, and secure."

These statements put U.S. policy in line with international agreements, such as the *Universal Declaration of Human Rights (UDHR)* adopted by the United Nations General Assembly in 1948 and its two subsequent covenants—the *International Covenant on Civil and Political Rights (ICCPR)* and the *International Covenant on Economic, Social and Cultural Rights (ICESCR)*. Specifically, Article 19 of the UDHR states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (United Nations, 1948) In a sense, the UDHR is a *de jure* recognition that freedom of expression is a universal value and that no nation should be able to claim sovereignty over information if those claims affect the rights of its citizens to inform themselves or speak out on their own behalf.

In the United States, the Department of State has taken the lead on implementing U.S. policy to promote a universal freedom to communicate in and through cyberspace. On 21 January 2010, speaking to an audience at the Newseum in Washington D.C., former Secretary of State Hillary Clinton delivered a seminal speech outlining the importance of Internet freedoms. Her speech expanded on President Roosevelt's "Four Freedoms" speech delivered on 6 January 1941, and also highlighted the work done by Mrs. Roosevelt when she helped draft the UDHR. In 1941, the President looked forward to a world founded upon four essential human freedoms: *freedom of speech and expression, freedom of worship, freedom from want, and freedom from fear*. (Roosevelt, 1941) Secretary Clinton added a fifth freedom to the list: *freedom to connect*. (Clinton, 2010) Her speech was a formal acknowledgement of the prominent role the Internet would play in US foreign affairs for the foreseeable future and the U.S. stance toward authoritarian claims concerning information sovereignty for the purpose of political censorship.

On 8 December 2011, the State Department issued a factsheet describing its Internet freedom programs. The document highlighted six programming areas important to protecting freedoms online: *counter-censorship technology, secure mobile communications, digital safety training, emergency funding for activists, Internet public policy,* and *research on Internet repression*. It also stated that since 2008 the U.S. Congress has appropriated $70 million to fund these efforts. As a result, the State Department, in concert with its partners, now has a portfolio of over 20 circumvention and secure communications tools. These tools help 1.9 million unique users per month and have received more than 115 million downloads. The State Department has also provided in-person training for over 7500 Internet activists in contested environments and made non-technical support materials available in over 10 languages to assist those in oppressed information environments. (Department of State, 2011)

Of course, not all nations feel the same way about freedom of expression. For example, the official press agency of the People's Republic of China, the Xinhua News Agency, stated, "information technology that has brought mankind all kinds of benefits has this time become a tool for interfering in the internal affairs of other countries." They made this statement in response to the Green Revolution in Iran, which Chinese authorities saw as having been facilitated by American technology. (Morozov, 2011, p. 12) Another example comes from the deliberations leading up to the December 2012 World Conference on International Telecommunications (WCIT-12). One of the key items on the conference agenda was revising a 24-year old treaty known as the International Telecommunications Regulations. Despite apparent contradictions to the UDHR, Russia proposed language expressing that the public should have unrestricted access to international telecommunication services, "except in cases where international telecommunication services are used for the purpose of interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity and public safety of other states, or to divulge information of a sensitive nature." Many fear that if such language were to be ratified, then authoritarian governments might be able to justify political censorship by pointing to international law. In defense of U.S. policy and the UDHR, the U.S. delegation to the conference declared it would block any proposals that support online censorship or undermine the current governing structure of the Internet. (Lardner, 2012) In the end, 89 of 144 participating nations signed the "Final Acts" of the WCIT-12. The United States, United Kingdom, Canada, Australia and others opposed the final document, while Russia, China and many Arab, African, and Latin American countries were signatories. (International Telecommunications Union, 2012) The results of the vote highlight the diversity of international opinion on the subject.

This section on information sovereignty highlights the multifaceted nature of sovereignty in cyberspace. From an architectural perspective, nations wish to protect their investments in cyberspace and the integrity of their cyberspace systems. At the semantic layer, where humans-to-human interaction occurs, nations have some striking differences over how to approach protecting information. The United States and many other nations profess a belief in universal freedom to communicate. They have established policies codifying this belief because it is in line with democratic ideals. On the other hand, non-democratic nations see freedom of expression as a threat to their ability to control information within their sovereign borders.

5. CONCLUSION

International norms governing appropriate conduct in cyberspace are immature. As nations become more dependent on cyberspace, they are struggling to clearly define their claims within it and to determine appropriate responses when those claims are jeopardized. The sovereign aspects of cyberspace should not be limited to only the physical infrastructure that supports the flow of electronic information, but should also include key aspects of all the layers of the Internet Protocol Stack. Additionally, efforts to codify cyberspace sovereignty should account for the semantic layer of cyberspace where information resides. Information sovereignty is growing in importance as governments grapple with controlling the information their citizens can transmit and receive. As with any other domain, nations should clearly link their sovereign claims in cyberspace to national security objectives to support their prioritization, develop appropriate responses and clarify intentions on the international stage.

Assertions of sovereignty are unsustainable unless a nation has a sufficient ability to patrol and protect its claims. Nations will continue to invest in cyberspace capabilities that allow them to protect their sovereign claims within the domain. These steps are necessary to overcome the combination of technological, legal, and military challenges that nations faces as the world's reliance on information technologies continues to expand at an exponential rate.

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

REFERENCES

Atlantic Council. (2010). *ACT Workshop Report: NATO in the Global Commons*. Retrieved from http://www.act.nato.int/images/stories/events/2010/gc/report01_wash.pdf

Clinton, H. (2010). *Remarks on internet freedom*. Retrieved January 21, 2010, from http://www.state.gov/secretary/rm/2010/01/135519.htm

Colangelo, A. (2009). De facto sovereignty: Boumediene and beyond. *The George Washington Law Review*, *77*(3). Retrieved from http://docs.law.gwu.edu/stdg/gwlr/issues/pdf/Colangelo-77-3.pdf.

Department of Defense. (2005). *Strategy for homeland defense and civil support*. Retrieved from http://www.defense.gov/news/Jun2005/d20050630homeland.pdf

Department of Defense. (2006). *Joint publication 3-13, information operations*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Department of Defense. (2010). *Joint publication 1-02, department of defense dictionary of military and associated terms*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Department of Defense. (2013). *Joint publication 3-14, space operations*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf

Department of Homeland Security. (2002). *National strategy for homeland security*. Retrieved from http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf

Department of Homeland Security. (2003). *National strategy to secure cyberspace*. Retrieved from http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

Department of Homeland Security. (2009). *National infrastructure protection plan*. Retrieved from www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Department of State. (1960). *State department press release #249 concerning U-2 incident*. Retrieved from http://eisenhower.archives.gov/Research/Digital_Documents/U2Incident/5-6-60_No249.pdf

Department of State. (2011). *Factsheet: State Department Internet Freedom Programs*. Retrieved December 8, 2012, from http://www.humanrights.gov/wp-content/uploads/2011/12/20111208-Fact-Sheet-InternetFreedomPrograms.pdf

Evron, G. (2008). *Battling Botnets and online mobs: Estonia's defense efforts during the Internet War. Georgetown Journal of International Affairs*, 121-126. Retrieved from http://dx.fi/media/blogs/dx/0000699.pdf

Freedom House. (2012). *Freedom on the net 2012*. Retrieved from http://www.freedomhouse.org/sites/default/files/inline_images/FOTN%202012%20FINAL.pdf

Institute of Electrical and Electronics Engineers. (2011). *Registration authority general information*. Retrieved from http://standards.ieee.org/develop/regauth/general.html

International Telecommunication Union. (2011). *Radiocommunication sector*. Retrieved from http://www.itu.int/ITU-R/index.asp

International Telecommunication Union. (2012). Signatories of the final acts. In *Proceedings of the World Conference on International Telecommunications*. Retrieved from http://www.itu.int/osg/wcit-12/highlights/signatories.html

Internet Assigned Numbers Authority. (2010). Retrieved from http://www.iana.org

Kanuck, S. (2010). Sovereign discourse on cyber conflicts under international law. *Texas Law Review, 88*(7) Retrieved June 1, 2010, from http://www.texaslrev.com/sites/default/files/issues/vol88/pdf/Kanuck.pdf

Kurose, J., & Ross, K. (2009). *Computer networking: A top-down approach* (5th ed.). Addison Wesley.

Lardner, R. (2012). *A battle for internet freedom as un meeting nears*. Associated Press. Retrieved June 22, 2012, from http://bigstory.ap.org/article/battle-internet-freedom-un-meeting-nears-0

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. New York, NY: Public Affairs. doi:10.1017/S1537592711004026.

Reinhardt, D. (2005). *The vertical limit of state sovereignty*. McGill University. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA436627

Roosevelt, F. (1941) *Transcript of President Franklin Roosevelt's annual message (four freedoms) to Congress (1941)*. Retrieved from http://www.ourdocuments.gov/doc.php?flash=true&doc=70&page=transcript

Ruffner, K. (1995). *Corona: America's first satellite program*. Center for the Study of Intelligence. Central Intelligence Agency. Washington D.C. Retrieved from https://www.cia.gov/library/publications/additional-publications/corona-between-the-sun-and-the-earth/corona.pdf

Stanford Encyclopedia of Philosophy. (2010). *Sovereignty*. Retrieved from http://plato.stanford.edu/entries/sovereignty/

Terrill, D. (1999). *The Air Force role in developing international Outer Space law. Maxwell AFB*. AL: Air University Press.

Tikk, E., et al. (2008). *Cyber attacks against Georgia: Legal lessons identified*. Cooperative Cyber Defense Centre of Excellence. Retrieved from http://www.carlisle.army.mil/DIME/documents/Georgia%20 1%200.pdf

United Nations. (1945). *Charter of the United Nations*. Retrieved from http://www.un.org/en/documents/charter

United Nations. (1948). *The Universal Declaration of Human Rights*. Retrieved from http://www.un.org/en/documents/udhr/index.shtml

United Nations. (1967). *Outer Space treaty*. Retrieved from http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_21_2222.html

United States Air Force. (2010). *Air Force doctrine document 3-12, cyberspace operations*. Retrieved from http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf

United States of America. (2001). *U.S. Patriot Act*. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

United States of America. (June 2010). *National Space Policy of the United States of America*. Retrieved from http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf

United States of America. (May 2010). *National security strategy*. Retrieved from http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf