Dr. Josh Kvavle, right, demonstrates Google Glass headset for Chief of Naval Operations Admiral Jonathan Greenert during Rapid Innovation Cell meeting (U.S. Navy/Peter D. Lawlor)

One Size Does Not Fit All

The Multifaceted Nature of Cyber Statecraft

By Andrea Little Limbago

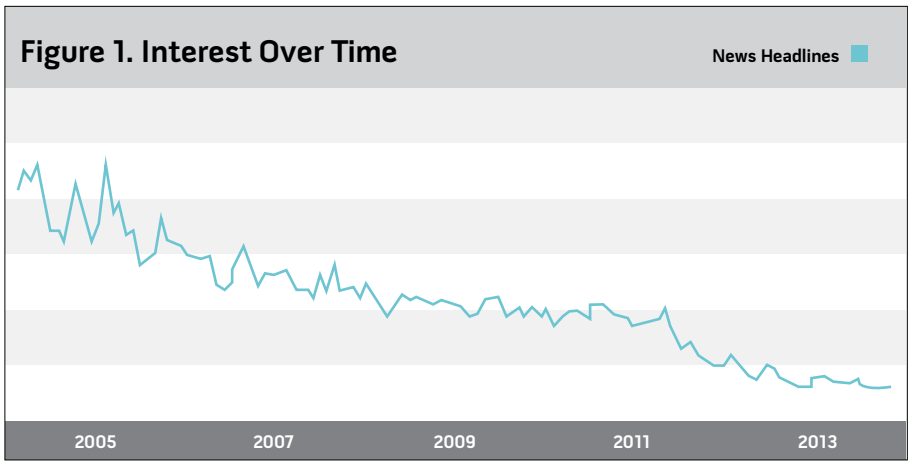
Cyberspace is frequently referred to as the fifth domain, alluding to its perceived role as the next major battlefield after land, sea, air, and space. However, this oversimplification of cyberspace underestimates its transformational impact within and across each of these domains. Moreover, framing cyber solely as a battlefield and coercive domain ignores the diverse ways in which both state and nonstate actors use cyber statecraft to pursue their objectives. It is an understatement to say that the introduction of cyberspace as a fifth domain has had disruptive effects on the international system, but to date there has been little discussion on the myriad ways in which actors exploit cyberspace for geopolitical gain. From Stuxnet at one extreme to government-sponsored Facebook accounts at the other, digital disruption has significantly increased the tools available to state and nonstate actors. Even transitions of power are now often first publicized in cyberspace. For example, following the recent coup in Thailand, martial law was officially declared via Twitter and a new Facebook account and was dubbed by some researchers as a *#cybercoup*.

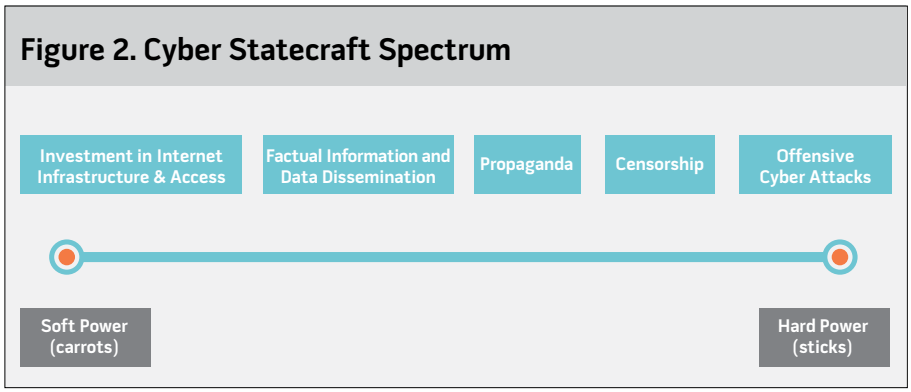
To better evaluate the strategic implications of cyber as a domain in which to achieve national security objectives—from antiaccess/area denial to governance, democratization, and economic growth—policymakers need a rigorous, multifaceted framework that examines cyber statecraft not only as a military tool, but also as a more holistic form of statecraft. Such a framework is long overdue to help make sense of the great technological disruption that continues to shape the international political system. While the military component is essential, cyber statecraft is often viewed

Dr. Andrea Little Limbago is the Principal Social Scientist at Endgame, a security intelligence and analytics software company.

only through this coercive lens, when in fact it is much broader. Even within the military aspects of cyber statecraft, little has been written about the various tools available to actors in this domain, which has led to everything from cyber censorship to cyber espionage being lumped together under the broad umbrella of *cyber attacks*. These comparisons greatly impede the ability of practitioners and theorists alike to assess the strategic implications of cyber statecraft.

In comparing cyber studies to the evolution of nuclear strategic studies, Joseph Nye notes, "Strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950."[1] In short, cyberspace analyses and theories lag behind changes in the operating environment, resulting in a theoretical and operational void that has strategic implications. The classification of cyberspace as solely a domain of conflict has contributed to this theoretical stagnation, limiting policymakers' understanding of the ways in which cyberspace can be leveraged for broader applications of statecraft. But the militarization of cyberspace is not the only culprit here; the gap between the technical and national security policy communities is also partially to blame. The technical nature of discussions on cyberspace has hindered a coherent understanding of cyber as statecraft. Moreover, the phenomenal speed of technological change has rendered it difficult for policymakers and the larger strategic studies community to remain apace of developments within the cyber domain.





The Cyber Statecraft Spectrum

On the surface, it may seem pedantic to build a theoretical framework for analyzing and understanding the various implementations of cyber statecraft. Lacking such a framework, however, cyber statecraft risks perpetuating the perception that it is solely an offensive tool. In his book *A Fierce Domain*, Jason Healey notes the increasing militarization of the term *cyber*.[2] While initially a neutral term, current references to cyber generally imply offensive behavior, while *Internet* is used when discussing the positive technological impacts of cyberspace. In fact, discussion of cyberspace as a unique domain has decreased dramatically over the last 15 years. This trend is quite stark when conducting a quick review of Google search term trends for *cyberspace*, as depicted in figure 1. Cyber is increasingly used as a prefix for a variety of offensive activities such as cyberwar, cybercrime, and cyber attacks.

This trend parallels changes in perceptions of economic statecraft, which was initially viewed as a form of state coercive power. As mercantilism gave way to a more liberal global economy, strategists began to attribute pacifying effects to economic statecraft as well. The recognition of the potential of economic tools to promote peace and development helped ensure that economic statecraft was viewed as more than just a coercive tool in power politics. Just as economic statecraft generally refers to the use of economics as a persuasive political instrument, cyber statecraft can be similarly regarded as the use of cyber tools to achieve political objectives. Moreover, unlike other tools of statecraft, cyber tools are not pigeonholed into a discrete category. Cyber statecraft permeates each of the diplomatic, information, military, and economic elements of power. This likely is due to the unique nature of cyberspace and its multiple layers, including both the physical and communication domains. In each case, however, cyber statecraft serves as the means to achieve political goals within that element of power. Similar to the rise of economic statecraft during the mercantilist period, cyber statecraft has emerged as an omnipresent tool of choice in the current era of globalization and pervasive information technology.

Contrary to common perceptions, cyber statecraft is used to exert both hard power (that is, coercion, punishment) and soft power (such as persuasion to adopt

Maryam Mirzakhani was awarded 2014 Fields Medal—International Congress of Mathematicians' first female prize winner in its 80-year history—for "her outstanding contributions to the dynamics and geometry of Riemann surfaces and their moduli spaces" (courtesy of Maryam Mirzakhani)

similar goals, attraction), and everything in between. While by no means an exhaustive list, figure 2 depicts a broad categorization of the cyber tools most frequently employed, ranging from positive incentives for Internet freedom and access on one extreme to offensive cyber attacks on the other. This framework depicts the *physical* layers of cyberspace on either extreme of the spectrum, with the *communication* aspects occupying the middle ground.

The remainder of this article provides current, concrete examples of the use of cyber statecraft across the power spectrum and, in doing so, suggests a strategic framework for understanding and leveraging cyber as tool of statecraft. As the following examples illustrate, state and nonstate actors employ cyber statecraft in diverse ways to pursue a range of objectives. As with other forms of statecraft, cyber statecraft can be used for benign or malicious intents. In conjunction with the tool employed, intent becomes an additional determining factor of whether the application of cyber statecraft is a carrot or a stick. Therefore, the goal is not to provide an exhaustive overview of every tool possible within cyber statecraft, but rather to expand perceptions of cyberspace to include the diversity of tools accessible within this domain along the power spectrum. Moreover, as the examples illustrate, cyber statecraft is unique in its asymmetric nature, capable of empowering not only major powers but also serving as a means for weaker actors to have a disproportionate impact in the international arena.

Investment in Internet Infrastructure and Access

State investment in cyber infrastructure—while also promoting connectivity through physical infrastructure—fosters technology-driven solutions to a wide range of economic, political, and social issues that plague the developed and developing world alike. Many governments—and even some nonstate actors—implement cyber infrastructure to empower populations through the positive externalities that often coincide with Internet access. Therefore, government investment both in the expansion of physical infrastructure as well as in access to the Internet is absolutely essential for achieving political objectives. Information technology infrastructure—including the hardware as well as its legal aspects—serves as the mechanism through which governments transmit content used for attraction and persuasion. Numerous positive political and economic externalities have been associated with greater Internet access, especially in the developing world. Greater Internet access can increase private-sector competitiveness, enhance educational opportunities, and spark economic efficiencies. For instance, technological participation—only possible via an existing cyber infrastructure—can provide a means for reaching at-risk populations. Connectivity could become a key tool in combating radicalization by providing greater access to information, education, and economic opportunities as well as entertainment. The possible economic benefits are particularly prevalent in populations that rely on mobile money transfers and Internet banking as core components of their economy.

The potential for this soft power mode of cyber statecraft to shape the current geopolitical environment is likely to grow as Internet access continues to spread globally—especially as countries leapfrog archaic technologies in favor of modern communication systems. For instance, the 2012 World Bank report *Information and Communication for Development* identifies mobile broadband as having an even stronger impact on economic growth than fixed broadband.[3] In many developing countries, mobile money platforms enable both aid organizations and the domestic population to circumvent economic blockades and provide assistance as well as integration with the global economy.

Kenya is one of a growing number of countries that has received accolades for its concerted expansion of Internet access over the past few years. According to the World Bank World Development Indicators, Internet usage in Kenya has increased by 400 percent over the last 5 years.[4] This is significant, particularly since Kenya was threatened with rising unrest following a controversial election in 2007, when less than 10 percent of the population had Internet access. The impact of this expanded access is not solely economic. It also encourages the development of human capital through access to online education tools and

information such as daily market prices—essential knowledge in agrarian areas. As Kenya's situation demonstrates, investments in Internet expansion are critical to a government's ability to provide the environmental conditions for the effective use of soft power. While not necessarily new, this phenomenon has recently received more rigorous attention as governments devote resources specifically for the creation and expansion of Internet architecture and a technology-based economy. In the 1970s, for example, India set aside an area near Bangalore to create an electronic city. However, the legal and economic systems lagged behind, and the information technology hub did not truly begin to emerge until economic liberalization took hold in the 1990s.

Building up a cyber architecture is not solely a tool for achieving inward-facing domestic objectives, but it is also emerging as a component of power politics as states vie for regional influence. For example, fiber networks and cell towers can be used to help build alliances between countries and expand a major power's sphere of influence. This tactic is also increasingly employed by some multinational corporations to achieve their own objectives. Google's Project Link, which aims to build fiber networks in Africa, is a case in point. Conversely, the Europe/Brazil effort to build an underwater cable with the goal of circumventing U.S. surveillance efforts demonstrates the role of power politics within cyberspace. Finally, the creation of cyber infrastructure could become a tool in peacekeeping missions and conflict interventions. Following a conflict, restoring the cyber infrastructure may become just as important as providing access to essential services such as security, water, and electricity as technology becomes the medium through which disparate aid efforts and financial assistance can be coordinated and systematically dispersed, while also serving as the bedrock for reconstructing postconflict political, economic, and social institutions.

Factual Information and Data Dissemination

While the popular discussion focuses heavily on Internet censorship, many state and nonstate actors also leverage cyberspace as a means to diffuse factual information to their populations, provide greater transparency, and signal their intent. In Iran, President Hassan Rouhani ran on a platform of greater Internet openness. While he has undoubtedly implemented coercive cyber tools, which will be discussed subsequently, Rouhani simultaneously uses his Twitter account to spread a more positive message of transparency. Recently, he used Twitter to congratulate Iranian mathematician and Fields Medal–winner Maryam Mirzakhani, and included a picture of her without a headscarf—an apparent attempt at demonstrating openness and preventing further "brain drain" from Iran. This is not a single occurrence with Rouhani. He also previously tweeted the content of his call with President Barack Obama following the September 2013 United Nations General Assembly in New York. Similarly, the Thai government's tweet announcing martial law can be viewed as a means of promoting transparency by openly disseminating critical information to the greater population. Twitter remains a mechanism through which the Thai people interact with the new military-led government.

Ohio National Guard Computer Network Defense Team members conduct operations during Cyber Shield 2015, March 2015, at Camp Atterbury, IN (Ohio National Guard/George Davis)

Governments also employ cyber tools to defend their actions or indirectly signal intent that would be politically imprudent to express directly. For instance, President Dilma Rousseff used her Twitter account to defend Brazil's preparation for the World Cup. Prime Minister Shinzo Abe also appears to be using his Twitter account to signal to the Japanese people his foreign policy intentions. Abe only follows a handful of people on Twitter, but India's Prime Minister Narendra Modi is one of them. It is too soon to tell whether this indicates closer future ties between the two countries, but social media is an easy and subtle way to inform the population of a leader's intent or interests.

Finally, mobile technologies have provided the technological foundation for community policing programs in both the developing and the developed world. Rwanda has implemented crowdsourcing initiatives that leverage mobile platforms to strengthen the rule of law, thereby enabling the community to pass along information regarding looting and violent incidents and to simply serve as citizen journalists. The crowd-sourcing of information for the purpose of depicting

Slovenian soldier assesses mission group's response to cyber attack during Combined Endeavor 14, world's largest C4 systems exercise (U.S. Marine Corps Forces Europe/Derrick K. Irions)

events factually and in real time is not limited to state actors but is actually a tactic employed more often by nonstate actors such as nongovernmental organizations as well as the general population. This is apparent during events as diverse as the Venezuelan protests, the Wenzhou train crash in China, and the recent Ebola crisis in West Africa. Of course, intent plays a key role in categorizing cyber behavior as the insertion of factual information or as propaganda. Government propagation of false information is increasingly common.

Propaganda

The spectrum of cyber statecraft has geopolitical relevance not only through its positive tools of persuasion and attraction. Cyber statecraft is also used by governments and nonstate actors for more punitive intents and the dispersal of misinformation. Vladimir Putin's aggressive behavior epitomizes the exploitation of cyberspace as a propaganda machine. He has used fake Facebook accounts and other well-known social media outlets to depict the Crimean annexation in a positive light. This includes, but is not limited to, falsifying crimes and atrocities committed by Ukrainian extremists. He also has employed the Web to shape the narrative regarding Malaysian Flight 17, providing a range of incredible scenarios ranging from denial that it was shot down to claiming he was the intended target. Similar to how leaders used traditional tools of statecraft in previous eras, he relies on cyber tools to promote a rally-round-the-flag effect and gain domestic support for Russian policy. As in historical examples, Putin applies not just one tool of cyber statecraft but instead integrates cyber propaganda with rising censorship and greater government control of the Internet. China takes a somewhat different approach to online propaganda. The government hires online commentators, often referred to as the 50-cent party, who are paid to participate in online communities to counter anti-party content, promulgate the party agenda, or deter sensitive content.

Violent extremist organizations similarly employ cyber statecraft as a propaganda tool and a key mechanism for recruitment and radicalization. Social media is largely used as the venue for these propaganda instruments. However, some of the more tech-savvy groups, such as Hizballah, have also created apps to recruit followers and disperse their ideologies. Other nonstate groups, such as the Sinaloa Cartel and those linked closely to governments such as the Syrian Electronic Army, similarly create YouTube videos and Twitter accounts as revisionist mechanisms to shape the discourse on current events or to propagate the promise of a luxurious lifestyle as a member of their groups.

Censorship

State use of cyberspace applies to both the manipulation of content, as previously discussed, and the censorship of it. Internet censorship has produced a wide range of outcomes, and the conditions under which it achieves the desired result remain vague. Depending on its depth and breadth, Internet censorship may actually fuel unrest instead of extinguishing it. For instance, Venezuela's attempts in 2014 to censor Twitter only ignited growing protests against the government. Thailand has similarly tried to censor various social media sites, both after protests began last year and after the imposition of martial law. Turkey recently lifted its block on YouTube, which was enacted after recordings of a security meeting were leaked. The subsequent political crisis resulted in increased Internet censorship over the last year, which sparked protests that still plague the Recep Tayyip Erdogan government. Similarly, Rouhani recently banned Instagram, which now joins Facebook and Twitter as an officially banned social media outlet in Iran. Ironically, Rouhani himself is a prolific Instagram user with a large following. Finally, the Serbian government's mismanagement in the wake of some of the country's worst flooding in over a century ignited a vocal cyber backlash. In response, the Serbian government employed censorship to control the narrative, removing sites that highlighted erroneous government actions or were critical of the government writ large.

While the previous examples focus on Internet censorship as a means to limit antigovernment content, China has taken a somewhat different approach, albeit with similar tools. A recent Harvard publication, "How Censorship in China Allows Government Criticism but Silences Collective Expression,"[5] analyzes a wide range of social media data and finds that the major goal of Chinese censorship is to prevent social mobilization. While the previous examples focus on limiting antigovernment rhetoric, Chinese leadership is much more likely to censor any content that may lead to group mobilization, regardless of the topic of the content. This tendency surfaced in 2014 with the 25th anniversary of the 1989 Tiananmen Square Massacre. Chinese censors blocked major social media outlets and references pertaining directly or indirectly to Tiananmen Square, with the objective of preventing any similar social mobilization.

Offensive Cyber Attacks

At the extreme end of the cyber statecraft spectrum, an actor's offensive use of cyber tools rounds out their punitive uses in statecraft. Offensive cyber tools range dramatically in severity and they themselves comprise a broad spectrum of statecraft tools. They could arguably be compartmentalized into four distinct areas: insertion (for example, malware), blocking (distributed denial of service [DDoS]), removal (cyber espionage), and destruction (such as of critical information or infrastructure). In 2009, the United Arab Emirates relied on the partially state-owned telecommunications company Etisalat to request that its BlackBerry users update their phones with service enhancements, which consequently implemented spyware on devices that provided the government with unauthorized access to private information. The pro-government Syrian Electronic Army, a loosely knit group of hacktivists, went even further and has been credited with—among other cyber

attacks—the implementation of Dark Comet and Blackshades malware against antigovernment activists. Although the strength of its direct ties to the Bashar al-Asad regime is unclear, the nonstate group does function as a government surrogate and has aimed domestic attacks against antigovernment activists. Many of their tools bear a resemblance to those used by Iran against its population during the Green Revolution, and many analysts believe Syria is using Iranian-designed offensive software. It is possible the Asad regime used similar tools in 2012 during the unprecedented 2-day Internet blackout in Syria.

These examples illustrate the increasing trend of states employing cyber sticks against their own populations. Of course, offensive cyber statecraft is not limited to domestic implementations. Cyber attacks have also clearly become a tool in interstate power politics, evident in conflicts and disputes as diverse as those between North and South Korea, Russia and Georgia, and India and Pakistan. In some of these instances, similar to how the Syrian Electronic Army has perpetrated cyber offense, nonstate groups closely aligned with the state government actually carry out the cyber attack, elevating the complexity of the interstate conflict due to the ambiguous nature of attribution in cyberspace. States certainly have the advantage in implementing highly technical and complex offensive tools such as those used in the Olympic Games, the German-based R2D2 Trojan, and Russian CosmicDuke. Similarly, to date, interstate dynamics maintain a monopoly on the use of destructive cyber tools such as Stuxnet, which damaged Iranian nuclear reactors in Natanz, as well as the Shamoon virus, which attacked the Saudi Arabian oil company Saudi Aramco. Shamoon infected three-quarters of the company's personal computers (PCs), but was stopped before affecting the oil supply. The Aramco attack required the company to replace tens of thousands of its PCs and is believed to have originated from Iran.

Given the asymmetric nature of the cyber domain, these tools do not reside solely in the domain of state actors, although the scale and scope can obviously vary significantly when employed by nonstate actors. Chinese hackers recently stole health records by exploiting the Heartbleed bug, while the Target and Neiman Marcus data breaches are perhaps the most prominent examples of successful cyber espionage aimed at multinational corporations. The decentralized, loosely knit hacktivist group Anonymous has aimed its tools at both state and nonstate groups, carrying out DDoS attacks against the Israeli government and using their cyber exploits to support Arab Spring movements. Nevertheless, governments are countering the group's influence. The British government's DDoS attacks against Anonymous might be the first publicized instance of a state-sponsored DDoS campaign. As these examples continue to surface, each new revelation sets a precedent for a potential rise in offensive cyber statecraft within cyberspace. However, attribution issues escalate the role of misperception within cyberspace, rendering it much more difficult to comprehend the long-term impact that the instantiation of these tools will have on international relations.

Conclusion

This initial overview of a cyber statecraft framework—and the range of tools available to state and nonstate actors—provides a more structured and nuanced approach for exploring and understanding the growing use and implications of cyber statecraft. This is long overdue, as the national security implications of cyber statecraft remain greatly underexplored yet are rising in importance. Cyber as a tool of statecraft has been commandeered by an overemphasis on its militarized aspects. This focus on cyber's offensive manifestations ignores the nuanced nature of this critical domain and its broader application to geopolitics. Although powerful and disruptive, cyber statecraft comprises much more than just intelligence or offensive capabilities. Analysts and policymakers alike must begin viewing cyber statecraft not as a discrete offensive tool useful only in narrow cases, but rather as a form of statecraft on par with other more traditional forms of statecraft, with state and nonstate applications ranging from attraction to coercion along the soft-hard power continuum. Applying a more formalized statecraft model to cyberspace helps add robustness and promote greater comprehension of the role of cyber statecraft for security and policy leaders, while adding to the international relations community's understanding of the national security and geopolitical implications of cyber statecraft and cyberspace writ large.

It is time to end the hyperfocus on cyber as a predominantly offensive tool that is not only inherently destabilizing and exacerbates the security dilemma, but also omits the diverse ways states operate within the domain. The examination of cyber as statecraft would also benefit from increased coordination between the technology and strategic studies communities. The technical nature of this domain is likely one of the causes of the inattention cyber statecraft has received relative to its importance in the international system. Although still in its infancy as a domain, a cyber statecraft framework will enable more holistic thinking about how actors leverage cyberspace and will ideally open the door for future research at the technology-policy nexus, and thus promote an expanded comprehension of the ways in which this technical disruption affects global affairs. **JFQ**

Notes

[1] Joseph S. Nye, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly 5* (2011), 19.

[2] Jason Healey, ed., A *Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

[3] World Bank, *Information and Communication for Development: Maximizing Mobile* (Washington, DC: The World Bank, 2012).

[4] World Bank, *World Development Indicators* (Washington, DC: The World Bank, 2015), available at <http://data.worldbank.org/products/wdi>.

[5] Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107 (May 2, 2013), available at <http://gking.harvard.edu/files/gking/files/censored.pdf>.