ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey

CYBER STATECRAFT INITIATIVE

Pursuing Cyber Statecraft

> The Atlantic Council's Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of cooperation and conflict in cyberspace through global engagement and thought leadership. The initiative, in partnership with VeriSign, leverages the Atlantic Council's extensive global network of national security practitioners and experts to help create overlapping communities of interest with governments, non-government organizations and others working to solve challenges in cyberspace.
>
> For more information, contact the Director of the initiative Jason Healey at **jhealey@acus.org** or follow his commentary on cyber issues on Twitter at **Jason_Healey**.
>
> The Cyber Statecraft Initiative is generously supported by VeriSign.

If the world is going to solve problems of cooperation and conflict in cyberspace, states and non-state actors alike must apply a wider range of tools. Our experience in this domain is still limited to a few decades – and there are still comparatively few digital natives – so it is not surprising that we have not hit upon the ideal set of concepts and instruments.

Cyber statecraft will be a means to discover and implement these concepts and instruments: some may be new, but many others will be rooted in how states and non-states have solved similar challenges in other domains of society and international relations. Though the US Government has both been pursuing a vision of "21st Century Statecraft" and international cyber engagement, as yet these two concepts have not been comprehensively brought together to describe cyber statecraft. Accordingly, the Atlantic Council's Cyber Statecraft Initiative will bring together the United States and international governments, private sector, academics, think tanks and others to address and solve issues of cyber statecraft. This Issue Paper will begin this process by introducing the idea, summarizing important aspects of it, and outlining the approach for solutions.

Cyber Statecraft

The concept of "cyber statecraft" has not yet been thought of as a strategic approach to securing the cyber domain, but will prove to be decidedly valuable in addressing cyber concerns in the future. Cyberspace has over the course of a few decades become central to the US economy, society, and military. However, this dependence should not be a revelation, as it has been highlighted by each of the last three US administrations. In 2009, President Obama described cyberspace as a "strategic national asset" while six years earlier President Bush characterized it as "the nervous system of [critical] infrastructures—the control system of our country." In 1998, President Clinton noted that our military and economy are "increasingly reliant upon … cyber-based information systems."

Despite this recognition, cyberspace is still poorly understood by both practitioners and policy makers alike. Physically it can be thought of simply as "digital infrastructure" (President Obama) or "interconnected IT" (Bob Gourley). This is not how many of us, especially the younger "digital natives" experience cyberspace, however. Far from still being a "consensual hallucination", as originally described by science fiction author William Gibson in 1984, cyberspace has taken on a unique reality and the US Department of Defense now considers it a separate domain, or territory, similar to air, land, space, or sea.

Among cyberspace's distinguishing features are ease of access, being (somewhat) borderless, and the ease of offense compared to defense, and being predominantly built and used by the private sector. Just like the other domains, though, in cyberspace states must first control their own internal territory (except, of course, in space) then find ways to cooperate internationally. When cooperation fails, they must compete or come into conflict within the bounds of agreed-upon norms. Finding the best path between many hazards is the role of statecraft.

Cyber Statecraft: What is at Stake?

Internet Governance: There is currently a tug of war over the governance of the Internet. Some nations (such as Russia and China) prefer the United Nations to lead, with technical rules similar to those that interconnect phone systems.

However, a one-country, one-vote approach could Balkanize the Internet with each country maintaining its own Internet, just as they run their own phone system – with different rules, standards, tariffs, and taxes. The United States has not supported this approach, backing the existing multi-stakeholder process, where nations have a voice, but so do non-profits, individuals, and companies.

Cyber statecraft should define national interests, help assemble coalitions of like-minded stakeholders, influence others, find compromises where they exist, and leverage where they do not.

Though statecraft has been called "the skillful management of state affairs," a more useful definition is "the art of government and diplomacy." While decisions by and agreements among states must be a central focus, non-state actors play an even more outsize role in cyberspace than in areas of statecraft. In this sense, *statecraft is not just for states anymore*: though government invented cyberspace, corporations, non-profits, multi-stakeholder groups, and individuals have expanded it through content, networks, computers, mobile phones, and countless other devices.

Cyber statecraft then is the overlap between cyberspace and the art of government and diplomacy, especially but not solely for issues of national and international security, and practiced by states and non-states. This broad concept includes both "cyberspace applied to statecraft" as much as "statecraft applied to cyberspace."

"Cyberspace applied to statecraft" would include what President Obama hailed as "unprecedented transparency and accountability and new ways for Americans to participate in their democracy" as information technologies have changed traditional statecraft through global reach, speed of breaking news, ease of communication, and the multiplication of influential actors. To put this into the context of the Department of State's Quadrennial Diplomacy and Development Review, this aspect of cyber statecraft seeks to answer, "How can we do a better job of advancing the interests of the American people *using cyberspace*?" This would include both new, transformative technology and "how we can harness it in service of our diplomatic and development goals" as well as the needed cyber security to protect diplomatic communications, information, and systems.

The **Cyber Statecraft Initiative** will focus on the application of statecraft to cyberspace to foster greater cooperation, find the right amount of national sovereignty of cyberspace, improve governance, establish norms, contain or avoid conflict, and foster international freedom of opinion and expression.

Though the application of cyberspace to statecraft has many fascinating and challenging aspects, the Atlantic Council's future efforts will focus for the time being on the complement: the application of statecraft to cyberspace to foster greater cooperation, find the right amount of national sovereignty of cyberspace, improve governance, establish norms, contain or avoid conflict, and foster international freedom of opinion and expression. This aspect of cyber statecraft seeks to answer "How can we do a better job of advancing the interests of the American people *in cyberspace*?" and encompass what President Obama called "the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy."

Preventing future WikiLeak-style disclosures of diplomatic traffic is "**cyberspace applied to statecraft**."
Responding wisely after any such disclosures is "**statecraft applied to cyberspace**."

Applying Statecraft to Cyberspace

States have generally approached cyber statecraft through one of three traditional approaches, treating these challenges either as (1) a technical hurdle, (2) a cyber crime to be prevented or investigated or prosecuted, or (3) as a field of warfare just in a new domain. Each of these approaches has been generally successful in its own area. However, each is its own clan and there has been little cross flow of trust, information, and ideas between these clans to the detriment of smart policy.

Despite these commonalities, nations have taken very different approaches in their cyber statecraft. For example, in international engagement on cyber issues:

- The **United States** has released an International Cyber Strategy that is perhaps the first national "foreign policy" for the Internet. Previously, the US government had varying (and often competing) agendas in cyberspace: fighting crime, protecting freedom of expression and intellectual property, promoting innovation, preventing attacks, ensuring strong Internet governance and resilience, and enabling military operations. Because there was no overarching vision, the different government departments involved in these agendas were all too often at cross purposes. Rooted in US values like free speech and innovation, the Strategy puts forth a common framework allowing, for the first time, a better balance between all these digital agendas to enable smarter policy making.
- **France** was perhaps the first Western nation to declare sovereign borders for Internet content, forcing Internet companies in 2000 to respect French laws limiting access to Nazi material. The Internet has proven not "impossible" to regulate nationally, as its gurus claimed, but instead it has had to make provision for local laws. France has been using their presidency of the 2011 G8 to get agreement on the best balance of cyberspace regulation and innovation.
- **Australia** has further conceptualized national regulation, making a novel distinction between cyber security (concerned with the confidentiality, integrity, and availability of information and system) and cyber safety (focused on harmful content, such as exposure to illegal and offensive content, cyber-bullying, stalking) while building up their technical perimeter to keep out such "safety" threats.
- Cyber statecraft also must include issues of cooperation and conflict. **Canada** has staked important ground by declaring that, "helping to build cyber security capacity of less developed states and foreign partners will help forestall adversaries from exploiting weak links" in cyber defenses.
- Many nations (especially the United States) would agree with the **United Kingdom** that, "future conflict will see cyber operations conducted in parallel with more conventional actions in the maritime, land, and air environments."

Cyber Statecraft: What is at Stake?

Response to Patriotic Hackers: The term "patriotic hackers" describes those individuals and groups that use malicious cyber activity in support of nationalistic goals. Such attacks can be escalatory, potentially causing the other governments to miscalculate or overreact.

In the late 1990s when the term originated, Chinese patriotic hackers were encouraged by their government to deface or conduct denial of service attacks against webpages in the United States during times of tension, such as after the Belgrade embassy bombing (1999) and the Hainan Island incident (the 2001 EP-3 collision and emergency landing in China).

In contrast, in the lead-up to the Iraq invasion of 2003, the Federal Bureau of Investigation warned US hackers not to become patriotic hackers as "regardless of the motivation … such activity is illegal and punishable by a felony." The US Government does not seem to have made any similar announcements after denial of service attacks disrupted WikiLeaks websites hosting stolen diplomatic cables.

Cyber statecraft should help resolve such issues between nations and offer solutions to deal with both their own nationalistic hackers and those from overseas.

- The **United States, South Korea, Germany, the United Kingdom, and Japan** have all recently created, or will create, new military cyber centers.
- The **Shanghai Cooperation Organization**, comprised of China, Russia, and Central Asian nations, expressed their worry about a "main threat" of the "use of the dominant position in the information space to the detriment of the interest and security of other States … [and] dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States."
- Through the **UN Group of Government Experts** (UNGGE), fifteen nations came together to develop measures to "share best practices, manage incidents, build confidence, reduce risk, and enhance transparency and stability." Though this may sound like an underachievement, the UNGGE had representatives from the United States, United Kingdom, Russia, China, India, Brazil, Belarus, Germany, France, Italy, Estonia, South Africa, South Korea, Qatar, and Israel – the first time such a broad range of countries has agreed on issues of cyber statecraft and a significant step forward.

Cyber Statecraft: The Way Ahead

According to Dennis Ross, diplomat and negotiator, "Statecraft starts with having objectives and being able to match available means to those objectives." Cyber statecraft is a young field and the new U.S. International Cyber Strategy is the first major national effort to attempt to match a broad range of cyberspace objectives. It describes a desired goal of an Internet that is (1) **open** to innovation,(2) **interoperable** the world over, (3) **secure** enough to earn people's trust, and (4) **reliable** enough to support their work. While these are laudable goals, they cannot be an end state.

The innovation, expression and wealth of the Internet flows from a deep well of problems and cyberspace can no more be permanently made safe than can the air, land or sea. Protecting rights, pursuing innovation, and ensuring access for all will be a never-ending challenge, usually technical problem solving but sometimes peace-keeping or warfighting. Accordingly, cyber statecraft must bridge the technical elite of cyberspace – the geeks, who understand current technologies and guide future ones – with national security professionals – the wonks, involved in policies to help nations cooperate and avoid (or prevail in) conflict.

The Levers of Cyber Statecraft

To date there has not been any organized study of the "levers" of cyber statecraft. While other levers (from demarches, restriction of visas, and economic pressure, up to nuclear threats and warfare) are shifting in the larger national security arena, they are still relatively well understood.

In cyberspace, some levers may work exactly the same, but others may work very differently or not at all. There may indeed be some levers that are novel, because of the nature of cyberspace or cyber conflict.

The Cyber Statecraft Initiative has begun a project to help catalogue these levers and think through how the United States and its allies may use them – or how they may be used against us.

To "match available means" to these objectives, the United States government has started to increasingly resource its cyberspace efforts, such as recent diplomatic pushes for Internet freedom, or the funding increases as part of the Comprehensive National Cybersecurity Initiative. Other nations have been following suit and in some cases (such as Estonia) seem to be well ahead of the United States .

Over the remainder of 2011, expect increasing national attention to cyber statecraft with norms at center stage. Efforts will focus on "a more comprehensive, structured dialogue … to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace" in the words of William Hague, the UK Foreign Secretary, who will host a conference in November.

Only a few years ago, a discussion on "foreign policy for the Internet" would have generally gotten blank stares whereas now it is a topic for foreign ministers, presidents and prime ministers and G-8 summits. Cyber statecraft is becoming not just respectable but recognized as critical. Hopefully, the current mood will last, as nations are defining goals, starting to match them with resources, and seemingly in a mood to discuss areas of common interest.

August 2011