Cyber offensive measures, such as North Korea’s Sony hack and Russian interference in our elections, have received a growing amount of attention in recent years. So have cyber defensive and cybersecurity measures, with countries growing increasingly concerned about their resilience to online threats. But between offense and defense sits another, less-recognized tool of modern statecraft: cyber diplomacy.

What Is Cyber Diplomacy?

Diplomacy in general can be defined as “the attempt to adjust conflicting interests by negotiation and compromise,” write academics André Barrinha and Thomas Renard. They note that diplomacy could once be thought of as “an activity solely undertaken by a select group of (mostly) white men elegantly discussing and negotiating the main issues in international politics in cocktail parties and at official receptions.” One of the ways in which today’s diplomacy looks quite different is the range of topics it touches—including cyber diplomacy.

Cyber diplomacy, according to Barrinha and Renard, is “the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace.” Countries have come to recognize that diplomacy can further a wide range of such interests, including “cybersecurity, cybercrime, confidence-building, internet freedom and internet governance.” It is important to note that cyber diplomacy does not refer to the use of online tools to conduct diplomacy on other topics—such as a virtual embassy or a state-run social media account posting about climate change—but rather diplomacy centered on cyberspace. Across topics and actors, the core goal of cyber diplomacy is to craft shared international norms and channels of cooperation, moving cyberspace beyond its Wild West days.

Diplomacy is traditionally thought of as an exercise carried out by government officials. But in cyber diplomacy, as in diplomacy on other topics, the set of influential actors has broadened substantially in recent years. Official diplomats retain a central role, of course. Starting with the United States in 2011, countries have issued cyber-focused foreign policy plans and created new offices and diplomatic jobs addressing these pressing issues. These offices, like the U.S. Office of the Coordinator for Cyber Issues, are key players in cyber diplomacy. International bodies like the United Nations and European Union have joined the effort, as have non-state actors like technology companies, security firms, technical experts, and civil society groups. Journalists and academics also offer important contributions to cyber diplomacy, helping the international community gather information on what countries around the world are doing and enabling us to understand the best path forward.

Bridging the divide between these groups will be key to any successful cyber diplomacy effort. However, doing so is not always easy. Officials have continued to express skepticism that international cyberspace norms exist, disregarding multilateral efforts to create such norms. Governments are often reluctant to share information with outsiders, such as tech companies they do not trust, journalists reporting on cyberattacks, or academics researching the topic. And tech
companies are oftentimes reluctant to share information with governments, citing privacy concerns.

The U.S. State Department’s Office of the Coordinator for Cyber Issues has articulated two main national cyber diplomacy goals: “(1) to promote acceptance and adherence to the U.S.–developed framework of responsible state behavior in cyberspace, and (2) to advance an open, interoperable, reliable, and secure cyberspace that benefits U.S. interests and promotes U.S. values.” This paper takes those two broad categories as starting points for its discussion of the key topics in cyber diplomacy. Both topics are critical: without a shared set of behavioral norms, nations will continue to experience cyberattacks that harm their economies and governments; and without a stable, open governance structure, nations cannot reliably share in the benefits cyberspace has to offer. Cyber diplomacy is central to both.

State Behavior in Cyberspace

Current State of Affairs

One of states’ top goals in cyber diplomacy efforts has been to establish a set of shared norms and values governing behavior in cyberspace, particularly with regard to cyberattacks, electronic espionage, and other forms of cybercrime. Cyberattacks threaten every component of society, from critical infrastructure and business to elections and health care. While many attacks come from non-state actors, or cannot be accurately attributed, state-sponsored cybercrime is also a pressing issue. Consider two massive 2017 cyberattacks: WannaCry, a North Korean-sponsored ransomware attack that cost $4 to $8 billion in global economic damage by shutting down critical computer systems, and NotPetya, a ransomware attack attributed to Russia that targeted Ukraine and spread globally, leaving $10 billion in damage. Cyber espionage has also been a problem, with intellectual property (IP) theft costing the U.S. economy hundreds of billions of dollars annually. For example, China has long sought to advance its economy by stealing trade secrets and IP from U.S. companies in sectors like AI, aerospace, and national defense—an effort Chinese hackers have continued even during the coronavirus pandemic. Without cooperation between states and strong norms to constrain this type of behavior, international peace, security, and prosperity will continue to suffer.

There have been some successful cyber diplomacy efforts to date. One 2017 report counted eighty-four overall cyber diplomacy initiatives around the world, including five multilateral treaties, twenty-four initiatives by regional organizations, eight private-sector initiatives, and seven academic initiatives. Bilateral agreements have been moderately successful. The United States and China signed a landmark cybersecurity agreement in 2015 that significantly reduced China’s cyber theft of U.S. trade secrets and IP. However, the agreement has all but broken down. China soon thereafter signed a similar deal with the United Kingdom and accepted the G20’s norm against cyber-enabled IP theft. Cyber dialogues have cropped up across the world, often focusing on state behavior in cyberspace.

International organizations have also undertaken efforts aimed at restraining cyber offensive measures. The U.N. Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), founded
in 2004, is one such consensus-building effort. The UN GGE’s 2013 report stated that international law, including the U.N. Charter, applies in cyberspace. Its 2015 report recommended eleven “voluntary, non-binding norms of responsible State behavior” in cyberspace, such as not attacking critical infrastructure. While these norms still need to be developed and implemented, the UN GGE reports mark significant milestones. The 2016-17 UN GGE failed to reach consensus, but another convened last year and will last until 2021. The European Union has also been active in cyber diplomacy efforts.

In the private sector, technology companies have joined the conversation. For example, Microsoft has called for a non-governmental International Cyberattack Attribution Organization. The group would bring companies together in attributing and responding to cyberattacks. Microsoft has also called for a Digital Geneva Convention that would “commit governments to protecting civilians from nation-state attacks in times of peace.” And Microsoft has criticized governments for “hoarding” vulnerabilities instead of alerting companies so they can fix them before an attack occurs, which Microsoft said happened when the NSA failed to warn it of the vulnerability that enabled the 2017 WannaCry attack.

Academic institutions and civil-society organizations have also paid increasing attention to diplomacy’s role in shaping behavior in cyberspace. Perhaps most notably, the 2017 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations identifies 154 black-letter rules governing states’ rights and obligations. Journalists, bloggers, and security researchers have helped bring secretive events and groups to light, filling in the large gaps in publicly available information.

Bridging the Divide

Increased collaboration between civil society, government, academia, and the private sector would be highly beneficial for efforts to promote responsible state behavior in cyberspace. Take, for example, one of the larger challenges facing cyber diplomacy efforts: cyberattack attribution. Because hackers disguise themselves, it can be hard to discover who was responsible for a given attack and whether a state was involved, although technical detection tools have improved. Yet even when one state does suspect that a government-sponsored group was behind an attack, it may be reluctant to say so publicly. The risks of escalating conflict and straining diplomatic relations may be too high. And states may be unwilling to share sensitive evidence with companies or other states seeking to make attributions of their own. As the U.S. State Department acknowledges, these challenges have “made international or public-private cooperation to respond to specific threats more challenging.” For example, the FBI did not share the data supporting its attribution that North Korea was behind the Sony hack, and one private security firm even disagreed with the agency’s conclusion. Further, there is little international legal framework to govern attribution-making or set consequences for perpetrators, although the European Union has given thought to a sanctions regime. Greater international and public-private cooperation will help states accurately attribute and respond to attacks, and more effectively deter potential perpetrators. With this cyberspace issue and others, involving people across sectors and nations will be important to creating shared rules of the road.
Internet Governance

Current State of Affairs

Internet governance can be approached from two discrete, yet interrelated frames. The first frame focuses on technical governance of the Internet: Who should operate the sub-oceanic fiberoptic internet cables? Who should decide how IP addresses are handed out? Who should regulate top-level domains? The second frame looks to policy governance of the Internet and how important normative questions should be decided: Should online hate speech be regulated? Should retributive cyberattacks be punished? Should messaging platforms have backdoors for law enforcement officials? Of course, these two views of internet governance oftentimes converge. Net neutrality, for example, concerns both technical (ownership of internet cables) and policy (whether ISPs should be allowed to prioritize certain content) internet governance questions.

The United Nations has adopted the policy frame, defining internet governance as “the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.” The United States, on the other hand, has adopted the technical frame, restricting its understanding of internet governance to “largely technical questions.”

No matter which framework you adopt, internet governance is a thorny and contentious issue. For decades, countries around the world complained of American hegemony in controlling the Internet. These assertions were rooted in history: the Internet was created by the U.S. military in the ‘60s and ‘70s, and by the time the World Wide Web was developed by Tim Berners-Lee at the end of the Cold War, the United States stood as the world’s sole superpower. Naturally, the United States has had a unique role in maintaining the Internet. Even so, the United States does not “govern” the Internet.

The reality is that there is no central body that governs the Internet. Instead, there are a set of organizations—some comprised solely of either governments or private parties, others a mixture of both governments and private parties—that govern different aspects of the Internet. Yet by way of necessity, the technical governance of the Internet is much more centralized than the policy governance of the Internet.

Three of the most important technical internet governance bodies are the Internet Corporation for Assigned Names and Numbers (ICANN), described in detail below, the Internet Engineering Task Force (IETF), which standardizes internet protocols, and the World Wide Web Consortium (W3C), which standardizes world wide web protocols. These three organizations are responsible for most of the technical governing of the Internet. However, chief among them is ICANN. If one had to select the single most vital organization that helps run the Internet, it would be ICANN.

ICANN is important because it manages the Internet’s Domain Name System (DNS). The DNS is “often referred to as ‘the phone book of the Internet’ because it matches domain names with appropriate IP address numbers.” This allows for interoperability and is why typing
ICANN has had a short, yet controversial, history. It was started in 1998 by the U.S. Department of Commerce, and for most of its history was under the auspices of the U.S. government. Other countries were bothered that the United States held sizeable control over such a vital organ of the Internet, and pushed for global management of ICANN. For sixteen years, however, the United States refused to budge. And then, in June 2013, Edward Snowden released his first batch of leaks. These leaks engendered more distrust of U.S. control over ICANN and led to the heads of the major internet governance bodies jointly issuing the Montevideo Statement. The Statement called for “accelerating the globalization of ICANN” and emphasized the need for “multistakeholder Internet cooperation.” In response to these changing circumstances, the Obama Administration announced it would formally cede control of ICANN and initiated a two-year transition period to do so. On October 1, 2016, ICANN officially became a private organization.

As described above, the technical governance of the Internet is robust and organized. On the other hand, policy governance of the Internet is nowhere near as developed and is much more ad hoc. Moreover, there is no international body in this sphere with the power to issue binding decisions. Instead, the normative decisionmaking in this realm virtually always happens at the nation-state level. This has led to the development of fragmented “Internet rules” that differ country-by-country. There have been some attempts to describe and harmonize an international legal regime, most notably with the Tallinn Manual 2.0, mentioned above. However, the Tallinn Manual is the effort of private experts and thus has no binding effect on states.

The main international actor in this area is the Internet Governance Forum (IGF), an annual conference organized by the United Nations. The IGF started in 2005 out of a working group that established broad principles of internet governance. However, the IGF is nowhere near as powerful as its counterparts on the technical side of the internet governance framework. It has no executory power, and instead serves as a venue for vested stakeholders to discuss the latest issues in internet governance. In 2018, France used the annual IGF meeting to issue one of the most ambitious policy governance declarations in years: the Paris Call for Trust and Security in Cyberspace. The Paris Call aimed to establish ground rules for how state and non-state actors could interact with each other in cyberspace. Importantly, it imported “international law . . . international humanitarian law[,] and customary international law” into policy internet governance. As a reflection on the multistakeholder approach to internet governance, tech companies like Microsoft, Google, and Facebook all signed on the Call. Notably absent from the list of signees? The United States. And it was not the only one conspicuously absent: Israel, Iran, and China all refused to sign on to the Paris Call as well.

Overall, the technical governance of the Internet is both efficient and effective, but policy governance of the Internet is not.
ICANN prides itself on being a model for internet governance. It follows a multistakeholder approach, with representatives from the private sector, government, academia, and civil society all afforded a seat at the table. Undoubtedly, one of the strengths of internet governance is that the space is not dominated by governments. This is no accident: in the face of attempted government control over the Internet, the United States has been a fierce advocate for the private sector and other stakeholders. The Tunis Agenda for the Information Society of 2005, in which the United Nations first laid out principles of internet governance, affirmed that:

the international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. [Internet governance] should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet . . . .

In addition to international advocacy, in recent years technology firms have taken a leading role in establishing self-regulating internet governance norms. Microsoft has been a leader in this effort. In 2018, the company published principles to guide facial recognition technology, and challenged its peers to follow in its footsteps. Facebook has also been making strides in internet governance. In an unprecedented move, Mark Zuckerberg announced that Facebook will establish a quasi-independent Oversight Board to govern content moderation decisions. With just under 2.5 billion monthly active users on its main website, and over a billion monthly active users on each of WhatsApp, Messenger, and Instagram, the Oversight Board will be the first major “traditional” governmental institution ported to the Internet. Depending on how successful the Oversight Board is, it could usher in a new era of internet governance. This presents a prime opportunity for academia, civil society, the private sector, and government to work together to shape the future.

* * *

Cyber diplomacy presents both risks and rewards. In a world that has become premised on the Internet, it is vital that cyber diplomacy continues to grow and establish norms for the future. Coming technological advances, including blockchain, quantum computing, and deepfakes, just to name a few, will present serious foreign policy issues. By working across the public-private divide, and including stakeholders from across different fields, cyber diplomacy can make cyberspace a responsible and innovate environment for all.

Suggested Readings


