Cyber Diplomacy: Benefits, Developments, and Challenges

Dana Khabbaz, YLS ‘21

As dependence on the internet and computer technology grows, state interests further intertwine with the realm of cyberspace. Cyber diplomacy can serve as an important tool through which states can cooperate to set cyber norms and respond to cyber threats and vulnerabilities. To take full advantage of this tool, however, states must embrace cyber diplomacy, integrate it into their bureaucratic structures, and work to overcome the novel challenges it poses.

This paper begins by providing an overview of cyber diplomacy and highlighting the need for its use. Then, the paper outlines major international cyber diplomacy efforts. This paper next summarizes recent U.S. developments. Here, the United States serves as a case study of one state’s internal cyber diplomacy changes. The United States wields considerable influence on international law and has sometimes advocated in favor of cyber diplomacy. At the same time, the United States has occasionally served as an obstacle to cyber diplomacy progress and has struggled to integrate cyber diplomacy into its foreign policy. After the discussion of U.S. developments, the paper concludes by identifying seven key challenges to cyber diplomacy.

What is “Cyber Diplomacy”?

Cyber diplomacy is diplomacy “to secure national interests with regard to the cyberspace.” As a practice, cyber diplomacy is the natural response to the increasing global relevance of cyberspace. Through cyber diplomacy, states collaborate to respond to and addresses the cyber dimensions of international conflicts, crime, and information security.

A recent example of cyber diplomacy is the United States’ preparations for the release of 5G technology. In advance of its release, the United States has been engaged in cooperation with other states—primarily with European countries but also through the World Radiocommunications Conference in Egypt. Additionally, in its “National Strategy to Secure 5G,” released in March 2020, the United States called for adopting the “5G security principles” outlined in the 2019 Prague 5G Security Conference’s “Prague Proposals.” The strategy advanced a plan to coordinate with foreign states and private actors to protect 5G competition and transparency. Finally, Congress also passed the Secure 5G and Beyond Act in March 2020, which, among other things, requires the President to engage in cyber diplomacy.

Cyber diplomacy also came into the spotlight during tensions between China and the United States in 2015, after the United States accused Chinese hackers of cyberattacking and stealing data from the U.S. Office of Personnel Management. In resolving the matter, the two states engaged in cyber diplomacy. They agreed that neither would “conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business for commercial advantage.” The two also agreed to “work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace.”

The Need for Cyber Diplomacy
By its nature, cyberspace is decentralized and largely ungoverned. André Barrinha and Thomas Renard have compared it to “the high seas, airspace, and outer space.” Diplomacy is central to the use of any “global common,” including cyberspace. Acts over cyberspace, including cyber attacks, are frequently transnational in scope and thus may mandate a transnational response. To respond to “cross-national cyber-attacks,” for example, states must cooperate in “information sharing, evidence collection, and criminal prosecution” of attack perpetrators. Indeed, no state can singlehandedly protect itself against cyber threats.

Not only is cyber diplomacy critical to effective international responses to cyber threats, but states also need to engage in diplomacy to develop the norms that then govern these international collaborations. As cyberspace’s use and relevance continues to grow, states face a dearth of established standards governing cyberspace interactions and responses to cyber-related events. In this sense cyber law differs substantially from, for example, centuries-old laws governing the high seas. While some norms already exist in cyberspace, cyber-norm creation is ongoing, and international diplomacy can be critical in shaping the process.

Finally, cyber diplomacy is not only a necessity but also an opportunity. Cyberspace provides yet another venue for global interconnectedness. Cyber diplomacy can intersect with diplomacy of other subject matters and has implications for other issues of global importance, such as international human rights, public health, and climate change.

International Cyber Diplomacy Efforts

International cyber agreements have been sparse, and many cyber agreements have been bilateral or regional. Nevertheless, cyber resolutions, agreements, and even controversy can be evidence of states engaging in the practice of cyber diplomacy.

In 2004, the UN General Assembly established the “UN Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security” (UNGGE). The UNGGE was first proposed by Russia in 1998 in a resolution to the General Assembly. Since 2004, the UNGGE has released three nonbinding reports: one in 2010, one in 2013, and one in 2015.

The UNGGE’s most recent report, released in July 2015, discussed the adoption of international cyber norms and international cooperation on information and communications technology (ICTs). The report also called for states to use ICTs in accordance with their “[e]xisting obligations under international law.” In December 2015, the General Assembly adopted a resolution that affirmed the report and called upon UN member states “to be guided in their use of information and communications technologies by the 2015 report.”

UNGGE negotiations failed during a June 2017 session of the group. Russia, China, and Cuba expressed disagreement over the applicability of the UN Charter to cyberspace, provisions of which would allow a state to retaliate in self-defense to a cyber attack. In response, the U.S. representative criticized those governments for opposing accountability in cyberspace.

In September 2019, 26 countries signed a joint statement at the UN General Assembly on norms of cyberspace. The signatories, including the United States, were primarily European
countries and U.S. allies. In the resolution, the signatories referred to themselves as “responsible states that uphold the international rules-based order” and called for “greater accountability and stability in cyberspace.” The resolution also asserted the states’ commitment to the agreements of the UNGGE.

In December 2018, the UN Secretary-General established a new iteration of the UNGGE, the “Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.” This new group is U.S.-led and includes 25 countries. It convened for the first time in December 2019, and it will submit its final report to the General Assembly in 2021.

Also in December 2018, the General Assembly created the Open-Ended Working Group (OEWG), which met for the first time in June 2019. The Russian-led OEWG is open to all UN member states. The group is developing a report on ICTs and international security to be presented to the General Assembly in 2020.

The UN has undertaken other cyber diplomacy efforts in addition to the UNGGE and OEWG. In December 2018, the UN General Assembly adopted a resolution to “[c]ounter[] the use of information and communications technologies for criminal purposes.” The resolution was advanced by Russia, and it required the UN Secretary General to “seek the views of Member States” on challenges they face related to cybercrime. In addition, the resolution set cybercrime on the UN General Assembly’s agenda.

In December 2019, the UN General Assembly passed another Russian-led resolution on cybercrime. The resolution called for the creation of a committee of experts to develop a new international cybercrime treaty. In a blog post, Joyce Hakmeh and Allison Peters characterized Russia’s involvement in the resolution as part of Russia’s efforts to supplant the Budapest Convention on Cybercrime.

States have also organized cyber diplomacy efforts outside the United Nations. In 2001, the Council of Europe’s Committee of Experts on Crime in Cyber-space drafted an international treaty called the Budapest Convention on Cybercrime. The Convention was “the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security.” The treaty’s principle goal was to achieve a “common criminal policy” for cybercrime. To date, 65 states have ratified the treaty and 68 have signed it. Just over half of the treaty’s parties are European states, but several non-European states are also parties. In 2003, the Council released the Additional Protocol to the Convention of Cybercrime, which concerned “the criminalization of acts of a racist and xenophobic nature committed through computer systems.” The Additional Protocol was ratified by 32 states and signed by 45. Negotiations for the Budapest Convention’s Second Additional Protocol began in 2017.

In February 2015, the European Union adopted the Council Conclusions on Cyber Diplomacy. These Conclusions called for diverse cyber cooperation, including for human rights promotion, capacity building, internet governance, and criminal prosecutions. According to
André Barrinha and Thomas Renard, the Conclusions were the “first time the term ‘cyber-diplomacy’ was used in such an official government document.”

**U.S. Government and Cyber Diplomacy: Recent Developments**

As a state that wields substantial influence in international diplomacy, the United States serves as an illustrative case study of the complicated intra-state dynamics that impact cyber diplomacy. In the last few years, the U.S. government has undertaken several cyber diplomacy efforts in addition to its 5G technology strategy and its negotiations with China. These including the release of reports and proposals to reform and advance U.S. cyber diplomacy. The United States has by no means readily embraced cyber diplomacy, however. The Trump Administration has removed key cyber diplomacy positions from the State Department, and Congress has yet to pass comprehensive cyber diplomacy legislation.

In April 2016, then-President Obama formed a Commission on Enhancing National Cybersecurity. The Commission released a report in December 2016, which, among other things, called for greater cyber diplomacy and international engagement. The report also recommended the appointment of an “Ambassador for Cybersecurity” to lead cyber diplomacy.

Instead of adopting the report’s recommendation, in August 2017, then-Secretary of State Rex Tillerson eliminated the State Department Cyber Coordinator Office. The responsibilities of the role then transferred to Deputy Assistant Secretary of State Robert Strayer, who expressed optimism about achieving international cyber diplomacy agreements.

John Bolton, then-National Security Advisor to President Trump, also removed the role of cybersecurity coordinator from the National Security Council in May 2018. The responsibilities of the cybersecurity coordinator were redistributed among two other members of the National Security Council.

In July 2018, Secretary Pompeo announced the creation of the Digital Connectivity and Cybersecurity Partnership, through which the United States would assist other states with their cyber infrastructure. As of January 2020, the United States has committed to $51 million in cyber assistance to the Indo-Pacific region and $10 million to Latin America.

The White House released its “National Cyber Strategy” in September 2018. The Strategy stated that “[c]yberspace will no longer be treated as a separate category of policy or activity disjointed from other elements of national power.” Among many outlined goals, the Strategy called for “encourage[ing] universal adherence to cyber norms,” “build[ing] a cyber deterrence initiative,” and “counter[ing] malign cyber influence and information operations.” The Strategy incorporated cyber diplomacy with international partners into the three plans.

Also in September 2018, the Department of Defense released a Cyber Strategy that outlined three primary goals as part of its “strategic competition in cyberspace.” Its third goal called for the Department of Defense to “work with U.S. allies and partners to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing in order to advance . . . mutual interests.” The strategy also affirmed U.S. adherence to the UNGGE.
In June 2019, the State Department proposed creating a Bureau of Cyberspace Security and Emerging Technologies, which would be led by a coordinator with status comparable to an assistant secretary of state. The bureau would “lead U.S. government diplomatic efforts to secure cyberspace and its technologies, reduce the likelihood of cyber conflict, and prevail in strategic cyber competition.”

Congress has also been active in promoting cyber diplomacy in the last couple of years. In its 115th session (from January 2017 to January 2019), Congress introduced “226 pieces of legislation that primarily or tangentially focused on cybersecurity” and signed ten of those bills into law. Half of the introduced legislation and all of the bills that became law had bipartisan support. Of these legislation, Ishan Mehta and Jayati Dev categorize 26 as primarily relating to “foreign policy.”

While these numbers reflect a growing congressional interest in cyber diplomacy, efforts to pass comprehensive cyber diplomacy legislation have been less successful. In 2017, bipartisan legislators introduced the Cyber Diplomacy Act of 2017. The bill proposed creating an “Office of Cyber Issues” in the Department of State, headed by an official with ambassadorial rank. The bill was passed by the House and approved by the Senate Foreign Relations Committee, but never progressed further. Two years later, the House introduced a 2019 iteration of the Cyber Diplomacy Act. The new Act calls for establishing an Office of International Cyberspace Policy. The Office would be led by an official who would report either to the Secretary of State or Deputy Secretary of State. The 2019 Cyber Diplomacy Act remains under consideration in the House.

In Spring 2019, Congress convened a cyberspace “Solarium” commission—inspired by Eisenhower’s 1953 Solarium effort—to investigate cyber deterrence, persistent engagement, and international agreement. The congressional commission consisted of 14 members, including several bipartisan legislators, private stakeholders, as well as then-Acting Deputy Secretary of Defense David Norquist, then-Acting Deputy Secretary of Homeland Security David Pekoske, then-Deputy Director of National Intelligence Susan Gordon, and FBI Director Chris Wray.

The Cyberspace Solarium Commission released its report in March 2020. The report advocated for “layered cyber deterrence” to reduce the “probability and impact of cyber attacks.” The report outlined several recommendations. To “Shape Behavior,” the report recommended establishing an Assistant Secretary of State who leads a new Bureau of Cyberspace Security and Emerging Technologies. The report advised leveraging “non-military tools” to “build[] a coalition” and “persuade” other states to collaborate on developing international cyber standards. Internationally, the report also recommended “streamlining the Mutual Legal Assistance Treaty and Mutual Legal Assistance Agreement process and increasing the number of FBI Cyber Assistant Legal Attachés.” The report also proposed domestic congressional and bureaucratic reforms, including instituting permanent congressional committees on cybersecurity and establishing a National Cyber Director who advises the President on cybersecurity and coordinates cybersecurity policy.

Key Challenges
Cyber diplomacy poses numerous challenges for states, many of which intersect law, policy, politics, and technology. These challenges include (1) some states’ unwillingness to participate in cyber diplomacy; (2) the issue of attribution in cyberspace; (3) the rapid pace at which cyber diplomacy is developing; (4) political divisions among states; (5) gaps in states’ technological capacities; (6) cyber diplomacy’s overlap with other fields; and (7) the difficulty of safeguarding nonstate actors’ cyber interests.

**Challenge 1: States’ Reluctance to Engage in Cyber Diplomacy**

Like other forms of diplomacy, cyber diplomacy can only succeed if states are willing to cooperate. Unfortunately, states do not always view cyber diplomacy and the establishment of clear cyber norms as aligned with their interests. For example, the U.S. government has resisted prioritizing cyber diplomacy. Internally, it has eliminated a key cyber position in the State Department. Internationally, the United States has clashed with other states over its desire to recognize a self-defense right in cyberspace, which would justify military retaliation in response to cyber attacks. These disagreements ended negotiations at the 2017 session of the UNGGE. Thus, successful cyber diplomacy can prove difficult if states do not prioritize the process or view it as beneficial.

**Challenge 2: Attribution and Deterrence**

States’ reluctance to view cyber diplomacy as advantageous relates directly to the problem of attribution. Attribution is a persistent obstacle in cyber law, and the problem of attribution impacts the efficacy of cyber diplomacy. In cyberspace, acts cannot always be traced back to actors. Attribution not only makes international cyber law “difficult to apply,” but it also “means that the reasons why actors tend to adhere to international law are weakened, and . . . the transition from informal international norms to customary law may be much slower than otherwise expected.” In addition, modern international law is often enforced by holding actors accountable, including through use of countermeasures. Without attribution, some of these methods of accountability become difficult.

Deterrence is not altogether impossible without attribution, however. Joseph Nye suggests four principle methods of deterrence in cyberspace: “threat of punishment, denial by defense, entanglement, and normative taboos.” While threat of punishment may rely on attribution, the latter three methods do not. In “denial by defense,” states bolster their defenses to cyber attacks, “reduc[ing] the incentive for some attacks by making them look futile.” Deterrence by “entanglement” refers to states’ “interdependence” in cyberspace, which means “successful attack[s] simultaneously impose serious costs” on the attacking state. Finally, “normative taboos” refer to the “reputational costs” states may incur when violating international cyber norms. In these three deterrence methods—denial, entanglement, and norms—cyber diplomacy has the potential to succeed, even without attribution.

The difficulty of attribution poses several possible consequences for cyber diplomacy. On one hand, without clear attribution, states may have an “expectation that by avoiding conclusive attribution, they could also satisfy other foreign policy interests without cost.” Thus, the perceived benefits of using cyberspace’s anonymity offensively may lead some states to disfavor
defensive cyber laws. On the negotiating front, these conflicting state interests can make cybersecurity agreements difficult. On the other hand, the uncertainty of cyberspace may motivate states to engage in cyber diplomacy. In fact, these “challenges” of cyberspace attribution “have been a catalyst for considerable progress in negotiations over norms of state behaviour.”

**Challenge 3: Rapid Evolution**

Much of cyber diplomacy is developing in reaction to new conflicts and threats. Cyber technology is also developing at a rapid pace, making it difficult for states to proactively address issues before they emerge. In some ways there is “an element of learning involved” in states and groups adapting to the changing conditions of the cyber age.

In addition to the inherent challenges associated with such a rapidly-evolving field, cyber diplomacy’s novelty also exacerbates political tugs-of-war. Any form of diplomacy necessarily deals with political tensions and alliances. However, in cyber diplomacy, laws and norms underlying the diplomacy are not as established. As a result, states battle not only over cyber resources and rights, but also over the ability to construct the very standards that govern cyberspace. This tug-of-war explains, for example, the Russian push for a UN cybersecurity agreement in place of the European-written Budapest Convention.

**Challenge 4: Political Divides**

While cyber diplomacy can strengthen cooperation among allied states, it may also exacerbate divisions among other states. For example, U.S. actors have already signaled a desire to partner with “a community of like-minded states” to shape cyber norms. This category may exclude weak states not aligned with the United States, as well as U.S. competitors like Russia. Tensions over these alliances came to a head during UN cyber negotiations in the summer of 2017, where talks over laws governing cyber attacks failed along Cold-War lines.

**Challenge 5: Gaps in State Cyber Capacities**

International law has developed over time largely through customary state practices and by treaties. Since cyber law is more recent, present-day diplomatic decisions may create future cyber law’s foundation. However, cyber diplomacy has a high barrier to entry—in practice, only states with sufficient technology, budget, and institutional capacity can engage in cyber diplomacy. This reality means that poorer or technologically weaker states may be left out of cyber-law creation, and the body of cyber law that emerges may center the priorities of wealthier, more powerful states. This inequality already exists in the Eurocentric, colonial origins of modern international law, and some critics challenge the legitimacy of international law on these grounds. If these inequalities persist in cyber-law formation, cyber law may fall vulnerable to similar criticism.

**Challenge 6: Intersectionality**

Cyberspace is not a standalone system—the digitization of government operations intersects cyberspace with many other traditional state interests. For example, cybersecurity is
now essential for defense and national security, and cyber negotiations can substantially impact domestic economic interests. As a result, states must conduct cyber diplomacy in concert with other forms of diplomacy. This interconnectedness has implications for states’ bureaucratic structures. Cyber diplomacy’s growing relevance may mandate specially-designated roles and offices, such as those proposed for the United States in Congress’s Cyber Diplomacy Act. On the other hand, those positions cannot be so siloed so as to disrupt their coordination with other bureaucratic actors.

**Challenge 7: Preserving the Interests of Nonstate Actors**

Cyber diplomacy may carry drawbacks too. Presently, private actors and nonstate groups, including businesses, political dissidents, and minority groups, may enjoy the freedom of an underregulated cyberspace. This underregulation, to some, means liberty and safety. However, the “diplomacy” in cyber diplomacy makes it interstate by its very nature. Negotiations exclusively among states may result in the overprioritization of state-based interests like prosecuting cybercrimes—potentially at the expense of other interests like internet freedom. Without active collaboration among public and private interests, cyber diplomacy runs the risk of trampling on the most critical advantages cyberspace poses for nonstate actors.

The United States is one state that has begun recognizing this tension. Currently, the United States collaborates with the private sector on cyber matters and has expressed its prioritization of internet freedom. In addition, a recent congressional report articulated a vision of cybersecurity that seeks to protect internet freedom and safeguard private actors from surveillance.

**Suggested Background Readings**


