TOWARDS EFFECTIVE CYBER DIPLOMACY:

A GUIDE TO BEST PRACTICES AND CAPACITY BUILDING

ABOUT THE CYBERSECURITY TECH ACCORD

Founded in 2018, the Cybersecurity Tech Accord is a coalition of over 150 global technology firms committed to advancing trust and security in cyberspace. As an organization, we firmly believe that protecting the online environment is in everyone's interest and that industry, governments and civil society all have a role to play in achieving that.

Therefore we – as enterprises that create and operate online technologies – promise to defend and advance its benefits for society. Moreover, we commit to act responsibly, to protect and empower our users and customers, and thereby to improve the security, stability, and resilience of cyberspace. We uphold those core values through four principles:

1. WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE.

- We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.
- We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

2. WE WILL OPPOSE CYBERATTACKS ON INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE.

- We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.
- We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

3. WE WILL HELP EMPOWER USERS, CUSTOMERS AND DEVELOPERS TO STRENGTHEN CYBERSECURITY PROTECTION.

- We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.
- We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

4. WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY.

- We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.
- We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.

In many countries around the world, October is celebrated as Cybersecurity Awareness Month, an opportunity to reflect on and improve both individual and organizational cybersecurity and resilience. To honor the occasion, we have developed this guide on cyber diplomacy to showcase good practices that we have observed in our interactions with governments around the world over the last three and a half years. Digital technology connects us all, and consequently, cybersecurity is a borderless and global challenge. As a result, effective cyber diplomacy is essential to the security of our shared online environment and will only grow in importance in years to come. We hope that as increasing numbers of governments – and other stakeholders - invest in having dedicated teams to address this critical issue and engage in international dialogues and processes, together we can advance peace, security and stability in cyberspace.

Contents

Cybersecurity at the heart of national security

Regardless of where you are in the world, the online environment has likely become fundamental to many aspects of your life. This is as true for countries as it is for individuals. While information and communication technologies (ICTs) afford innumerable new opportunities for states and their citizens related to development and innovation, cyberspace also poses significant risks to states that span criminal activity, espionage and influence operations, and even cyberwar.[1] Undeniably, these technologies, and attacks against them, have become core tools of modern geopolitics, critical to national interests.

The COVID-19 pandemic has only accelerated the use of cyberattacks as a low-cost, high-reward means to seek sensitive information and financial gain, with both cybercriminals and state actors exploiting the vulnerabilities stemming from increased reliance of society, business, and individuals on technology. These threats have become increasingly sophisticated in recent years, and the range of targets has expanded over time to include government agencies, critical infrastructure, healthcare entities and entire supply chains.

The range and importance of these risks and rewards mean that states must identify their interests and values in cyberspace and develop strategies to pursue them at the national level. At the same time, it also means they need to invest in protecting their online environment, to not only ensure the resilience of government institutions, but critical infrastructure sectors, and the economy more broadly. From a national security perspective, states therefore have at least three broad options for protecting against these new-age threats: *defense*, *deterrence*, and *diplomacy.*[2]

Improving cybersecurity by bolstering defenses is fortunately an increasingly common response to cyber threats. Governments around the world have prioritized identifying and protecting their critical infrastructures in particular. The second option – *deterrence* – builds on defense and involves mechanisms that discourage unwanted activity by other actors. Deterrence may occur either by denial (e.g., via effective cybersecurity defenses that discourage attack) or by punishment (e.g., via credible threats of retaliation). The source of these consequences may be within the cyber domain or in other domains, such as economic sanctions or domestic prosecutions.

Alongside defense and deterrence, a number of states have invested in diplomatic methods to advance their interests and values in cyberspace – the subject of this paper. To date, however, only a select group of states have dedicated cyber diplomacy resources and this is therefore a fairly new field. It is our view that it is in the interest of *all* states' to stand up, train, and deploy diplomatic resources to advance their values and interests in cyberspace and we hope that the suggestions captured in this paper can help guide those efforts and engagements.

[1] Martha Finnemore and Duncan Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 432-36. https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf

[2] Madeline Carr, "Cyberspace and International Order," in *The Anarchical Society at 40: Contemporary Challenges and Prospects*, eds. Hideki Suganami, Madeline Carr, and Adam Humphreys (Oxford: Oxford University Press, 2017), 166-68; Sico van der Meer, "Defense, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity," in *Securing Cyberspace: International and Asian Perspectives*, eds. Cherian Samuel and Munish Sharma (New Delhi: Pentagon Press, 2016), 95.

What is cyber diplomacy?

As indicated above, cyber diplomacy, or "digital diplomacy," is a fairly new field and therefore a sometimes misunderstood term. With that in mind, we will put forward a definition to help anchor the recommendations of this paper. Here, cyber diplomacy is defined as the *use of diplomatic methods to secure a state's interests and values in cyberspace.*[3] It is important to distinguish this from other uses of the term cyber diplomacy to refer to the use of cyber means (e.g., social media) to communicate on any subject. Instead, for our purposes, cyber diplomacy encompasses diplomatic activity to effectuate a state's interests *in* cyberspace.[4] In our view cyber diplomacy involves *all* available diplomatic methods (both online and offline means of communication and information exchange); it is simply the cyber-related subject matter that defines the field.

With this definition in mind, cyber diplomacy can fulfill at least four distinct functions:

Information gathering and reporting on the issue and/or other states' and stakeholders' related interests and activities;

Communications and public outreach regarding a state's foreign policy interests vis-à-vis a cyber issue;

Negotiations regarding a state's foreign policy interests vis-à-vis a cyber issue;

Diplomatic responses to unwanted cyber activity, whether attributing the origins of an unwanted cyber operation or using diplomatic means to impose costs on states that engage in them.[5]

[3] André Barrinha and Thomas Renard, "Cyber Diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, nos. 4-5 (2017): 355. https://www.tandfonline.com/doi/pdf/10.1080/23340460.2017.1414924?needAccess=true

[4] Barrinha and Renard, "Cyber Diplomacy: The Making of an International Society in the Digital Age," 355; "Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction," Shaun Riordan, *USC Center on Public Diplomacy*, May 12, 2016. https://www.uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

[5] Barrinha and Renard, "Cyber Diplomacy: The Making of an International Society in the Digital Age," 355; see generally Hedley Bull, *The Anarchical Society: A Study of Order in World Politics*, 3rd ed. (Basingstoke: Palgrave, 1977).

Importantly, however, diplomatic methods should not be confused with a state's foreign policy or interests. As underlined above, diplomacy is the instrument of communication, not the message communicated. For cyber diplomacy to be effective, a state must first grapple with its cyber foreign policy goals.[6] The depth and breadth of the issues cyber diplomacy addresses are extensive, and their relevance to states is growing. Below we provide a non-exhaustive list of examples that have benefited from engagement by cyber diplomats:

- **Responsible state behavior:** norms and international legal rules that detail behavior that is prohibited, permitted, or required of states in terms of their operations in ICT contexts;

- **Cyberconflict:** relevant international rules and confidence building measures to constrain states' capacity to engage in offensive cyber operations;

- **Internet Governance:** the constitution, operation, and protection of the network of networks and related communication technologies across multiple levels from national laws to the Internet Engineering Task Force's (IETF) standards and protocols to Internet Corporation for Assigned Names and Numbers' (ICANN) multistakeholder governance model..

- **Management of cybercrime:** the domestic and international criminal laws that proscribe certain behavior online by individuals or organizations and their impact across borders, including identifying criminal activity, as well as evidence collection, extradition, and other forms of law enforcement cooperation.

States with a cyber diplomacy capacity have chosen to engage in one, a few, or all of these issues in line with their foreign policy interests. Different states, moreover, prioritize these (and other ICT-related issues) differently. Some states focus their diplomatic efforts on internet governance, while others may devote more attention to combatting cybercrime. All states, however, have a stake in the first issue – identifying what norms and legal restraints constitute "responsible" state behavior and conforming their policies, practices, and laws to those expectations.

Cyber diplomacy is defined as the use of diplomatic methods to secure a state's interests and values in cyberspace

[6] Edward Marks, "Defining Diplomacy," *The Foreign Service Journal* (January/February 2015): 19; Ivor Roberts, *Satow's Diplomatic Practice*, 6th ed. (Oxford: Oxford University Press, 2010), ch.1.

Why should states engage in cyber diplomacy?

There are at least three reasons states should seek to understand cyber diplomacy and pursue such a capacity. First, issues related to cyberspace are of increasing relevance and concern not just to a few select states, but to all nations, this includes cybersecurity.[7] In a connected world, threats in the digital domain have the potential to harm any country, and they increasingly do. The 2021 Microsoft Exchange hack demonstrates the impact an online attack can have on thousands of organizations across the globe; the threat of electoral interference through malign online activities challenges democratic processes; and data breaches increasingly threaten national security interests, business operations, and fundamental human rights.[8]

Second, diplomacy offers a long-standing and effective means for addressing international problems and remediating challenges before they escalate or grow. Cyberspace may present novel and dynamic issues, but they are no more immune from diplomatic attention than other complex global problems, such as terrorism or climate change. Indeed, cyber diplomacy offers states a ready-made and relatively efficient vehicle for gathering information about the problems posed and the views and interests of other states and stakeholders. Beyond its capacity to offer valuable input, cyber diplomacy can help states (publicly and/or privately) advance their views and foreign policy interests

Third, cyber diplomacy negotiations are ubiquitous and ongoing. States with cyber diplomacy capacities can participate in these conversations and negotiate the contours and contents of any agreements they generate. In contrast, states lacking such capacity will either be left out of any agreements or receive them as a *fait accompli*.

In sum, cyberspace presents a problem set that requires attention, and diplomacy is one of the oldest and most respected traditions for redressing global problems. The diversity and robustness of existing diplomatic dialogues highlight the need for all states to build their capacities to participate and engage or risk being left behind (or out entirely) in laying the groundwork to address one of the most important and pervasive global issues of the day.

[7] Carr, "Cyberspace and International Order," 178.

[8] Elizabeth Dwoskin and Karla Adam, "More Than 150 Countries Affected by Massive Cyberattack, Europol Says," *Washington Post*, May 14, 2017. https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?utm_term=.868a27573305.

Readymade forums for engaging in cyber diplomacy

In recent years, major cyberattacks like SolarWinds, and influence operations targeting elections have attracted greater diplomatic consideration. International meetings have multiplied, and although some of these forums are new, others have been grafted onto existing international organizations (e.g., the United Nations (UN), the International Telecommunications Union (ITU)), regional intergovernmental organizations (e.g., the European Union (EU), Organization of American States (OAS), Organization for Security and Cooperation in Europe (OSCE), Council of Europe, etc.), and political arrangements (e.g., Wassenaar). States can therefore engage in a plethora of readymade platforms, such as:

- **Bilateral dialogue:** Bilateral diplomacy offers states with a cyber diplomacy capacity the potential to form coalitions of like-minded states through closed door conversation and identification of shared values and interests. They may also create cooperation and capacity building opportunities between two or more states, as well as advance trust and confidence in a domain where it can be difficult to understand other states' interests and capabilities.

- **Regional forums:** Regional diplomacy allows states to pool collective resources, demonstrate political will, and close capacity gaps. For example, the EU Diplomatic Toolbox provides a regional framework for developing diplomatic responses to cyber activities.[9] Some regional organizations, such as the OAS, have internal capacities on cybersecurity-related issues that may benefit states new to these topics.[10] Regional dialogues like the ASEAN-hosted "Asian Regional Forum" (ARF) provide states a platform to express shared interests that facilitate communication, reduce tensions, and open up greater opportunities for agreement.

- **Multilateral forums:** Efforts at the UN have already generated consensus on several critical cyber norms.[11] These dialogues have traditionally taken place in successive iterations of the Group of Governmental Experts (GGE) on information security, the first of which began in 2004. In 2021, the sixth GGE, as well as the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), a parallel platform open to all member states to discuss peace and security in cyberspace, adopted consensus reports.[12][13] States may also participate in issue-specific organizations that bring their expertise to cyberspace issues in fruitful ways (e.g., the Organization for Economic Cooperation and Development's (OECD) knowledge of economic development, the World Trade Organization's (WTO) expertise in trade in goods and services, and the Wassenaar Agreement's expertise in export controls).

[9] Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 9916/17 (7 June 2017) http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf; Annegret Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy," *SWP Comments*, no. 19 (2018): 3-5.

[10] OAS, "Cyber Security." https://www.sites.oas.org/cyber/en/pages/default.aspx.

[11] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." U.N. Doc. A/70/174, July 22, 2015, 26 ("2015 GGE Report").

[12] "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security." United Nations General Assembly. May 28, 2021. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[13] "Final Substantive Report: Open-ended working group on developments in the field of information and telecommunications in the context of international security." United Nations General Assembly. March 10, 2021 https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

- **Multistakeholder efforts:** In cyberspace, some of the most important stakeholders are not states. Industry, civil society, and academia are vocal and active in cyber diplomacy as well. Multistakeholder initiatives, such as the Paris Call for Trust and Security in Cyberspace[14], offer states an opportunity to participate in a broad-based coalition of like-minded actors who, together, may wield more leverage than individual governments and be able to dynamically support implementation of international expectations.

- **Technical networks:** Some cybersecurity issues can only be addressed in technical communities. Thus, to advance their own interests and values in cyberspace, states are acquainting themselves with these networks and how they operate. In particular, the existence of a national Cyber Security Incident Response Team (CSIRT) creates a venue for international communication with other national CSIRTs not only on technical threats and remediation, but also on a broader array of technical-policy issues. At the same time, for states unable to communicate because of political or military conflicts, "science diplomacy" (using technical networks in lieu of diplomatic dialogue) can serve as an alternative vehicle for communication.[15]

- **Industry networks –** Given the pervasive role of industry in cyberspace, states also need to consider engaging with industry in various ways.

    - States may encourage ICT actors within a state that have sufficient size and resources to develop their own policies on one or more cybersecurity-related issues and to communicate their views on these issues with other foreign industry representatives or with foreign states and international organizations.

    - Alternatively, a state may advance its cyber foreign policy by encouraging national ICT industry members to join and exercise an active voice in various influential industry networks (e.g., the Cybersecurity Tech Accord, the Charter of Trust).[16]

    - States may even engage diplomatically with industry directly by appointing representatives dedicated to this engagement to ensure more regular and structured consultations.

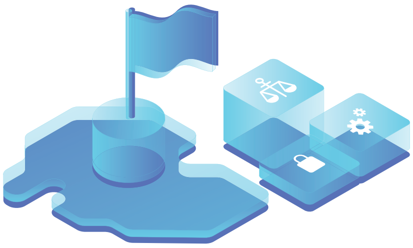
It is likely clear by now that there is no shortage of global forums where dialogues on international cybersecurity have been and continue to take place. And as this diplomatic space continues to grow and evolve, it can be daunting for any government to try and maintain a presence across every forum when dealing with limited diplomatic resources. As mentioned earlier, it is important to keep in mind that diplomacy is merely the *how*, and so before engaging in any of these spaces governments should first identify their national interests and build diplomatic capacities to strategically employ where they are most needed.

[14] "Paris Call of 12 November 2018 for Trust and Security in Cyberspace," *France Diplomatie*, 12 November 2018. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[15] Carr, Tanczer, and Brass, "CSIRTS and Global Cybersecurity: How Technical Experts Support Science Diplomacy," 60-61.

[16] Brad Smith, "34 Companies Stand Up for Cybersecurity with a Tech Accord," *Microsoft*, April 17, 2018. https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord; "Building a Consensus for Cybersecurity," *Siemens*, February 15, 2019. https://new.siemens.com/global/en/company/stories/research-technologies/cybersicherheit-charter-of-trust.html.

Examining existing practices for ensuring an effective cyber diplomacy capacity



National approaches

In the last few years, more than 100 governments have developed national cybersecurity defense strategies to combat cybersecurity risks. This includes countries as diverse as Australia, China, Chile, Israel and Germany. The United States was one of the first countries to go down this path; in 2011, it adopted a strategy for dealing with cyber issues that explicitly incorporated diplomatic resources alongside defense and development activity.[19] Shortly thereafter, the United States created a new position in the State Department, the Coordinator for Cyber Issues was the first diplomat solely assigned to deal with cyber-related topics. Most recently, the US Congress created a new position, the National Cyber Director, charged with overseeing the cyber defense and cybersecurity budgets of civilian agencies.[20]

Other states have since elevated officials to similar positions. Australia appointed its first cyber "ambassador" in 2016, with France taking this step in 2017,[21] Estonia[22] and the Netherlands[23] following suit in 2018, and the UK doing the same in 2019.[24]

States have built their cyber diplomacy capacities in diverse ways. In surveying the current landscape, states have used a similar set of "building blocks" to construct and deploy cyber diplomacy. We identify and discuss below seven standard practices that states with a cyber diplomacy capacity have used to develop and/or deploy that capacity.

1. **Establishing a national cyber strategy**: Almost all states with a cyber diplomacy capacity prefaced it with an internal exercise – drafting a national cyber strategy. These strategies often focus on cybersecurity, but some have a broader ambit, outlining the state's relationship to cyberspace as a whole. Several states have publicized their strategies, so there are several existing precedents from which other states may draw. Prominent examples include: the 2018 US Cyber Strategy,[25] the 2020 Australian Cybersecurity Strategy,[26] and Japan's 2021 Cybersecurity Strategy.[27]

[17] Fadia, Ankit, et al. "Follow the Leaders: How Governments Can Combat Intensifying Cybersecurity Risks," 23 June 2021. www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks.

[18] Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Aegis Paper Series*, no. 1703 (Stanford: Hoover Institution, 2017): 6. https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

[19] Barrinha and Renard, "Cyber Diplomacy: The Making of an International Society in the Digital Age," 359.

[20] The White House. "Statement by National Security Advisor Jake Sullivan on National Cyber Director and CISA Director Nominations," 12 Apr. 2021, www.whitehouse.gov/briefing-room/statements-releases/2021/04/12/statement-by-national-security-advisor-jake-sullivan-on-national-cyber-director-and-cisa-director-nominations/.

[21] Ministère de l'Europe et des Affaires Étrangère, "La stratégie internationale de la France pour le numérique", 2017. https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-strategie-internationale-de-la-france-pour-le-numerique/

[22] Catherine Stupp, "Estonia's First Cyber Ambassador Seeks to Improve Global Cyber Defense," *Wall Street Journal*, September 7, 2018. https://www.wsj.com/articles/estonias-first-cyber-ambassador-seeks-to-improve-global-cyber-defense-1536358734; Australian Minister for Foreign Affairs, Press Release, "Ambassador for Cyber Affairs," Nov. 16, 2016. https://foreignminister.gov.au/releases/Pages/2016/jb_mr_161110.aspx?w=tb1CaGpkPX%2FlS0K%2Bg9ZKEg%3D%3D.

[23] "Timo S. Koster." International Institute of Communications. https://www.iicom.org/profile/timo-s-koster/

[24] Duncan MacRae. "Cybersecurity Ambassador Appointed to Promote UK Expertise." Digit. 30 April 2019. https://digit.fyi/uk-cyber-security-ambassador/

[25] United States, The White House. *National Cyber Strategy of the United States of America*, Sept. 2018. trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[26] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy 2020* https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

[27] Japan's 2018 Cybersecurity Strategy, https://www.nisc.go.jp/conference/cs/dai17/pdf/17shiryou02.pdf

The process of developing a strategy requires a government to deliberate and articulate clear national priorities for cyberspace. These will then be used to guide the construction and deployment of any cyber diplomacy capacity. Note, these strategies are not static. States can and should revisit and revise them over time.

2. **Identifying a focal point for cyber diplomacy:** Following the adoption of a national cyber strategy, a number of countries have realized that they require a focal point within their government that deals with cybersecurity and that they need a similar function when it comes to dealing with matters related to foreign policy and cyberspace more generally. There are several models for doing so:

   - **The Cyber Ambassador Model:** A foreign ministry office, coordinator, or "cyber ambassador" is designated to organize the promotion and pursuit of the state's interests, values, and strategies externally, while leaving the performance of those functions internally distributed among different government agencies or even non-state actors. This position is typically high-level, with broad coordinating authority over a range of cyber-related issues, rather than siloed within one functional bureau.

   - **The Cyber Agency Model:** A new government department is created, centralizing all cyber-related activities, similar to other thematic departments (e.g., Ministries of Finance or the Environment).

   - **Disaggregated Diplomacy:** Different diplomatic capacities are constructed for different cyber issues. A state may, for example, have a different cyber lead for internet governance than for negotiating rules for responsible state behavior. Under this model, states may also structure each lead differently; for example, Germany has appointed a coordinator for all cyber issues (including internet freedom and internet governance) along with a separate department for only some of them (e.g., cybersecurity and cyber capacity building).[28] Alternatively, under this model, a state may designate cyber diplomats within all its institutions who have a role to play in cyber enterprises (e.g., ministries of interior, defense, law enforcement, finance, communications).[29]

States also vary in the mandate granted to their designated focal point, including an emphasis on international affairs issues, such as negotiating rules for responsible behavior in cyberspace and internet governance; or with a broader, more expansive remit encompassing economic issues like digital trade or technology regulation.

The choices states have made in creating focal points have come with trade-offs, different costs and benefits, and varying resource requirements. The cyber ambassador model provides a single focal point for external engagement with the promise of quicker or more flexible positioning. But, like other foreign ministry officials, a cyber ambassador may be separated from other domestic agencies that have authority over various cyber-related issues, thus limiting the Ambassador's authority. Those problems are less likely to occur where a single agency handles both internal and external engagements on cyber topics. The disaggregated diplomacy approach tries to avoid these issues but does so by requiring a much greater investment of resources, not to mention risking discordant communications given the number of individuals/offices that may be involved.

[28] Barrinha and Renard, "Cyber Diplomacy: The Making of an International Society in the Digital Age," 360.
[29] Ibid, 359-360.

3. **Standing up a government-wide policy process:** Establishing a focal point for cyber diplomacy marks only the beginnings of a cyber diplomacy capacity. Cyber diplomacy requires buy-in from a wide range of stakeholders in, and sometimes outside, a government. All relevant parties need to be aware and supportive of the policies and norms towards which the diplomatic efforts are driving. Building that buy-in requires integrating the cyber diplomacy focal point into a whole-of-government process. For some states, that process is accomplished by simply adding cyber topics to the agenda of existing national or domestic security councils.

   Alternatively, the designated cyber focal point may lead directly, thereby empowering the foreign ministry to conduct cyber diplomacy on behalf of all relevant government stakeholders. Participants in such a process may include all offices and ministries with ties to cyber policy, including defense, law, human rights, economics, and other ministries charged with building out information technology infrastructure. For example, Australia's Ambassador for Cyber Affairs convenes a quarterly whole-of-government International Cyber and Critical Technology Engagement Group.[30] These meetings help amplify the cyber ambassador's work, increase cross-department communication and collaboration, and ensure effective coordination and prioritization.

4. **Developing technical and legal expertise to engage competently on cyber issues:** Even for states that have extensive resources, one of the key challenges in cyber diplomacy has been identifying and developing personnel with sufficient expertise to engage on cyber issues competently. This has not meant that states with cyber diplomacy capacities only staff their offices with personnel who have degrees in computer science or law. But states have favored cyber ambassadors who can engage with other states and stakeholders in credible ways, whether on how the technology works or the international legal and normative frameworks within which it sits. There are multiple ways states have built up such expertise, including:

   - Hiring those who have the requisite education or background experience

   - Developing rotational programs within the government to leverage personnel from other agencies with legal or technical expertise[31];

   - Taking advantage of a growing number of capacity building opportunities for re-training existing diplomatic personnel to understand the nature and scope of issues relating to cyber diplomacy; or

   - Accepting secondments or other personnel loans from ICT firms or academic institutions, who can join a cyber diplomacy team for a set period and support its mission.

5. **Dedicating the required resources to operate effectively inside the government and abroad:** To date, states with an effective cyber diplomacy operation have invested substantial time, money, and diplomatic expertise into the effort. They have assigned cyber diplomacy leads with sufficient political capital to access senior government leadership and call upon their attention and decision-making authority.[32] Given the costs involved, however, states may seek to leverage other actors or institutions to further their cyber diplomacy efforts. This may be done by consolidating different agencies or offices focused on cyber into one bureau to streamline resources. Some states have sought more creative partnership opportunities with other governments, civil society, academia, and the private sector to serve as a force multiplier for resources. For example, in support of its 2016 National Cyber Security

[30] See DFAT, Australian Ambassador for Cyber Affairs. https://dfat.gov.au/about-us/our-people/homs/Pages/ambassador-for-cyber-affairs.aspx.

[31] See e.g., White House, Executive Order on America's Cybersecurity Workforce, May 2, 2019. https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/.

[32] Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," 6.

Strategy, the UK's Foreign Commonwealth and Development Office (FCDO) launched an International Cyber Security Capacity Building Programme, which aims to improve cyber security capacity in Eastern Europe, ASEAN nations, the Middle East and North Africa, India, Brazil, and Mexico.[33] The FCDO also worked with the Cybersecurity Tech Accord to produce a comprehensive overview of cybersecurity awareness efforts across the Commonwealth of Nations and to capture industry guidance for what makes such campaigns effective.[34]

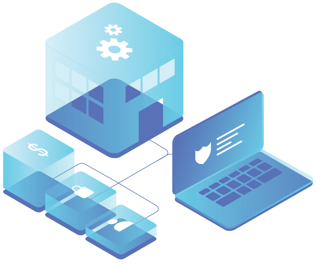
6. **Incorporating a strategic communication strategy for diplomatic inputs and outputs:** With all the components of a cyber diplomacy capacity in place, states have to decide whether and how these components are used. Successful cyber diplomacy involves more than just building the capacity; states must use it effectively.

   States have thus structured their cyber diplomacy operations to take advantage of the various inputs from other states and stakeholders on both the nature and extent of cyber-related issues of international concern and how other states propose to address (or redress) these problems. In addition, states have used their cyber diplomacy capacities to communicate their foreign policy priorities and proposals to others. These communications may be through classic diplomatic channels (e.g., demarches, attending various cyber-related conferences and meetings) or modern means of communication (e.g., social media or a dedicated website). In either case, most effective cyber diplomacy operations will incorporate a strategic communications campaign to advance a state's priorities or secure its resources. In addition, in several cases, states have used cyber diplomacy as a vehicle for reaching agreements with other states. For instance, in 2021, the United States and Singapore signed three memorandums of understanding (MOUs) to deepen cyber-security partnerships.[35] At the multilateral level, states continued to advance the dialogue on the applicability of international law to cyberspace.

7. **Developing a diplomatic toolkit for responding to unwanted cyber behavior:** In addition to information gathering, negotiations, and communications, states have engaged in cyber diplomacy to impose costs on those who engage in unwanted cyber behavior. Thus, states building a cyber diplomacy capacity have identified diplomatic tools they can use – in isolation or in concert with like-minded states – in response to cyber operations by other states or non-state actors. These tools include in-domain responses (e.g., botnet takedowns, taking websites offline) and out-of-domain ones (coordinated attribution, sanctions). Several states with cyber diplomacy capacities have developed diplomatic toolkits (e.g., the EU Cyber Diplomacy Toolbox) or have one emerging (e.g., the US effort to start a "Cyber Deterrence Initiative").[36]

Industry Approaches

One of the key features of cyber diplomacy is that is it rooted in multistakeholderism. Unlike other areas on which diplomats focus, like nuclear proliferation, where the technology and associated decisions on its regulation are essentially within the sole purview of states, cyber diplomacy implicate a variety of non-state actors, including industry and civil society.



[33] "FCO Cyber Security Capacity Building Programme 2018 to 2021," *Foreign and Commonwealth Office*, January 15, 2018. https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2018-to-2021.

[34] "Cybersecurity Awareness in the Commonwealth of Nations." Cybersecurity Tech Accord. March 2020. https://cybertechaccord.org/uploads/prod/2020/03/TechAccord-awareness-06.pdf

[35] US Cybersecurity and Infrastructure Security Agency (CISA), United States and Singapore Expand Cooperation On Cybersecurity, 2021. https://www.cisa.gov/news/2021/08/23/united-states-and-singapore-expand-cooperation-cybersecurity.

[36] Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy," 5; *National Cyber Strategy of the United States of America* (2018), 21.

This is demonstrated by the fact that several ICT companies have developed their own cyber diplomacy capacities, reflecting the fact that global operations mean that ICT companies have interests independent of any one government, including their state of origin. ICT companies also often engage in global cyber diplomacy efforts precisely because their platforms are where all the action happens: states use ICTs to launch and defend against cybersecurity operations, and it is, therefore, the ICT ecosystem that is the subject of attention in cyber diplomacy circles.

While recognizing that much of the decision-making here remains predominantly a domain for nation states, the impetus behind the emergence of new actors in this field is important to understand. We identify and discuss below several common practices that ICT companies, individually or as part of broader coalitions, have developed and deployed.

1. **Using forensics capabilities to respond to major cyberattacks:** : In December 2020, FireEye and Microsoft worked together to identify the group behind the hack on the software company SolarWinds, publicly revealing that the attackers' country of origin might have been Russia. Later in the year, Microsoft again pointed out attacks by the same group, adding momentum to government activity to sanction these actors.[38]

2. **Joining states as part of multistakeholder agreements:** The most prominent example of this is the Paris Call for Trust and Security in Cyberspace, with 705 companies joining alongside 79 states to support the agreement's nine core principles. In 2021, the Paris Call engaged its supporters further by establishing six working groups to strengthen the Paris Call community and to implement tangibly the principles structuring it. The Cybersecurity Tech Accord was tasked with chairing Working Group 3 and, in the course of 2021, has held a series of meetings, attended by over 80 representatives from governments, industry, civil society and academia, to advance the discussion on multistakeholder engagement in the UN dialogues on cyber.[39]

3. **Forming consortia of like-minded industry actors and public-private partnerships:** The two most prominent groups are the aforementioned Siemens-led Charter of Trust, which has focused on developing a methodology to secure supply chains, and of course the Cybersecurity Tech Accord. These types of industry coalitions have proven quite effective at organizing norms of behavior for industry itself, as well as in creating vehicles for regular interactions between industry and governments.

4. **Supporting states' capacity building efforts in cyberspace:** In 2019, the Cybersecurity Tech Accord published a set of recommendations to support the OAS in identifying approaches for effective confidence-building measures, an important tool to develop trust between states in cyberspace.[40]

5. **Interfacing with states on key technical issues of international concern:** Broadly conceived, information sharing and analysis centers (ISACs) and CSIRTs regularly interface with state officials on cybersecurity issues.[41] These interactions may not traditionally be viewed as diplomatic in nature, but in substance (sharing information, communicating positions, negotiating agreements on standards and best practices) they often function like more formal cyber diplomatic efforts.

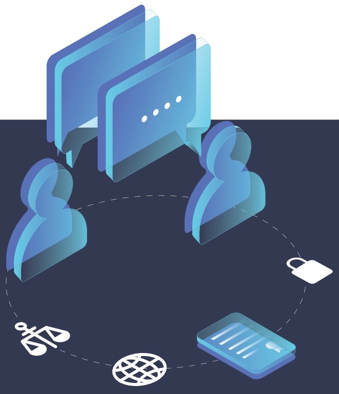
[37] CyberScoop, How FireEye attributed the SolarWinds hacking campaign to Russian spies, 2021. https://www.cyberscoop.com/fireeye-russia-solarwinds-kevin-mandia-postcard/

[38] Microsoft, Another Nobelium Cyberattack, 2021. https://blogs.microsoft.com/on-the-issues/2021/05/27/nobelium-cyberattack-nativezone-solarwinds/

[39] "Paris Call: Identifying new ways for multi-stakeholder cooperation." Cybersecurity Tech Accord. May 2021. https://cybertechaccord.org/paris-call-identifying-new-ways-for-multi-stakeholder-cooperation/

[40] "Promoting international peace and stability by building trust between states in cyberspace: The importance of effective confidence-building measures." Cybersecurity Tech Accord. April 4, 2019. https://cybertechaccord.org/uploads/prod/2019/04/FINALOASWP.pdf

[41] Carr, Tanczer, and Brass, "CSIRTS and Global Cybersecurity: How Technical Experts Support Science Diplomacy," 62-63.



Recommendations for effective engagement on cyber diplomacy

1. **Understand the need:**
Robust cyber diplomacy should start with a government's awareness that these issues can have a profound impact not only on international cyber stability, but across all areas, including the domestic economy, trade negotiations, and other international engagements. Cyber-issues are an integral component of a country's foreign policy agenda and should clearly articulate the government's focus areas while indicating long-term objectives for international cooperation, including which stakeholders (e.g., public, private, regional, global) would be engaged.

2. **Create a government-wide focal point:**
Cyber diplomacy is complex. It requires the ability to engage in international and domestic law while understanding various government departments' decisions on local industry and technology use. Therefore, states must identify and develop a focal point for cyber diplomacy efforts, even as they have different models to choose from in doing so. This may require robust coordination among different governmental entities so that the policy position expressed in the international arena is coordinated and aligned with other governmental bodies.

3. **Prioritize resources:**
It can be challenging for states to prioritize cyber diplomacy among the multitude of other open diplomatic engagements. At the outset, countries may want to focus their cyber diplomacy efforts on influencing regional bodies or prioritizing certain initiatives, rather than seeking to be engaged in all relevant fora.

4. **Invest in training and education:**
Effective engagement in international discussions requires governments to develop additional competencies and skills focused on cyber-issues to supplement traditional methods and processes of diplomacy and trade. Even with limited resources, states can still pursue training for government officials to build expertise and understanding while engaging on cyber-related topics. There is an array of governmental and non-governmental resources that states may employ to build and improve their capacities on various cyber-related issues from internet governance to cybersecurity and, in a few cases, cyber diplomacy itself.

5. **Create mechanisms for multistakeholder collaboration:** Given the potential impact the ICT industry can have in this space, states should develop processes that allow for input from industry and civil society in determining particular positions and approaches that touch on their areas of interest..

6. **Seek opportunities for sustained dialogue:** Given the plethora of bilateral, regional, multilateral, multistakeholder, and private networks within which cyber diplomacy may occur, states should think strategically about which, and how many, of these forums will advance their foreign policy goals. Based on that assessment, states may adjust the depth and breadth of their cyber diplomacy capacity.

7. **Demonstrate commitment to international peace and stability:** States that build a cyber diplomacy capacity should commit to the application of international law, including international humanitarian law, and human rights law. Countries should also demonstrate the commitment to the implementation of the agreed norms of voluntary state behavior in cyberspace, such as the ones confirmed by the sixth UN GGE and by the OEWG in 2021.

HTTPS://CYBERTECHACCORD.ORG/