Conceptualizing Cyberspace Security Diplomacy

The Honorable Christopher A. Ford

At a time when crippling ransomware incidents[1] have drawn awareness to the risks of cyberattack as perhaps never before—and in which cyber criminals often enjoy toleration and a symbiotic relationship with the government in safe haven jurisdictions such as Russia[2]—cybersecurity and cyber defense are topics of critical importance. In response to these threats, government officials[3] and private cybersecurity experts[4] alike seek effective responses, which increasingly involves cybersecurity-focused diplomatic engagement. This article offers a tentative framework for conceptualizing this challenge and developing more systematic approaches for cybersecurity policy interventions that will support and facilitate cyber diplomacy.

The Advent of Cyberspace Security Diplomacy

In their ongoing arms race with cyber criminals and state-sponsored cyber adversaries, the Western countries afflicted by such cyberattacks are working to find more effective approaches to combat the problem. Most efforts are technical in nature, relating to specific means to resist and counteract the tactics, techniques, and procedures (TTPs) used by cyber adversaries to exploit information systems, or to ways to hold them accountable through law enforcement or other means.

The Hon. Christopher Ford is Distinguished Policy Advisor at MITRE Labs and a Visiting Fellow at Stanford University's Hoover Institution. He previously served as U.S. Assistant Secretary of State for International Security and Nonproliferation, also performing the duties of the Under Secretary for Arms Control and International Security. The views expressed here are his personal opinions, and do not necessarily represent those of anyone else.

A less well known but growing component of the West's cyber defense, however, is also diplomatic, in the form of cyberspace security diplomacy. As exemplified by the U.S. State Department's Office of the Coordinator for Cyber Issues (CCI)[5] this work involves engaging with foreign counterparts to develop and articulate common understandings of peacetime norms for cyber activity; this includes the principles set forth by United Nations experts in 2013 that states should not attack each other's civilian critical infrastructure in peacetime.[6] It also involves promoting the adoption of common positions in attributing cyberattacks to malicious cyber actors and in imposing penalties (e.g., sanctions, public condemnation, or prosecution) upon those actors.

Cyberspace security diplomacy was responsible for a 2019 agreement reached by 28 Western countries expressing support for the "evolving framework of responsible state behavior in cyberspace," supporting "targeted cybersecurity capacity building to ensure that all responsible states can implement this framework and better protect their networks from significant disruptive, destructive, or otherwise destabilizing cyber activity," and pledging to "work together on a voluntary basis to hold states accountable when they act contrary to this framework."[7] It is now not unusual for US officials to impose sanctions upon malicious cyber actors in other countries, nor for US law enforcement agencies to issue criminal indictments.[8] Work by US diplomats, intelligence officials, and law enforcement officers to engage their international counterparts, moreover, has helped encourage foreign governments impose concrete international steps to penalize such malefactors as well.[9]

In the US, such cyber-diplomacy has been undertaken under the aegis of the *2018 National Cyber Strategy*, which called for "an international Cyber Deterrence Initiative" that would include building "a coalition [of states] and develop[ing] tailored strategies to ensure

adversaries understand the consequences of their own malicious cyber behavior."

> The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.[10]

Such diplomacy cannot solve all today's problems of rampant cybercrime and state-sponsored cyber assaults, of course, but it is a key piece of the puzzle as Western societies build effective responses.

Cyber diplomacy involves convincing others to agree upon cyber threat assessments, the attribution of specific attacks to specific actors, and what sorts of response may be appropriate in any given case. While there are extremely technical aspects of this work (such as the analysis of cyber-attackers' TTPs and intelligence-derived information in connection with attribution assessments) cyber diplomacy is not only a technical matter but also a persuasive and even political exercise, in which international counterparts work to develop areas of agreement and decide upon courses of action. Because cyberspace security diplomacy is a relatively new field, though, little study has hitherto been done of the persuasive aspects of this work.

The Diplomacy of International Cyber-Collaboration

Cyberspace security diplomacy revolves heavily around international efforts to come to agreement on cyber threats – and on the *attribution* of a cyber-attack to a particular malicious cyber actor. "Attribution diplomacy" is critical to the State Department's cyberspace security engagements. Though the conventional wisdom used to hold that such attribution was all but impossible in cyberspace,

> ... [i]t actually is possible to do more by way of attribution than most observers once thought possible. It is sometimes even possible to share enough information with one's friends and partners that they, too, can have a reasonable degree of confidence in the source of an attack.[11]

Attribution engagement opens possibilities "not just for more direct forms of response and deterrence, but indeed also for cyber diplomacy."

> ... [W]e are getting better and better at mobilizing partners to condemn the condemnable ... In February 2020 [for instance], 20 individual states — and the European Union as a whole — also joined in condemning the disruptive cyber attack against the country of Georgia mounted in October 2019 by the Russian GRU military intelligence service.
>
> In April 2020, moreover, the United States and several other likeminded countries issued concerted statements in response to an alert issued by the Czech Republic about its detection of impending cyber-attacks targeting its health sector, warning that such actions would result in consequences. This was the first time that likeminded states have come

> together to warn against a specific *future* cyber-attack, and we believe our warning had an effect; despite preparatory work by the would-be perpetrators, no major cyber-attack ultimately occurred in that case.
>
> Reinforced by the increasing imposition of not just United States but now also European Union sanctions in egregious cyber cases — coupled with "defend forward" activities [by the U.S. Department of Defense] — this cyberspace security diplomacy is helping to increase the costs and risks faced by the perpetrators of malicious cyber activity.[12]

Such diplomatic engagement in support of collaborative action among allies and partners against cyberspace threats is also a hallmark of Biden administration policy. In July 2021, for instance, President Biden announced that "[a]n unprecedented group of allies and partners," including the European Union (EU), the United Kingdom (UK), and North Atlantic Treaty Organization (NATO), was "joining the United States in exposing and criticizing the PRC's malicious cyber activities."

> Our allies and partners are a tremendous source of strength and a unique American advantage, and our collective approach to cyber threat information sharing, defense, and mitigation helps hold countries like China to account. Working collectively enhances and increases information sharing, including cyber threat intelligence and network defense information, with public and private stakeholders and expands diplomatic engagement to strengthen our collective cyber resilience and security cooperation. Today's announcement builds on the progress made from the President's first foreign trip. From the G7 and EU commitments around ransomware to NATO adopting a new cyber defense policy for the first time in seven years, the President is putting forward a common cyber approach with our allies and laying down clear expectations and markers on how responsible nations behave in cyberspace.[13]

In connection with this announcement, US officials announced the criminal indictment of four hackers from China's Ministry of State Security (MSS) for their involvement in "a multiyear campaign targeting foreign governments and entities in key sectors, including maritime, aviation, defense, education, and healthcare in a least a dozen countries."[14] Beyond these unilateral national measures, however, Biden administration officials declared that these international cyberspace security partners had agreed, for the first time as a group, to "share intelligence on cyberthreats and collaborate on network defenses and security."[15] On the heels of the EU agreement to extend its legal framework for an additional year for imposing sanctions in response to cyberattacks, the Biden administration's message in announcing the new group of international cybersecurity partners suggested that such collaborations are the wave of the future.[16]

A Framework for Thinking About Threat Persuasion

Naturally, the impact such collaborations will have upon the cost-benefit calculations of

those who engage in malicious cyber activity—particularly when such activity is sponsored by state-level actors—still remains to be seen. Because cyber-diplomacy is increasingly important, however, this article suggests a lens through which to think systematically about the processes of persuasive engagement between international partners and to help develop concepts for how specific policy interventions could facilitate such diplomacy.

Abstracting from the specifics of the cyber arena, one could imagine a basic framework for the dynamics of persuasive threat engagement—that is, of trying to persuade another actor, in a context highly dependent upon specialized technical information or intelligence collection, that a third party presents a threat or is responsible for a particular offense. Here, the likelihood of agreement will depend upon the interaction of three main variables: (1) the strength and reliability of the threat information available from the first party; (2) the degree of trust the second party places in the first party; and (3) the magnitude of the practical consequences or implications of reaching agreement.

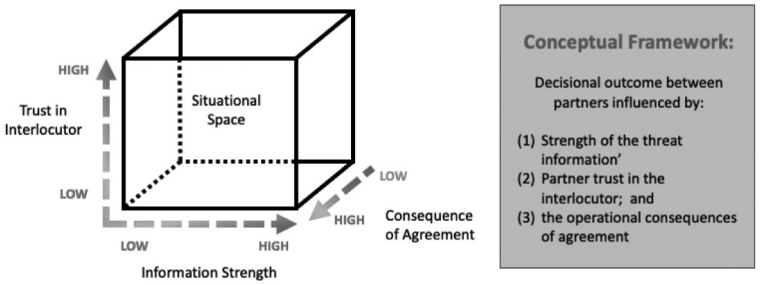
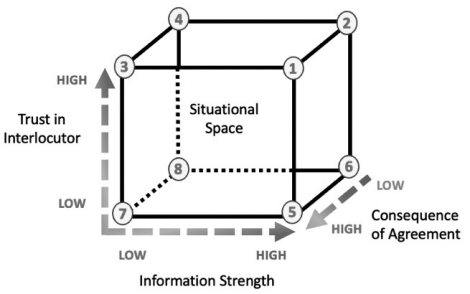


Figure 1. Situational Space

This situational space is represented in **Figure 1**. The reliability of the information is depicted along the X axis of the cube, from low strength on the left (*i.e.*, ambiguous technical assessments and/or low-confidence intelligence assessments) to high strength on the right (*i.e.*, compelling assessments and/or high-confidence information). The general level of trust the second party feels it can have in the honesty, integrity, and good faith of the first party is depicted along the Y axis, running from low trust (at the bottom) to high trust (at the top).

Finally, the consequences of agreement are depicted along the Z axis – running into the page, as it were, and making **Figure 1** into a three-dimensional graphic – from high to low. This consequences axes encodes the assumptions that agreeing upon the existence of a threat, or upon the fact that a given third party is indeed responsible for some bad act, will tend to put pressure upon the second party to take some course of action in response. To the degree that such a course of action would tend to impose greater risks or burdens upon the second party (*e.g.*, imposing sanctions upon a country likely to react harshly to such pressure), the consequence would be scored as high. To the degree that agreement would tend to lead to less costly or risky actions (*e.g.*, making verbal condemnations, or punishing a third party which would have few ways to retaliate), the consequence score would be rated as low.



#	Trust	Info Strength	Consequence
1	H	H	H
2	H	H	L
3	H	L	H
4	H	L	L
5	L	H	H
6	L	H	L
7	L	L	H
8	L	L	L

Figure 2. Situational Polar Cases

This graphic representation can be interpreted as shown in **Figure 2**. The table on the right sets out the eight polar cases that can be mapped three-dimensionally across the situational space of **Figure 1**. The various polar cases in the table are mapped onto the diagrammed cube on the left, defining the outer boundaries of situational possibilities. Graphically speaking, situations *in between* these hypothesized extremes of maximal or minimal information strength, trust, and consequence—*e.g.*, "fairly strong" information, "some distrust," or "moderate" or "uncertain" consequences—would appear inside the cube rather than on its outer limits.

The impact of these variables in terms of their presumed impact upon decisional outcomes is depicted graphically in **Figures 3, 4, and 5,** as follows:

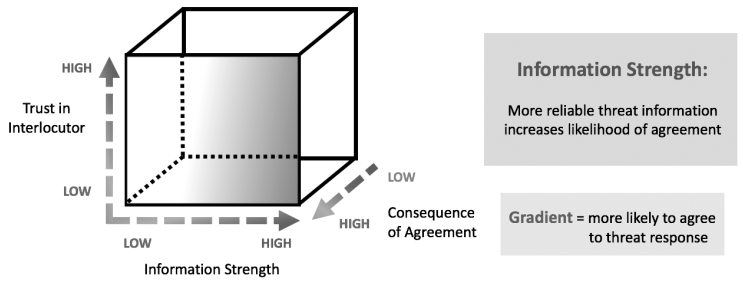


Figure 3. Likelihood of Agreement: Part I

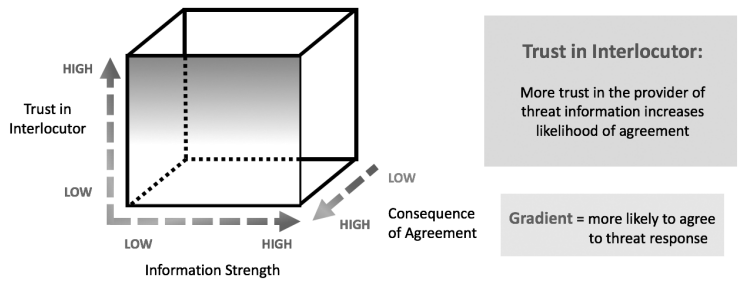


Figure 4. Likelihood of Agreement: Part II

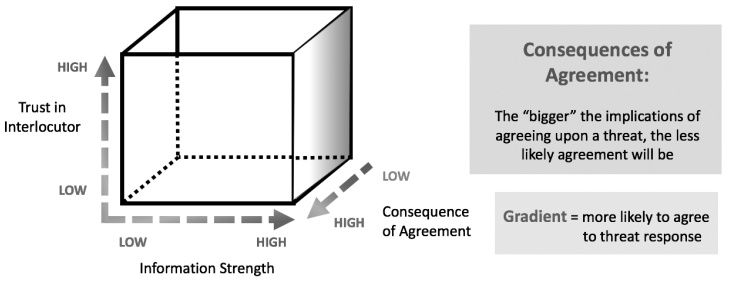
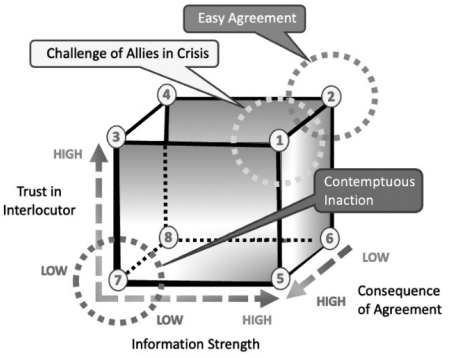


Figure 5. Likelihood of Agreement: Part III

These graphics may appear complicated, but the insights behind them are simple. One's interlocutor will be maximally likely to agree when the information is highly reliable, when that interlocutor has a strong relationship of trust in the party making the request, and when the consequences of agreement are easily borne. Agreement is correspondingly less likely where information is weak, trust is low, and the likely operational consequences of such agreement are high.

Just how likely agreement is in any given case will depend upon where it is in the graphic space depicted by the situational cube created by the axes representing the degree to which reliable information is available, the *degree* to which the second party trusts the first, and the magnitude of the likely consequences of agreement. This is shown in **Figure 6**:



#	Trust	Info Strength	Consequence	Agree?
1	H	H	H	Maybe
2	H	H	L	Yes
3	H	L	H	Unlikely
4	H	L	L	Maybe
5	L	H	H	Unlikely
6	L	H	L	Maybe
7	L	L	H	No
8	L	L	L	Unlikely

Figure 6. Likelihood of Agreement: Part IV

In **Figure 6**, the author has added his (subjective) assessments of likely decisional outcome to the tabular depiction on the right of the eight polar cases of **Figure 2**. In **Figure 6**, **Cases #7, #2, and #1** represent what may be particularly interesting examples. The first two of these are asymptotic decisional situations. In **Case #7**, the first party asks a great deal of the second (high consequences) but is not trusted by the second (low trust) and can only provide low-reliability information to support its case (low information strength). This is labeled contemptuous inaction, for that is very likely the reaction which such a demand would elicit.

In **Case #2**, by contrast, a trusted interlocutor provides solid information in support of its case, yet asks relatively little of the second party. Here, agreement would surely be all but inevitable.

A more challenging case is **Case #1**, in which a trusted interlocutor provides powerful information in support of its argument but asks a great deal of its interlocutor, thus setting the stage for a compelling but high-consequence decision. In **Figure 6**, this is labeled challenge of allies in crisis, for it suggests the kind of situation that might be faced by a close alliance responding to clear threats, but in ways that could lead to war. With sufficiently strong information and high trust, the parties might well agree, but it could be a difficult decision.

Example of Threat Persuasion Conceptualized

To try to put some real-world case studies into this framework, one might imagine the following potential examples:

- Afghanistan. After the terrorist attacks of September 11, 2001, the US felt it possessed very reliable information when it attributed those assaults to al-Qaeda. Washington thus turned to its NATO allies, with which it had a long and strong relationship of trust, asking them to participate in combat operations against the Taliban. Strong information and high trust produce strong scores along both the X and Y axes. The consequences for those allies, however, were arguably moderate, in the sense that they were being asked to go to war, but only against a low-technology enemy, in a theater where the US would clearly do most of the work, and in a context in which those allies would likely face terrorism at home anyway unless al-Qaeda were disrupted or defeated. The Afghanistan case might thus be depicted as **Point A** in **Figure 7**.

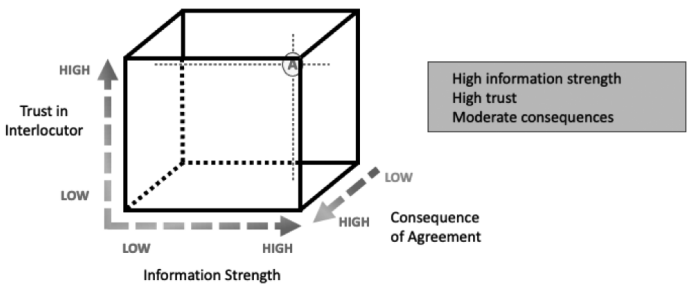


Figure 7. Thought Experiment: Afghanistan.

- **Iraq WMD.** Before the Iraq War of 2003, the US had what it and some of its most important and trusted allies felt was solid information on Iraqi weapons of mass destruction (WMD) threats. At the time, there was also a fairly high degree of trust on such matters among US allies.

  The Iraq WMD case differs from Afghanistan, however, in that the perceived consequences of action were higher. At issue here was actually invading a country with a sizable military, and without UN Security Council "permission." These implications

made action in Iraq much more fraught and challenging for US allies than taking action in Afghanistan, even before it became clear that the WMD intelligence information was gravely flawed. In this sense, the initial Iraq situation could arguably be situated at **Point B** in **Figure 8**, with both information reliability and allied trust declining over time toward **Point C**. (US officials were fortunate that their call for assistance occurred more toward the B end than the eventual C point of this progression.)

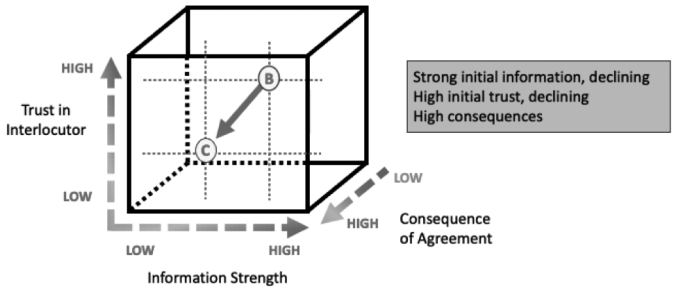


Figure 8. Thought Experiment: Iraq WMD.

- **Iran Nuclear Threats.** In dealing with Iran's clandestine nuclear program, the US had to contend with the legacy of distrust created by the Iraq WMD imbroglio in at least three respects. First, that historical baggage undermined confidence in WMD-related intelligence from unilateral national sources, particularly US ones. Second, it heightened allies' unease about US good faith. Third, it increased the perceived consequences of agreeing with Washington that Iran was trying to develop nuclear weaponry, by initially raising in some minds the specter of Iraq-style war if the US assessment of Iranian activity were accepted.

Partially counteracting these dynamics, however, was the role played by the IAEA as a third-party validator of at least some of the Iran nuclear threat information. This helped counteract some of the distrust of US information and good faith felt by other countries, since it was difficult to contest the IAEA's findings that Iran had been, at the very least, violating its safeguards obligations and engaging in exceedingly suspicious dual-use nuclear activity. (Eventually, in fact, the IAEA came to acquire significant information about Iran's nuclear weapons effort,[17] even before Israel exposed a huge archive of Iranian nuclear weapons program data to the world.[18]) As time went on, moreover, it became clearer—especially as the US became embroiled in the Iraqi insurgency—that a possible US invasion of Iran was not at issue after all, but rather merely a safeguards noncompliance finding by the IAEA and subsequent UN Security Council sanctions. Accordingly, the perceived significance of the Iran question moved along the Z-axis toward a lower consequences score. These shifts are shown in **Figure 9** as a movement between **Point D** and **Point E** within the situational cube; this arguably made possible the UN sanctions regime against Iran that was imposed beginning in 2006.

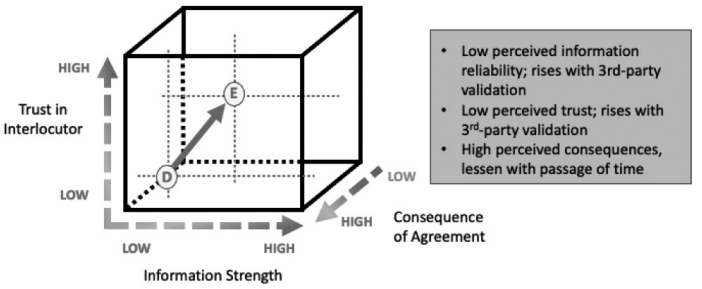


Figure 9. Thought Experiment: Iran Nuclear Threats.

- **Russia's INF Violation.** A more recent case can be found in the US attempt to persuade its allies of Russia's violation of the Intermediate-range Nuclear Forces (INF) Treaty. The US found Russia to be in noncompliance with INF in 2014, but it took years to bring NATO partners on board. Part of the difficulty related to the information in question. From a US perspective, the intelligence was strong, but it relied in part upon sources and methods that the US could not share with most NATO partners. The UK was the first to agree, as it benefits from "Five Eyes" intelligence-sharing. France and Germany, however, held back for longer, partly because they did not have access to as compelling a collection of intelligence, and partly because the perceived political consequences of agreeing on Moscow's violation were uncomfortably high with the likely collapse of an arms control agreement. These challenges for Paris and Berlin became more acute with the election of President Donald Trump, whom they distrusted on a personal basis even on top of their political desire to avoid giving a victory to the US arms control hawks who viewed Russia's development of INF-class missiles as a material breach of the Treaty.

  The US turned things around and won allied agreement, however, for at least three reasons. First, it was able to share more intelligence with France and Germany, and walked their experts through some of the analysis that had contributed to the US conclusion. This shifted things along the information reliability axis. Second, irrespective of precisely how far the missile in question could be shown to have been flight-tested, it became increasingly clear that Russia was moving forward with production and deployment, and this was coming to present a significant new threat to NATO. This shifted things along the consequences axis since, as politically distasteful as the collapse of an arms control treaty was to European sensibilities, there was no way to avoid Russian INF-class threats no matter what NATO agreed.

  Third, US allies came to realize that Washington would pull out of the INF Treaty in response to these threats irrespective of whether its partners agreed upon the Russian violation. These last two factors had the effect of shifting the situation significantly along the consequences axis, demonstrating that in light of Russia's actions there was no way to save

the Treaty. (These developments also suggested there might be a real cost to NATO if this issue were to split the Alliance just as new Russian nuclear missiles came into service.) This increase in information strength and lessening of the perceived consequences of agreement can be seen in **Figure 10,** in the movement between **Point F** and **Point G**, and led to NATO's unanimous decision that Russia was in material breach of the Treaty.[19]

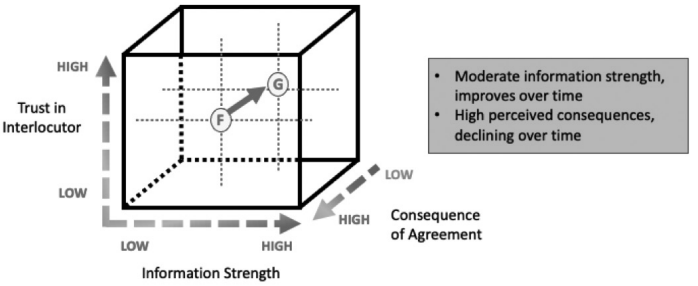


Figure 10. Thought Experiment: Russia's INF Violation.

- **Huawei in Britain.** One thought experiment related directly to cyberspace diplomacy is the UK's decision to ban products from the Chinese company Huawei in the UK's fifth generation (5G) telecommunications networks. Britain had been the first European country to offer Huawei a foothold in its networks,[20] but Huawei's increasing penetration of the British 5G market was a significant concern of US officials, who worried that the Chinese government might use Huawei and its equipment for malign purposes, and that Beijing's control over UK networks would provide it strategic leverage against this longstanding US intelligence-sharing and security partner.

  Officials in London had been reassured by their own experts that they could mitigate the risk, but US officials disagreed, and pressed their counterparts to end reliance upon Huawei. At the State Department, for instance, officials pointed out the dangers of allowing a company subject to control by the Chinese Communist Party (CCP) to manage the UK's emerging 5G economy, the moral problems of subsidizing Huawei's ongoing work in facilitating human rights abuses in Xinjiang, and the risks of espionage or other malicious cyber activities. They also noted that, even by their own admission, British government experts had failed to mitigate technical risks associated even with Huawei's fourth-generation technology, and that mitigation in 5G would be impossible.[21] In early 2020, the US stepped up the pressure, sending a high-level delegation to London to present "a new dossier of intelligence challenging the UK's claim that it would be able to mitigate the risks of adopting Huawei technology in its 5G network." (One of these officials reportedly said that adopting technology from Huawei would be "nothing short of madness.")[22] Raising the ante further, another US official reportedly warned London that "Donald Trump is watching [this decision] closely," while a third observed that "Congress has made it clear they will want an evaluation of our intelligence sharing" with the UK if China were permitted control over British 5G networks.[23]

UK officials downplayed this threat to "Five Eyes" intelligence-sharing,[24] but US officials up to the level of Secretary of State Pompeo had indeed speculated about this possibility for months after the US had banned Huawei from its own networks.[25] In early 2020, the issue acquired an increasingly public profile in the UK, particularly as parliamentarians called for inquiries into Huawei risks.[26] Meanwhile, the Chinese government was lobbying in Huawei's favor, even as press accounts revealed that Beijing had threatened trade retaliation against the Faroe Islands if Huawei did not get the 5G contract there.[27] Huawei itself also spent lavishly to win British favor, such as in donating to a charity founded by Prince Charles[28] and offering $1.25 billion for a new research institute at Cambridge University.[29]

A few weeks after the US delegation's visit, the UK announced that Huawei would continue to be permitted to build British 5G networks, but would be kept out of core parts of the system and would not be permitted to install equipment in or near particularly sensitive locations or facilities.[30] This British move was depicted as a defeat for the US,[31] but the UK revised its Huawei plans in July 2020, banning purchases of new Huawei 5G equipment after the end of the year, and also decreeing that existing Huawei equipment needed to be removed from UK networks by 2027.[32] UK officials then told telecommunications providers that they must stop installing Huawei equipment beginning in September 2021, and called for the "complete removal of high-risk vendors" from British 5G networks.[33]

From the outside, it is difficult to assess the specific reasons for the shifts in UK policy against Huawei during 2020. The intelligence information about Huawei reportedly provided to British officials by the US delegation may have had some impact, though it is unlikely that this proved decisive, since the initial decision to permit Huawei to control up to 35 percent of UK 5G networks was made after receiving the information in question.[34] Press reports have suggested that several additional factors likely played a role. Pressure had already been growing on the Johnson government within the Conservative Party, but this increased with the Chinese government's crackdown on pro-democracy demonstrators and civil society in Hong Kong, as Beijing began moving in 2020 to destroy the "one-country, two-systems" dispensation it had long promised would protect freedoms there. (In widely televised violence, Hong Kong police had been cracking down on pro-democracy demonstrators since mid-2019,[35] and in June 2020, Chinese authorities forced upon Hong Kong a harsh new law against "subversion."[36]) These developments highlighted the danger presented by the nature of the Chinese regime the Johnson government had initially been willing to give more than a one-third role in the UK digital economy. They also drew attention to the seeming ease with which Beijing could twist nominally independent Chinese entities (the supposedly independently elected government of Hong Kong, but also implicitly essentially any Chinese company, including Huawei) into instruments of CCP coercive power.[37]

In addition, the US announced additional moves against Huawei in the spring of 2020 that tended to "throw Huawei's supply chain into chaos"[38] and made 5G reliance upon it

more difficult to sustain. Specifically, the US government imposed new limits on the use of US-made semiconductor design tools in making chips destined for Huawei. Since US-origin design software dominated the high end of the chip manufacturing market, this cut off a crucial source of Huawei technology,[39] as US export control officials would treat Huawei-destined transfers with a presumption of denial.[40] This helped lead the UK to conclude that it would have increasing difficulty in relying upon Huawei for 5G technology, thus making agreement to US demands seem less costly. "American sanctions" against Huawei, claimed one former UK diplomat, "left the UK with little choice."[41]

These shifts changed the UK government's perception of the relative consequences of agreeing to the US request for a Huawei ban, since the political impact of not agreeing was clearly rising because of CCP brutality in Hong Kong, even as the UK's ability to reap the anticipated economic benefits of continued access to low-cost Huawei equipment was being called into question by tightening US export control rules. Accordingly, the Johnson government's response adjusted. According to one government minister, "[a]s facts have changed, so has our approach."[42] The Huawei case may be seen in the shift from **Point H** to **Point I** in **Figure 11.** As depicted there, a small increase is depicted in the information strength, and a more significant shift in terms of a reduction in the perceived consequences (*i.e.*, political and economic cost) of agreement.

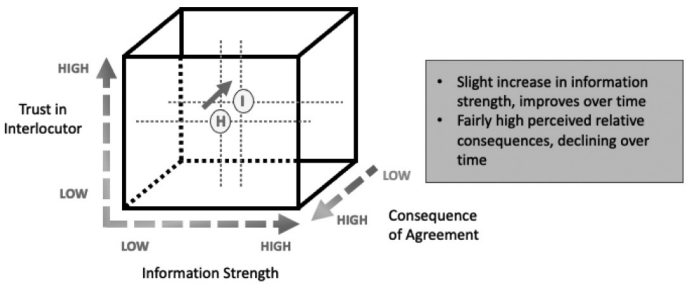


Figure 11. Thought Experiment: Huawei in Britain.

Implications for Policy Interventions

Whether or not one agrees with this author's assessments of outcome probabilities in **Figure 6** (or with his characterization of the aforementioned historical examples), this three-dimensional framework for understanding the interplay of information reliability, trust, and consequence may be useful in structuring how to think about developing and implementing policy interventions to increase the odds of success in threat engagement diplomacy. Such a conceptualization may be especially useful as the US steps up its cyberspace security diplomacy, as this framework may help point the way toward interventions specifically intended to boost information strength (X-axis), strengthen interlocutor trust (Y-axis), and/or lessen the perceived consequences of agreement (Z-axis) in order to drive situations more in the direction of the

decisional-outcome "sweet spot" depicted graphically below – that is, to push situations toward the zone of situational outcomes most conductive to agreement, as shown in **Figure 12** as a portion of the spherical zone around **Case #2** (easy agreement).

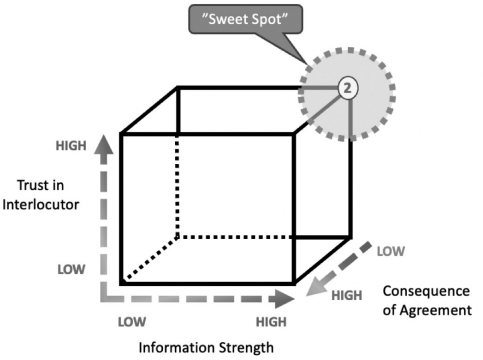


Figure 12. Desired End State of Agreement.

In the cyberspace context—in which diplomatic engagements often center around attribution diplomacy—such policy interventions could take various forms, including at least the following:

I. **Improved information sharing** is a way to help drive situations rightward along the information strength (X) axis in ways that would, all other things being equal, create a greater likelihood of agreement. This could mean doing more to share with international partners intelligence reporting that supports attribution analysis, either passing it directly to partners with whom one has good cyber-intelligence relationships (*e.g.*, within the "Five Eyes" partnership) or by downgrading information to be shared with others. Information sharing can also occur via public criminal indictments—which must meet due process standards and ultimately survive beyond a reasonable doubt proof standards for conviction if they get to court—or perhaps in connection with the imposition of sanctions.[43]

Whatever the means, however, building more effective mechanisms for secure sharing of attribution-relevant information would probably have the effect of making attribution agreement more likely. It can also help strengthen interlocutors' perceptions of trust in the sharer, potentially causing agreement-conducive movement along the graphical Y-axis as well. (A country sharing more information with a second-party partner that is more trusted by the third-party target of diplomatic suasion than is the first country can also help spur movement along both axes: it enables the recipient of this information to leverage its own relationship of trust with the ultimate target.) Augmented information sharing can thus result in movement within the cubic situational space along both the X and Y axes, as depicted in **Case I** in **Figure 13**.

To the degree that attribution-relevant information can be shared publicly, or at least very widely within the broad open-source cybersecurity community, one might expect this to also support more positive outcomes in attribution diplomacy. The MITRE Corporation's

"ATT&CK Matrix," for instance, compiles and displays information about known malicious cyber activity TTPs for cybersecurity professionals on an open-source basis,[44] providing a resource for cybersecurity officials around the world whose job it is to defend against such attacks. In cases where private sector or governmental attribution assessments have been made about specific intrusions, however, it might be possible in the future to include not just information about specific TTPs themselves but also an indication of which bad actor originated a given technique and with whom that technique's use is most frequently associated. To the degree that subsequent attribution diplomacy relies upon analysis of cyber-attack techniques, such a public record of past associations between bad actors and specific TTPs could help increase the credibility of subsequent attribution assessments, strengthening diplomatic persuasiveness.[45]

II. **Third-Party Validation** can also play an important role in increasing both information strength and interlocutor trust. In the cyber context, the third-party validation role is often played by private-sector cybersecurity firms who, in the wake of major incidents, often make public attribution assessments that can complement and reinforce those made by governments. Such validation can move things in agreement-friendly directions along both the X and Y axes of our situational graph, by augmenting the strength of information available for cyber-diplomatic persuasion and increasing the trust others can have. Working to strengthen interactions and engagements with a diverse range of private sector cybersecurity firms can be a way for government cyber-diplomats to increase the traction they will have with foreign counterparts. This is suggested graphically by **Case II** in **Figure 13**.

III. **Risk Mitigation** is another approach that could be used to increase the likelihood of positive decisional outcomes. This could include cyberspace-related capacity-building programming, analogous to the money the US spends through the State and Defense Departments to augment partner countries' ability to support nonproliferation-related objectives.[46] The US already does some cyber-related capacity-building programming[47] – to which, incidentally, the MITRE Corporation has made important contributions, both directly for the US and in working with 10 sponsor countries in East Asia[48] – but it probably should do more, especially as it builds out its cyber diplomacy capabilities.[49] Such capacity-building efforts could focus in particular upon measures designed to support attribution diplomacy, such as improving partner countries' own cyber collection and analytical capabilities (improving information strength), strengthening relationships between US and partner country cyber-related institutions (increasing trust), and improving partner incident response and cyber-systemic resilience (reducing the consequences of joint attribution decisions by helping better protect partners from cyber retribution). Through this prism, capacity-building programming could produce agreement-conducive movement along all three axes in the graphic representation, as shown by **Case III** in **Figure 13.**

IV. Over time, the US ability to build up a **Track Record of Accuracy** and a history of collaborative attribution decisions with its cybersecurity partners will also contribute to success in cyberspace security diplomacy. As noted, this is a new arena, since the conventional wisdom held that cyber attribution was essentially impossible. US officials are gradually building a record of engagement and collaboration on cyber attribution that is robbing the field of its initial strangeness, increasing relationships of trust, habituating foreign counterparts to attribution-focused engagement, and demonstrating that attribution is sometimes possible after all. This can hopefully create something of a virtuous circle of accelerating diplomatic success. This augmented trust is depicted graphically by Case IV in Figure 13 below.

V. Improved Information Collection is a final way to improve the odds of cyber-diplomatic agreement. With better intelligence information that supplements technical analysis of cyber-adversary TTPs, better analysis in understanding and drawing inferences from such TTPs and their patterns of employment, and other sources of relevant information, improved knowledge is likely to produce movement to the right along the Information Strength (X) axis, as shown by **Case V** in **Figure 13**.

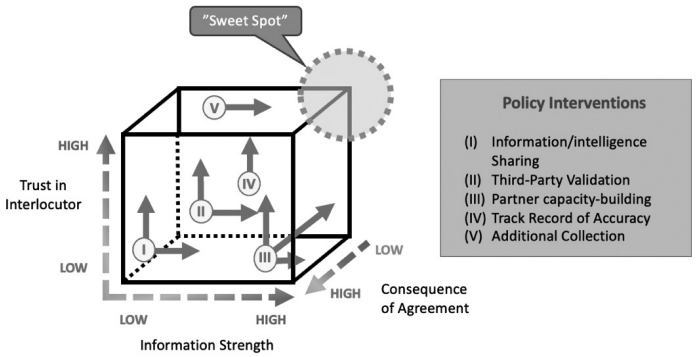


Figure 13. Policy Interventions.

CONCLUSION

This article is not intended to provide a comprehensive list of the ways in which policy interventions could improve the prospects for successful cyberspace security diplomacy. It has tried, however, to provide an intellectual framework for thinking about this problem, and to sketch out the key variables—information strength, partner trust, and operational consequence—that affect the likelihood of success in attribution diplomacy. This framework can help policy analysts and decision-makers focus more effectively on how to improve the ways in which our nation responds to cyberspace threats.

NOTES

1. Collin Eaton and Dustin Volz, "Colonial Pipeline CEO Tells Why He Paid Hackers $.4 Million Ransom," *The Wall Street Journal* (May 19, 2021), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636; Julie Creswell, Nicole Perlroth, and Noam Scheiber, "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business," *The New York Times* (June 3, 2021), https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html.
2. Ellen Nakashima, Hamza Shaban, & Rachel Lerman, "The Biden administration seeks to rally allies and the private sector against the ransomware threat," *The Washington Post* (June 4, 2021) (quoting senior Biden administration official that "countries like Russia ignore their activities as long as they don't target companies, people or government agencies inside their borders"), https://www.washingtonpost.com/business/2021/06/04/white-house-fbi-ransomware-attacks/; U.S. Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority" (April 15, 2021) (noting that the Russian Security Service [FSB] "cultivates and co-opts criminal hackers … enabling them to engage in disruptive ransomware attacks and phishing campaigns"), https://home.treasury.gov/news/press-releases/jy0127.
3. Brian Fung, Geneva Sands, Rachel Janfaza, and Zachary Cohen, "FBI director sees 'parallels' between challenge posed by ransomware attacks and 9/11," *CNN* (June 4, 2021) (noting that there is "a developing consensus within the Biden administration that ransomware ranks among the gravest threats to national security the United States has ever faced"), https://www.cnn.com/2021/06/04/politics/christopher-wray-cyberattacks-9-11/index.html.
4. Brenda R. Sharton, "Ransomware Attacks Are Spiking. Is Your Company Prepared?" *Harvard Business Review* (May 20, 2021), https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared.
5. U.S. Department of State, Office of the Coordinator for Cyber Issues website, https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-coordinator-for-cyber-issues/.
6. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations report A/70/174 (July 22, 2015), at 8, ¶ 13(f) (noting that states should not "conduct or knowingly support [cyber] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public"), https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
7. Joint Statement on Advancing Responsible State Behavior in Cyberspace (September 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/. The Joint Statement was signed by Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom, and the United States.
8. David E. Sanger and Andrew E. Kramer, "U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation," *The New York Times* (April 15, 2021), https://www.nytimes.com/2021/04/15/world/europe/us-russia-sanctions.html; U.S. Department of Justice, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations" (October 4, 2018), https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and; U.S. Department of Justice, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information" (December 20, 2018).
9. Lorne Cook, "First-ever EU cyber sanctions hit Russians, Chinese, NKoreans," *Associated Press* (July 30, 2020), https://apnews.com/article/malware-technology-foreign-policy-international-news-military-intelligence-978f1494313a545e6e7e568e5f9782bf; Laurens Cerulus, "EU countries extend sanctions against Russian, Chinese hackers," *Politico* (May 17, 2021), https://www.politico.eu/article/eu-council-cyber-sanctions-russia-china-hackers/.
10. *National Cyber Strategy of the United States of America* (September 2018), 21, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
11. Assistant Secretary of State Christopher Ford, "International Security in Cyberspace: New Models for Reducing Risk," *Arms Control and International Security Papers*, vol. I, no. 20 (October 20, 2020), 7, https://irp-cdn.multiscreensite.com/ce29b4c3/files/uploaded/ACIS%20Paper%2020%20--%20Cyberspace.pdf.
12. Ibid.
13. The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," press release (July 19, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

NOTES

14. "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity," *supra.*
15. Christina Wilkie, "U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange Servers" (July 19, 2021), paraphrasing Biden administration official, https://www.cnbc.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html.
16. Ionut Arghire, "European Union Extends Framework for Cyberattack Sanctions" (May 18, 2021), https://www.securityweek.com/european-union-extends-framework-cyberattack-sanctions.
17. IAEA, "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran," GOV/2011/65 (November 8, 2011), https://www.iaea.org/sites/default/files/gov2011-65.pdf.
18. David E. Sanger and Ronen Bergman, "How Israel, in Dark of Night, Torched Its Way to Iran's Nuclear Secrets," *The New York Times* (July 15, 2018), https://www.nytimes.com/2018/07/15/us/politics/iran-israel-mossad-nuclear.html.
19. Jim Garamone, "NATO Agrees: Russia in Material Breach of INF Treaty," *Defense.gov* (December 5, 2018), https://www.defense.gov/Explore/News/Article/Article/1705843/nato-agrees-russia-in-material-breach-of-inf-treaty/.
20. Adam Satariano, Stephen Castle, and David E. Sanger, "U.K. Bars Huawei for 5G as Tech Battle Between China and the West Escalates," *The New York Times* (July 14, 2020), https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html.
21. Assistant Secretary of State Christopher Ford, "Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," remarks to the Multilateral Action on Sensitive Technology (MAST) Plenary Meeting in Washington, DC (September 11, 2019), https://www.newparadigmsforum.com/p2431.
22. Helen Warrell, "U.S. presses Boris Johnson with new dossier on Huawei security risks," *Financial Times* (January 13, 2020), https://www.ft.com/content/1d7f44b4-3643-11ea-a6d3-9a26f8c3cba4; Dan Sabbagh, "Using Huawei in UK 5G networks would be 'madness,' US says," *The Guardian* (January 13, 2020), https://www.theguardian.com/technology/2020/jan/13/using-huawei-in-uk-5g-networks-would-be-madness-us-says. (By way of full disclosure, the author of this article was one of the officials on that U.S. delegation.)
23. Warrell, *supra*; Sabbagh, "Using Huawei in UK 5g networks," *supra.*
24. Dan Sabbagh, "US intelligence sharing will not be jeopardized if UK uses Huawei – MI5 head," *The Guardian (*January 12, 2020), https://www.theguardian.com/technology/2020/jan/12/huawei-technology-poses-no-threat-to-uk-security-ex-mi5-head.
25. Cecelia Kang and David E. Sanger, "Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear," *The New York Times* (May 15, 2019), https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html.
26. "Using Huawei in UK 5G network 'madness,' says US," *BBC News* (January 14, 2020), https://www.bbc.com/news/business-51097474.
27. Adam Satariano, "At the Edge of the World, a New Battleground for the U.S. and China," *The New York Times* (December 20, 2019), https://www.nytimes.com/2019/12/20/technology/faroe-islands-huawei-china-us.html.
28. Satariano, Castle, and Sanger, *supra.*
29. Huawei, "Huawei to Build an Optoelectronics R&D and Manufacturing Centre in Cambridge" (June 25, 2020), https://www.huawei.com/en/news/2020/6/huawei-optoelectronics-rd-manufacturing-centre-cambridge.
30. Adam Satariano, "Britain Defies Trump Plea to Ban Huawei from 5G Network," *The New York Times* (January 28, 2020), https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html.
31. Satariano, "Britain Defies Trump Plea," supra.
32. Leo Kelion, "Huawei 5G kit must be removed from UK by 2027," *BBC News* (July 14, 2020), https://www.bbc.com/news/technology-53403793; Satariano, Castle, and Sanger, *supra.*
33. "Huawei ban: UK to impose early end to use of new 5G kit," *BBC News* (November 30, 2020), https://www.bbc.com/news/business-55124236; "Britain bans new Huawei 5G kit installation from September 2021," Reuters (November 29, 2020), https://www.reuters.com/article/us-britain-huawei/britain-bans-nw-huawei-5g-kit-installation-from-september-2021-idUSKBN28A005.
34. Satariano, "Britain Defies Trump Plea," *supra.*
35. Austin Ramzy and Mike Ives, "Hong Kong Protests, One Year Later," *The New York Times* (June 9, 2020), https://www.nytimes.com/2020/06/09/world/asia/hong-kong-protests-one-year-later.html.

NOTES

36. "Hong Kong security law: what is it and is it worrying?" BBC News (June 30, 2020), https://www.bbc.com/news/world-asia-china-52765838.
37. *Quoted by* Satariano, Castle, and Sanger, *supra.*
38. Satariano, Castle, and Sanger, *supra.*
39. Assistant Secretary of State Christopher Ford, "U.S. National Security Export Controls and Huawei," Arms Control and International Security Papers, vol. 1, no. 8 (May 20, 2020), 7, https://irp-cdn.multiscreensite.com/ce29b4c3/files/uploaded/ACIS%20Paper%208%20-%20Export%20Controls%20and%20Huawei.pdf.
40. Ana Swanson, "U.S. Delivers Another Blow to Huawei With New Tech Restrictions," The New York Times (May 15, 2020), https://www.nytimes.com/2020/05/15/business/economy/commerce-department-huawei.html.
41. Satariano, Castle, and Sanger, *supra* (quoting unnamed former official who previously "represented the country's interests in Silicon Valley").
42. Ibid., quoting Telecommunications Minister Oliver Dowden.
43. In US practice, however, the evidentiary standards for sanctions are generally lower; nor do officials generally have to make public the evidence upon which they rely in making sanctions determinations.
44. MITRE Corporation, "ATT&CK Matrix for Enterprise," accessed on July 5, 2021, https://attack.mitre.org/#.
45. The ATT&CK Matrix does not currently or systematically include such notations, though it does occasionally indicate that particular hacker groups have employed particular techniques. MITRE Corporation, "Procedure Examples," accessed on July 5, 2021 (noting that the "APT28," "Sandworm," and "Volatile Cedar" groups have employed the "vulnerability scanning" technique coded with the identification number T1595.002), https://attack.mitre.org/techniques/T1595/002/.
46. Assistant Secretary of State Christopher Ford, "Reforming Nonproliferation Programming," remarks at the Stimson Center (September 25, 2018), https://2017-2021.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/reforming-nonproliferation-programming/index.html; Assistant Secretary of State Christopher Ford, "The Evolution of International Security Capacity Building," remarks to the CRDF Global Board of Directors (November 20, 2020), https://2017-2021.state.gov/the-evolution-of-international-security-capacity-building/index.html.
47. Kathryn Fitrell, "Office of the Coordinator for Cyber Issues: Leading and building effective international cyber diplomacy," *State Magazine* (February 2021), https://statemag.lab.prod.getusinfo.com/2021/02/0221office/.
48. MITRE Corporation, "MITRE Strengthens Cyber Capacity of Developing Nations" (December 2019), https://www.mitre.org/publications/project-stories/mitre-strengthens-cyber-capacity-of-developing-nations.
49. U.S. Department of State, "Secretary Pompeo Approves New Cyberspace Security and Emerging Technologies Bureau" (January 7, 2021), https://2017-2021.state.gov/secretary-pompeo-approves-new-cyberspace-security-and-emerging-technologies-bureau/index.html.