CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

SIIS 上海國際問題研究院
SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES

Managing U.S.-China Tensions Over Public Cyber Attribution

Ariel E. Levite, Lu Chuanying,
George Perkovich, and Fan Yang, editors

Managing U.S.-China Tensions Over Public Cyber Attribution

Ariel E. Levite, Lu Chuanying,
George Perkovich, and Fan Yang, editors

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, D.C. 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

Carnegie Europe
Rue du Congrès, 15
1000 Brussels, Belgium
P: +32 2 735 56 50
CarnegieEurope.eu

This publication can be downloaded at no cost at CarnegieEurope.eu.

Contents

About the Authors

Jon Bateman is a fellow in the Cyber Policy Initiative of the Technology and International Affairs Program at the Carnegie Endowment for International Peace.

Scott Collard is a nonresident scholar in the Cyber Policy Initiative of the Technology and International Affairs Program at the Carnegie Endowment for International Peace, a Lieutenant Commander in the U.S. Navy, and finishing his master's of public policy at the Harvard John F. Kennedy School of Government.

June Lee is a program coordinator in the Technology and International Affairs Program at the Carnegie Endowment for International Peace.

Ariel E. Levite is a nonresident senior fellow in the Nuclear Policy Program and Cyber Policy Initiative at the Carnegie Endowment for International Peace.

Lu Chuanying is the director of and a senior fellow at the Research Center for Global Cyberspace Governance, SIIS.

George Perkovich is the Ken Olivier and Angela Nomellini Chair and vice president for studies at the Carnegie Endowment for International Peace, overseeing the Technology and International Affairs Program and Nuclear Policy Program.

Xu Manshu is a senior fellow at the Research Center for Global Cyberspace Governance at SIIS.

Fan Yang is an assistant professor of law and the deputy director of the Cyberspace International Law Center in the School of Law at Xiamen University.

Foreword by Chen Dongxiao

"Managing U.S.-China Tensions Over Public Cyber Attribution" is the second joint research publication produced by the Shanghai Institutes for International Studies (SIIS) in collaboration with the Carnegie Endowment for International Peace (CEIP). The first joint publication, "China-U.S. Cyber-Nuclear C3 Stability," launched in April 2021, has presented an insightful analysis on China-U.S. cyber and nuclear security, offering many valuable policy recommendations for both governments, thus garnering high attention from the policy community and academia in both China and the United States. Inspired by the first concerted effort, SIIS and CEIP task forces carried out further studies and presented their latest findings in this compilation. With high respect, I applaud their unremitting efforts and collaborative spirit in accomplishing this informative publication of valuable academic and policy reference.

Public attribution is an important yet sensitive issue in cyberspace interaction between China and the United States. While gaps exist between the two countries' understanding of the issue (especially over the origin of the dispute, policy toward each other, cybersecurity accountability, and approaches to dispute settlement), such divergences have posed a growing negative impact on maintaining stable and healthy China-U.S. relations, both in this area and in broader terms. Building upon their expertise gained in long-term studies, SIIS and CEIP task forces spent over half a year to conduct comprehensive, in-depth, and constructive research through discussion and dialogue. They authored six articles on key issues of public attribution from different perspectives and worked together on the conclusion and recommendations. I believe this compilation will be one of the most pioneering and enlightening findings in the domain of public attribution for the reference of both countries' stakeholders in building stable and sound China-U.S. relations in cyberspace.

It is not only their expertise both teams have exhibited, but also the collaborative spirit and mutual trust they have built throughout the project that highlights this work. China-U.S. relations have entered a new phase characterized by emerging challenges to be addressed and increasing divergences to be managed. The

success of this project proves that China and the United States together are capable of finding pragmatic and practical solutions to meet today's challenges with expertise, cooperation, and trust.

SIIS attaches great importance to the study of cybersecurity and emerging technology. The Research Center for Global Cyberspace Governance was founded under SIIS in 2018 in a joint effort by the National Defense University, Fudan University, Nanjing University, Xiamen University, the Shanghai Academy of Social Sciences, among other leading universities and think tanks in China. To this day, the center has participated in the UN's rule-making process in cyberspace and several international projects of public influence at home and abroad. This compilation is yet another important output of this center. I congratulate the authors of this report and would also like to thank Xu Weidi, Du Yuejin, Li Yan, Li Bin, Lyu Jinghua, Lang Ping, Xu Longdi, Hui Zhibin, Cai Cuihong, Shen Yi, Zhu Lixin, and Dai Lina for their contribution and advice. Lastly and most importantly, my gratitude goes to the China-United States Exchange Foundation (CUSEF) for its generous support.

Chen Dongxiao
President of the Shanghai Institutes for International Studies

Foreword by Tino Cuéllar

Among the many factors that will shape global security and prosperity in the rest of the twenty-first century, the relationship between China and the United States looms especially large. Together, both countries constitute approximately 52 percent of global military spending, and almost 35 percent of global GDP.[1] If relations between the world's two largest economies and military powers become increasingly adversarial and akin to a zero-sum game, the world will almost certainly witness decades of a more costly and dangerous arms race, greater economic risk, more strained efforts to cooperate on innovation and lasting solutions on climate change and other global challenges, and more tenuous security. The people of both countries—along with populations in other countries that could become sites of fierce competition—will face a more uncertain and potentially dangerous future. Conversely, if the United States and China can take even modest and measured steps to redress each other's concerns without casting aside core interests, their citizens and the rest of the world can rebuild confidence in the possibility of a safer and more prosperous future. Today such an approach may be difficult to imagine given that the two countries have both divergent interests as well as common challenges. Without sustained and tenacious effort to pursue such cooperation, however, it stands no chance.

The Carnegie Endowment for International Peace endeavors to foster sensible cooperation and dialogue through in-depth research, timely analysis, and candid dialogue. Working with partner organizations throughout the world—in this case, the Shanghai Institutes for International Studies—our scholars can help the world better understand Chinese and American perceptions of daunting issues facing each country and the world. We can help both sides discern their differences and more thoroughly identify their interests—better than either can under the status quo or in response to more adversarial frameworks for relations. Over the course of a four-year project that resulted in the publication of the pathbreaking "China-U.S. Cyber-Nuclear C3 Stability" paper, researchers and advisers from the two organizations

demonstrated this willingness and capacity to cooperate in a world that calls for robust communication as well as candor about divergent views.

Now our institutions have again worked together to better understand how the United States and China approach crucial questions concerning public accusations about the conduct of cyber operations they consider unacceptable, and what each country might do to mitigate both the causes and the unwelcome effects of public attribution. The papers and conclusions in this collection emerged from a series of video discussions between the two groups, which informed the authors' early drafts. These drafts were the subjects of subsequent video conferences and written comments by all participants. Each paper represents the authors' own views; we did not seek to obtain agreement or consensus on them. The conclusion and recommendations were broadly acceptable to all participants, though we did not negotiate each word.

I extend my appreciation to the project leaders, authors, and advisers from both organizations, and (for the English-language version) the superb editorial and production team at Carnegie. We also thank the Hewlett Foundation, whose support made Carnegie's contribution to "Managing U.S.-China Tensions Over Public Cyber Attribution" possible. The talent and good will of the people from both our institutions and those who support us help demonstrate how it remains possible to achieve a candid exchange of ideas, diplomatic engagement, and genuine collaboration to understand and mitigate differences.

Mariano-Florentino "Tino" Cuéllar
President of the Carnegie Endowment for International Peace

CHAPTER 1

Cyber Attribution Lessons From the Maritime Domain

SCOTT COLLARD

Like the cyber domain, the world's oceans have extensive economic and strategic benefits, and are mostly concealed from the eyes and ears of the public. Maritime shipping accounts for 90 percent of global trade, sovereign islands provide exclusive economic and strategic benefits, and undersea cables provide vital arteries for information and financial transactions between countries. The contest for these resources attracts the interest of a multiplicity of actors from private enterprises, regional governments, and global superpowers alike, and many of these players are civilian and generally peaceful. However, adversary navies, pirates, smugglers, and terrorists span a wide diversity of motivations, skills, and training, promoting an operating environment that often results in disputes. Disputed actions are complicated by their technical nature and the uncertainties around discovering intended purpose and controlling entities. Like searching for stealthy naval platforms, cyber adversary detection is difficult, much of the activity is confidential, and norms are challenging to enforce. Unlike the maritime domain's established legal history, cyber law and policy is still in development; at the same time, governments and private sectors struggle to understand and enforce stabilizing rules and norms. This examination of public and private attributions through various channels in the maritime domain offers strategic takeaways for policy development and conflict resolution in cyberspace.

Conflict Resolution

International Law and Maritime Norms

Developing maritime technology in the early twentieth century encouraged transnational competition for resources in and control of the oceans. During this time, strategic public attributions of conflicts over territorial incursions and economic activity functioned to develop an international consensus. Recognizing the need to establish international maritime law from these norms, 168 member states of

the United Nations ratified the United Nations Convention on Law of the Sea (UNCLOS). UNCLOS serves as the legal framework that denotes maritime sovereignty and provides guidelines for naval activity. Although the United States signed the agreement, it was never congressionally ratified.[2] The majority of economic actors abide by the rules to mutual benefit, but some naval and malicious actors openly defy them. Absent the legal structure to prosecute these violations, UNCLOS regulations more resemble international standards that can be disobeyed with little consequence. Despite these imperfections, UNCLOS is fundamental to free trade and personnel safety, but more importantly it is the foundation for supplementary bilateral agreements providing attribution channels for conflict resolution. In this manner, we can draw a parallel to the developing cyber environment; there are few customary international laws specifically regulating cyberspace, and increased public attributions to cyber attacks draw international attention to the increasing disparity between existing law and cyber capabilities.

Defined cyberspace norms that mirror UNCLOS regulations are still in development. Institutions such as the UN Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) agree that international law applies to the cyber domain. However, established legal principles are difficult to apply to new technological innovation. Reports by the GGE and OEWG recognize the challenges with attributing unacceptable cyber behavior but lack the specifics of suitable enforcement. Without baseline norms, these reports fall short of the regulations that UNCLOS provides the maritime domain. Even so, every member of the GGE, including the United States and China, has agreed that "international law . . . is applicable and essential to maintaining peace and stability, and promoting open, secure, stable, accessible, and peaceful ICT environment."[3] Recognizing the need for "deepening common understanding on how international law applies to State use of ICTs," states are advised to settle disputes with "peaceful means such as negotiation, mediation, conciliation, arbitration, or judicial settlement" by "regional agencies or arrangements."[4] As the international community constructs the framework for responsible behavior in cyberspace, states can independently define attribution mechanisms for acceptable and legal cyber activity in a manner that protects economic interests, national security, and state sovereignty.

Previous maritime conflict resolutions provide models for directing U.S.-China cyber attributions. During naval actions in the 1960s, military ships and aircraft would regularly perform unsafe maneuvers called "bumping," in which a civilian or military platform radiates, blocks, or collides with another at high speed. These interactions often take place in crowded shipping lanes and are accompanied with simulated attacks. Some of these maneuvers are intended to discover protocol vulnerabilities, while some are purely antagonistic. These dangerous maneuvers were responsible for numerous deaths and collisions involving military and commercial vessels at the height of the cold war. U.S. and Soviet officials recognized the growing dangers of these unprofessional encounters, and following negotiations signed the Incidents at Sea Agreement (INCSEA) of 1972, the first of many similar bilateral agreements with consultative exchange mechanisms synergistic to UNCLOS. This joint international accord outlines and prohibits dangerous behavior at sea while establishing an instrument for government representatives to review and address disputes. Notably this agreement calls for 1) preliminary notice for potentially dangerous activities, 2) respective attaché channels to reconcile disputes, and 3) annual meetings that review agreement implementations.[5] The private consultation channels provided enforcement to UNCLOS regulations, and decreased government pressure to respond publicly to incidents. Today, these activities are predominantly curtailed, and infrequent occurrences like the 2001 bumping incident between a U.S. Navy surveillance aircraft and a Chinese Navy interceptor jet are resolved diplomatically, despite disagreement over the responsible nation.[6]

Cyber bumping could be referred to today as a number of harmful cyber attacks targeted daily against both governments and private entities. Increasingly aggressive operators cause more and more economic and social damage, as captured by the public attributions from both U.S. and Chinese officials in 2021.[7] Just as the GGE representatives agree that international law applies to ICT, they also report an increase in significant cyber incidents, suggesting that public attributions in their present state are ineffective in curtailing unwanted activity,[8] and highlight the opportunity for attribution channels that allow for peaceful operations while largely avoiding inadvertent conflicts. Notably, the mechanisms of INCSEA agreement models are used to resolve transboundary disputes across numerous international and economic associations, and mechanisms for cyber attribution will likewise reflect varying international relationships.[9]

Individual Actors

Following the establishment of norms and legal structures in place to monitor cyberspace, violations or even accidental incursions are foreseeable. Negligent government actors, cyber criminals, and opportunistic attackers will defy policies and norms. How should national governments handle these isolated but inevitable incidents? The maritime domain again offers a useful model to replicate.

Individual entities are the most accountable for their cyber or navigational security. In international waters, distinct units (ship captains, aircraft commanders) handle most norm violations with predefined procedures designed to prioritize safety and deescalate aggressive situations. For dangerous or antagonizing behavior, such as vessels in proximity or intentional posturing of weapons systems, UNCLOS protocol requires immediate and unit-directed public attribution while simultaneously recording the details of the incident, increasing defensive postures, and maneuvering for safety. This initial attribution details the suspect's identity and location on a public network, so that nearby entities can independently assess potential hazards and take defensive measures, and the accused unit is given an opportunity to correct unintentional behavior. The accusing unit then reports this violation to its controlling authority, continuing its operations without offensive response.

Controlling agencies use these activity reports to communicate their grievances to an international counterpart, in the form of private attribution, providing technical incident details as part of a forensic investigation. The sector commander provides the accused entity the option to resolve their transgression before electing to deploy countermeasures, such as prohibiting port entry or imposing fines against the violating ship's controlling agency. During these private bilateral discussions, agencies can sort out technical failures and human error from deliberate actions approved by controlling policy or doctrine. In this manner, mid-level authorities can reprimand unsanctioned activity such as a specifically maverick pilot or negligent ship captain without further escalation, or forward dangerous adversary policies to higher authorities. In many cases, nations withhold evidence that would disclose secret capabilities. This sensitivity necessitates a significant level of trust and fair-minded analysis of the evidence presented. Private channels are most likely to encourage this rapport, even when follow-on public disclosure is necessary for cost imposition or indictments.

Governments need defined channels to address cyber incidents. While some nations rarely attribute publicly, others attribute often but inconsistently. Research demonstrates that U.S. public cyber attributions are inconsistent in timing, entity, language, channel, and retribution.[10] In the absence of defined policies

and agreements, this ad hoc approach diminishes stabilizing effects of public attribution by appearing politically motivated or unfounded to the accused state. Additionally, U.S. public companies do not always confer with the government prior to attribution, which can create a confusing and unhelpful event narrative. Conversely, the absence of attribution suggests that nations are more apt to retaliate instead of imposing costs via legal or diplomatic means. Despite these varied attribution approaches, large-scale cyber attacks that cause significant damage to infrastructure, economic interests, or national security are increasing in frequency, and compel a consistent public and private attribution process supported by evidentiary presentation and transparent cost imposition. Signing formal agreements that build direct communication channels between adversaries appears daunting, but the precedent of maritime cooperation during the Cold War and present-day territorial contests in the western Pacific confirms that they are both possible and necessary. These communication channels for attributing cyber incidents free government entities to handle minor attacks within their jurisdictions, avoiding escalating and non-useful public outcry, and encourage nations to correct rather then defend impermissible cyber activity.

How would a cyber attribution channel function? The maritime environment offers a compelling starting point, but here the greater complexity of cyberspace provides unique challenges. The attribution channels could resemble those agreed to under INCSEA, where designated government officials meet yearly to address grievances and issue reprimands. Government representatives can also review actions taken to correct previous complaints and demonstrate progress. But the cyber domain presents new challenges not replicated in the maritime domain, including the diversity of actors, lack of legal structure, and potentially zero-sum competitions. Because of this, cyber attribution channels should be enforced by global institutions and courts, and they must provide accountability. Cyber enforcement may take form as a hybrid of maritime structures and existing precedent such as the dispute settlement system within the WTO—where no judgment is passed during consultations. However, like in the development of UNCLOS and INCSEA, the UN and other governing bodies must be proactive in developing even imperfect solutions so that cyber law precedents and conflict resolution can develop and flourish.

Adversary Detection and Characterization

Most surface activity in the maritime environment is economic, and these vessels prefer to be discovered and identified quickly to comply with maritime rules that ensure safe navigation. Because visual or electronic signatures can be nominal, technologies such as the Automatic Identification System (AIS) and Identify Friend or Foe (IFF) are used for identification in the maritime domain—but these signatures can be falsified, and these actions face harsh penalties on discovery. Similarly, cyber actors can hide their identities using IP address masking via virtual private networks, or with stolen information from a phishing scheme. So how should cyber governance consider activity that is designed to be unseen? The maritime domain again offers a useful starting point.

Submarine and cyber technology present similar detection and characterization challenges, and offer insights into attribution methods that best serve national interests. Submarines revolutionized naval warfare by introducing the ability to remain undetected. Like cyber actors, this advantage makes them a strategic asset for missions of intelligence gathering, surveillance, and electronic attack. Submarine detection relies on technical clues including electromagnetic frequencies, equipment signatures, platform type, location,

and tactical methods to characterize and interpret intent. Further complicating identification, foreign-produced submarines can belong to a host of supplied countries. When submarines are successfully discovered, knowing their production nationality, type, class, and objectives is an imperfect process with varying confidence levels. Additionally, nations are disinterested in presenting detection evidence to protect secret capabilities. In spite of these challenges, national defense prerogatives require nations to act even with imperfect confidence on the characterization of the attack, and article 51 of the UN charter extends self-defense rights to imminent network activities that constitute an armed attack, or imminent threat thereof.[11]

Takeaways

Nations that respectfully cooperate to address malicious cyber activity are better off. Due to their classified nature, nations are quick to deny responsibility when faced with public attributions for cyber or maritime activity. However, the proliferation of cyber actors and the increasing cost of damages compel countries to take defensive actions on these forensic discoveries. Successful conflict resolution processes require nations to collaborate with public information and evidence to determine the attacker's sponsoring organization and motivations prior to public accusation, which helps to disseminate the burden of proof. In the eyes of the international community, these collaborative methods reinforce subsequent public attributions in the event the undesired activity continues.

Public attribution plays an important part of a structured, diplomatic approach to resolving conflict in cyberspace, but requires established mechanisms and norms for proper efficacy. This chapter uses the precedent of the maritime domain to make three recommendations for the development of international cyber policy.

First, UNCLOS success highlights the need for international agreements to define and enforce norms in cyberspace. These multilateral negotiations must define server boundaries, classify prohibited targets such as critical infrastructure or intellectual property, and categorize appropriate protocols for addressing unwanted cyber behavior.

Secondly, nations must establish channels for addressing cyber incidents privately before public attributions are required for cost imposition. A stable cyber domain requires intergovernmental mechanisms that can quickly and privately address unwanted behavior at the appropriate public or private level, bounded by a treaty or formal agreement.

The third recommendation contrasts with the elusive nature of submarine activity; private attributions of suspected state-sponsored attacks encourage accused states to police their own cyber infrastructure and hinder illicit nonstate actors, especially on the states' indigenous software and servers. Defining and enforcing cyber norms, maintaining interagency mechanisms of private attribution, and transparent internal policies are attribution models from the maritime domain that can deliver stability in cyberspace.

CHAPTER 2

The Problem With Ill-Substantiated Public Cyber Attribution: A Legal Perspective

FAN YANG

Three Lenses to Interrogate Public Attribution

After a state—either its government or the private businesses therein—suffers a malicious cyber operation by a foreign actor, it is tempting to identify and publicly blame whoever it believes is responsible for the attack. Such cyber attribution efforts entail three generally recognized considerations, which stem from technical, political, and legal perspectives, respectively.

First, the attributing state must technically understand what happened and describe the truth as much as it can. The creation of a factual foundation for attribution is, in large part, a forensic process through signals intelligence to trace the malicious cyber activities back to a machine or a location. Yet pinning down the human actors who physically conducted the operation behind the screen often requires intense corroboration from human intelligence as well; it goes without saying that the ultimate establishment of responsibility falls within the purview of law. States' capabilities in this regard are far from evenly distributed,[12] which will inevitably lead to an asymmetric pattern of attribution practices. Empirical data shows that technically capable states tend to use public attribution more frequently, with their envisaged adversaries fixed on the receiving ends.[13]

Second, after the state has attained a certain level of confidence that it knows the source of a malicious cyber operation, it then has a series of political decisions to make—such as whether, when, and in what form to publicly hold the actor accountable, or whether to call for coordinated action from allies. This political decisionmaking is, of course, "a highly complex process which requires trade-offs of multiple considerations."[14] The accusing state may take into account a complex matrix of political pursuits, including: to show accountability to a domestic constituency; to name and shame the accused; to signal

for the purpose of effective deterrence; to serve as a window to observe possible reactions from the accused state; to hold a state legally responsible and to justify possible measures in response; or to signify a redline that the accusing state wants to draw in service of its efforts to establish norms. Simply put, a state's decision as to the timing, the seriousness, and the form of an attribution represents the final trade-off after a comprehensive evaluation over domestic pressure and interstate relations. In this sense, attribution is ultimately political.

Third, from a legal perspective, attribution means imputation by connecting the offense to an offender according to applicable rules, either domestic or international. For the purposes of this chapter, domestic imputation—such as indictment or sanctions against foreign individuals—is left undiscussed; specific focus is put on the intention to establish state responsibility as per applicable international law. Under this premise, legal attribution can legitimize future responding measures, such as self-defense or other countermeasures the accusing state may take, depending on the nature and severity of the original malicious cyber operations. Ideally, the international legal system should provide clear guidance for attribution. However, as will be discussed, the current body of international law is seriously inadequate on this issue.

It's worthy noting that states may still publicly accuse others of conducting unwanted cyber operations regardless of any clear legal basis for doing so. For example, the United States officially holds that political attribution in the form of official announcements does not require meeting any legal standards in the strict sense.[15] This reflects the complexity embedded within public attribution practice as to its diversified form and purpose. Since this chapter specifically focuses on the intention to hold an accused state responsible under international law, the appropriateness of examining an attribution according to technical, political, and international legal criteria should be clear.

The Problem With Ill-Substantiated Public Attribution

Compared to attribution that is confidentially processed and privately communicated, it's only logical that public attribution should be better supported. To the very contrary, however, public attribution is particularly susceptible to the problem of ill-substantiation—if not the absence of substantiation at all. The fundamental cause is that—to use the language of the three lenses analytical framework—the political desire to publicly blame an adversary state cannot be properly checked and balanced due to technical imparities and the lack of legal restraints. Under strong political impetus to publicly blame its adversary, the technically capable state seems to enjoy taking advantage of the lawless status quo.

The term "ill-substantiated public attribution" refers to a subcategory of reckless public denouncements that assign responsibility for a malicious cyber operation to a state without a solid legal logic of imputation or any adequate accompanying evidence. It's a problem with a moving scale, rather than a simple yes-or-no judgment. Around this concept, two illustrating points are necessary.

First, the appropriate level of substantiation should match the purpose and form of public attribution.[16] Think of an extreme case, for example, in which a state is held publicly responsible for carrying out cyber operations that amount to an armed attack,[17] activating the victim state's right to self-defense. Obviously, such a claim is subject to challenge unless it can be unequivocally supported.[18] A comparable situation is when there is a breach of general international legal obligation, say, of nonintervention, and the accusing state aims to establish responsibility that can justify its future countermeasures. The requirement to support this latter claim should be accordingly downsized.

Second, ill-substantiated public attribution has also instigated normative contentions among states. Since 2015, China, Russia, and other countries have consistently held the position that accusations must be substantiated.[19] The United States and the UK, among others, are firm advocates of the position that international law does not require disclosure of evidence to support accusations; states can, thereby, "act reasonably under the circumstances."[20]

This chapter does not contend that public attribution per se is necessarily a problem; rather, it argues that ill-substantiated public attribution is both unhelpful in securing the political pursuits of the accusing state and potentially detrimental to an orderly cyberspace. To list a few issues:

1. Ill-substantiated public attribution is ineffective for the purpose of deterrence because it's a cheap—and thus less convincing—form of signaling that is insufficient to legitimize possible responding measures.

2. Naming and shaming is unlikely to work as anticipated by the accusing state because reckless finger-pointing may be interpreted as slandering and defamation.

3. Public attribution is treated as a policy tool to ease domestic pressure to react against a foreign malicious cyber operation. But an ill-substantiated—and thus unhealthy—public attribution may breed populism, which will in turn squeeze the policy space.

4. The current asymmetrical pattern of ill-substantiated public attribution is structurally destabilizing because a constantly accusing state may make it normal to point fingers without enough substantiation, while a constantly accused state will grow increasingly resentful and eventually erupt.

5. Ill-substantiated public attribution contributes little—if not being outright detrimental—to norm-building, as it relies on the vacuum of applicable rules.

Legal Deficiencies That Encourage Ill-Substantiated Public Attribution

State responsibility arises when there is a breach of international obligation that can be attributed to the state per international law.[21] Apart from another long-recognized problem regarding the lack of primary rules on cyber obligations, ill-substantiated public attribution is enabled and encouraged by the legal deficiencies in the current body of international law that relates to attribution. The deficiencies are threefold:

1. International rules for attribution are inadequate to cope with cyber scenarios.

2. International legal evidence requirements are underdeveloped in general and insufficient for cyber in particular.

3. Legal consequences for making factually incorrect or wrongful public attributions are not clearly defined.

Attribution Rules

The International Law Commission's (ILC's) draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA),[22] especially articles 4 through 11, represent a fine codification of customary international law on attribution rules. Linking state organs' activity to that state, per ARSIWA stipulations, proves to be less troublesome; it's a different story when it comes to evaluating state responsibility for activities conducted by nonstate actors. Unfortunately, most of the situations that concern cyber attribution are in the latter camp. To address the issue of linking a nonstate actor's behavior to a state, existing proposals *de lege lata* are quite controversial. Two, respectively regarding control test and due diligence, will be examined below.

Regarding the legal standard of the level of control required for attribution to occur, the generally recognized approaches are:[23] the "effective control" test devised by the International Court of Justice (ICJ) in *Nicaragua v. USA*,[24] and the "overall control" test developed by the International Criminal Tribunal for the Former Yugoslavia Appeals Chamber in the *Prosecutor v. Tadic* decision.[25] Some argue that the overall control test should prevail in scenarios of cyber attribution because the effective control test is far stricter and thus may function as "a free pass to state sponsorship of cyberattacks."[26]

This proposal is not a suitable solution for two reasons.[27] First, both the test standards focus on the level of control a state exerts over the non-state actor—thus, they cannot cover cases of attribution when the malicious cyber activities suggests no obvious evidence of control. Second, the overall control standard was explicitly confined to "organized and hierarchically structured groups" such as military or paramilitary units;[28] as a matter of juridical fact, the stricter effective control test has been upheld in determining attribution concerning the acts of individuals or nonorganized groups.

Considering how difficult it is to persuasively demonstrate that a state is effectively or generally controlling a nonstate entity, an alternative would be to hold states responsible for regulating or preventing malicious

cyber operations within their jurisdictions. This is captured by the tendency to incorporate into the international legal principle of due diligence—first recognized by the ICJ in *United Kingdom v. Albania*, also known as the Corfu Channel case[29]—into cyber scenarios. But should we treat cyber due diligence as a primary rule of international obligation over state conduct or as a secondary rule to determine violation? There are competing viewpoints.

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* defines "due diligence" as a substantive obligation;[30] the United Nations Group of Government Experts (UN GGE) report endorses this approach with similar wording.[31] Per this understanding, the original task of attributing malicious cyber operations to a territorial state no longer requires an answer. A new task of legal estimation emerges: whether there is a breach of due diligence obligation. To satisfy this test, it must be proven that the original cyber operation stems from within the territorial state; that it causes serious, adverse consequences about which the territorial state has actual or constructive knowledge; and that the territorial state can but fails to take all feasible measures. Moreover, the original cyber operation must constitute a breach of international obligation should it be conducted by the territorial state.[32]

Turning to the minority approach of due diligence as an attribution rule, the identification of the actual author shifts to the state territory where the malicious cyber operation originated. According to such "indirect" or "imputed" attribution,[33] a state is deemed to be responsible for the cyber operation harming another state rather than for a breach of its due diligence obligation. This unorthodox approach seems a bit excessive. It's no wonder the UN GGE report specifically emphasizes that "the indication that an ICT [information and communications technology] activity was launched or otherwise originates from a State's territory or from its ICT infrastructure may be insufficient in itself to attribute the activity to that State."[34]

In light of these contending viewpoints, misusing and abusing due diligence to forge a legal argument to back up public attribution claims could facilitate ill-substantiation. It's thus important to reiterate the following points. First, due diligence, if imported to the cyber scenario, should be better understood as setting an obligation for a state rather than serving as a way to attribute. Second, the actual occurrence of a harmful cyber incident, which would have been unlawful if conducted by a potentially responsible state, is a prerequisite for the injured state to claim a due diligence violation. Third, even if state responsibility is successfully established along the legal path of due diligence, the responding measures that the accusing state might legitimately take should proportionately reflect the fact that the accused state did not conduct the malicious activities but, less harmfully, failed to address them with all feasible measures.

Evidentiary Requirements

General international law has not developed a set of clear rules or consistent guidelines on evidence. Key evidentiary issues such as burden and standard of proof are normally dealt with on an ad hoc basis. For cyber disputes, such ambiguity can be interpreted as a loophole that allows states to carry out malicious cyber activities without consequence; or it can be interpreted as an opportunity that allows states to sometimes make attributions recklessly.

Of those two evidentiary issues, burden of proof is less controversial. It is generally recognized that in "a bilateral dispute over State responsibility, the onus of establishing responsibility lies in principle on the claimant State."[35] Yet, somehow, a shift of the burden of proof has been mentioned as a mechanism specifically tailored for cyber attribution, sometimes referred to as a "virtual control" test.[36] The main argument behind this idea is that in cyber disputes, the origin state for the alleged misbehavior has better access to the knowledge necessary to establish certain facts. This would probably cause more trouble than it intends to solve,[37] as the *prima facie* responsibility of the accused state would be established with a shift of the burden of proof.

Regarding the standard of proof, a comparative assessment of international litigation can identify at least four different levels. In ascending order, these are:

1. The *prima facie* possibility, which requires only indicative evidence of the claim.

2. A preponderance of evidence, which concerns mainly the balance of probabilities of the two sides.

3. The "clear and convincing" standard, which requires the party to prove the factual claims are substantially more likely true.

4. Proof beyond reasonable doubt, which requires a full chain of evidence weighing together heavily toward one direction that is virtually indisputable.[38]

With some room for debate, ICJ cases and state practices support the "clear and convincing" standard for self-defense cases.[39] For disputes with lower-level severity, a generally accepted principle—although without any specifics—is that evidentiary standards should vary along a sliding scale based on the severity of the offense. Extant cases that adopt the "preponderance standard" are mostly regarding territory disputes, which rarely involve state responsibility.[40] From these premises, two deductions can be safely made. First, the adequate level of evidence for cyber public attribution should lie around the "clear and convincing" standard. Second, in any event, sufficient evidence to allow crosschecking can be a proper guideline.[41]

Some may disfavor setting an evidentiary standard. They may argue that the assessment of the adequacy of evidence is only meaningful in a legal forum, but most cyber public attribution cases won't ever go through litigation. This seemingly realistic viewpoint neglects the fact that clarity about the amount and quality of evidence has its merits. According to Kristen Eichensehr, "Even if setting an evidentiary standard decreases the total number of public attributions, having fewer *credible* attributions is preferable to having a greater number of ill-founded or erroneous attributions."[42]

Another opposing viewpoint is that it is hard to reconcile the evidentiary requirement on cyber attribution on one hand with the necessity to make a timely attribution on the other.[43] This dilemma indeed exists. It should be subject to careful evaluation in specific contexts. But challenges in collecting and exhibiting evidence should not excuse evidence-less accusations.

Erroneous Attribution

If a state makes a cyber attribution with facts that turn out to be erroneous—or, even more seriously, if it carries out self-defense or countermeasures against an accused state based on ill-substantiated allegations—what legal consequences should the accusing state face? Underdevelopment of this legal issue provides extra room for ill-substantiated public attribution because no foreseeable punishment exists for irresponsible or erroneous allegations.

To begin with, it's safe to infer that once the attribution proves to be based on false facts, the international wrongfulness of the subsequent self-defense or countermeasure adopted by the accusing state cannot be unquestionably eliminated. In other words, the accusing state may be held responsible for taking unjustified steps.

If the accusing state argues that it has used its best judgment and built its case for attribution on all then-available evidence in good faith, could claims of "reasonableness" and "honesty" exonerate its false judgment? Positive view is echoed by some scholarly papers,[44] as well as official statements.[45] For example, the *Tallinn Manual* explicitly asserts that "the exercise of the right of self-defense . . . is subject to the existence of a reasonable determination that an armed attack is about to occur or has occurred, as well as to the identity of the attacker. This determination is made *ex ante*, not *ex post facto*. Their reasonableness will be assessed based upon the information available at the time they were made, not in light of information that subsequently becomes available."[46]

Opposite views opine that with good faith or not, wrongful attribution in the first place will nonetheless make subsequent measures the fruit of a poisonous tree. The ILC holds that if, during an *ex post* examination, the attribution turns out to be wrongful because of errors in ex ante factual assessment, the mistaken state may be subject to responsibility whether its agents acted in good faith or not.[47]

Lastly, what if the accusing state makes a public attribution that later proves to be wrong, but it did not take concrete measures originally? Although the accused state does not suffer from the responding measures, harm to its fame and reputation has still been inflicted. Under such circumstances, should the accusing state be held partially responsible for the false attribution (which might have been intentional)? Would not holding it responsible encourage more ill-substantiated public accusations? This issue deserves more international discussion.

Toward a Norm on Responsible Public Attribution

Against the challenges posed by ill-substantiated public attribution, tentative solutions should be sought along the three lenses analytical framework, with due considerations paid to the technical, political, and legal dimensions. As this chapter focuses on the legal lens, an international norm on responsible state behavior in public attribution thus seems to be a possible way forward.

In this regard, the UN GGE has provided a sound basis by repeatedly emphasizing in its final reports that "the accusations of organizing and implementing wrongful acts brought against States should be substantiated."[48] Righteous in its nature, though, this norm only points out the need for accusations to be substantiated but fails to elaborate how. Vis-à-vis the legal deficiencies previously discussed, a norm on responsible public attribution should embody the following points.

Starting with an out-of-the-box thought and a preliminary norm: states should make a formal request of consultation before making cyber attribution public; such consultation should be mandatory, confidential, and within a time limit. Such minor improvements to the process have proved to be rather useful in cutting down interstate disputes in other fields of international law, such as the World Trade Organization dispute settlement mechanism.[49] If a similar mechanism exists in cyber conflict, the accusing state then has a way to consult privately with the accused state, seeking to have its interests met without forcing the latter into an awkward position. Most importantly, the substantiation problem may not be that contentious at this stage.

In a combined norm on the rules of attribution, evidentiary requirements and legal consequences of erroneous attribution could be termed as:

1. A state cannot be held responsible under international law solely because a problematic ICT activity was launched or otherwise originated from its territory or from its ICT infrastructure.

2. A state should substantiate its public attribution with an adequate level of evidence for crosschecking, by default to the extent of establishing a clear and convincing case, depending on the purpose and severity of its claim.

3. A state should refrain from taking responsive measures based on public attribution that has been inadequately substantiated, and it may take corresponding responsibility for making an erroneous or falsified attribution.

Before ending this chapter, it should be mentioned that entities other than states can also publicly attribute blame for a cyber operation, but for different aims and subject to different rules, if any. Private corporations, usually cyber security firms, may aim to enhance their influence, cultivate market demands, and ultimately cash out by selling products, services, and solutions on cybersecurity. Media may simply want an eye-catching story and may be easily manipulated by customized feeds of source information provided by enterprise or state organs. Since it falls outside of the purview of international law, the ill-substantiated public attribution problem with these entities merits a separate piece of analysis.

CHAPTER 3

The Purposes of U.S. Government Public Cyber Attribution

JON BATEMAN

Over the last ten years, U.S. government officials have publicly attributed dozens of cyber operations to foreign state-affiliated actors.[50] These public attributions have come in various forms, including formal statements, remarks by U.S. leaders and officials, indictments by the Department of Justice, sanctions announcements by the Department of the Treasury, and press leaks by anonymous government officials. These many public attributions have named multiple states and exposed cyber activities ranging from targeted espionage to indiscriminate destructive attacks. The pace of U.S. government public attributions has generally increased over time.

What is the purpose behind these public attributions? There is probably not a single, overarching goal that explains them all. Rather, the U.S. government appears to have multiple objectives that often (though not always) overlap with and reinforce each other. The importance of each objective likely varies based on specific circumstances and the views and priorities of U.S. leaders and officials serving at the time. Further complicating the picture, U.S. officials and outside experts have used a range of varying, evolving, and sometimes ambiguous terms and categories to describe these policy objectives.

This chapter seeks to clarify U.S. objectives by providing a single framework that synthesizes what can be learned from U.S. official statements and explanations—as well as expert analysis—of public attribution.[51] The chapter specifically focuses on what might be called "government-to-government attribution," meaning public U.S. government accusations that name a foreign government as responsible for a certain cyber operation.[52] Thus, it does not address attributions published by U.S. private companies or the media (unless these cite U.S. government sources), nor does it address U.S. government attributions of foreign individuals or organizations that stop short of directly implicating a state. This chapter mainly focuses on *why* U.S. leaders use public attribution, rather than *how* public attribution occurs (such as who makes the statement, what communication channel is used, and how much evidence is released). Finally, the chapter

does not express an opinion on whether U.S. public attributions are effective in achieving their goals; rather, it briefly describes American policy debates and common expert views on this question.

Cyber "Deterrence," Disruption, and Defense

U.S. officials almost always invoke the language of deterrence, cost-imposition, and accountability to explain their use of public attribution. While specific terms and ideas vary, the common thread is that public attribution can help punish foreign states for unacceptable cyber operations and thereby shape their future behavior. For example, under the administration of former U.S. president Donald Trump, the National Cyber Strategy stated that public attribution can help impose "consequences for irresponsible behavior that harms the United States and our partners."[53] Sasha Romanosky and Benjamin Boudreaux surveyed fifteen senior American career technology, government, or policy professionals about public attribution and found that "promot[ing] deterrence in cyberspace" was their most commonly given explanation for U.S. government public attribution.[54]

However, "deterrence" can mean many different things. Below, deterrence and related objectives are divided into three subcategories, some of which could be alternatively characterized as disruption or defense.

Influencing Foreign States' National Cyber Policy

First, public attribution can aim to dissuade the accused state (and other states) from carrying out certain types of cyber operations. For example, then Federal Bureau of Investigation director James Comey said in 2016 that "by calling out the individuals and nations who use cyber attacks to threaten American enterprise . . . we will change behavior."[55] Kristen Eichensehr called this objective "macro-level deterrence," because the goal is to achieve significant changes in foreign states' national-level cyber operations policy—that is, to dissuade them from conducting entire categories of cyber operations.[56]

The logic—or hope—is that publicly accusing a specific government of a malicious cyber operation will embarrass that government or subject it to international (or domestic) criticism, potentially motivating that government to stop such operations. This is sometimes called naming and shaming. In 2020, following the U.S. public attribution to Russia of cyber attacks against Georgia, then secretary of defense Mark Esper said, "when it might make sense, to name and shame, to call groups out—either groups or governments—we should do that."[57]

Most U.S. cyber experts believe that significant macro-level deterrence cannot be achieved by naming and shaming alone. The reputational costs to the accused state are simply not as great as the gains received from conducting cyber operations. Recognizing this, the U.S. government often pairs its public attribution statements with more tangible actions, such as sanctions and indictments. (In fact, U.S. law requires the government to publicly name the targets of its sanctions and prosecutions. Public attribution, then, is not always done for solely its own sake but is sometimes intended to enable these other U.S. responses.)

That said, sanctions and indictments have been criticized on much the same grounds as public attribution: their practical impact is too small to achieve much macro-level deterrence.[58] Sanctions are

often applied to individuals without significant ties to the U.S. banking system, and U.S. indictments rarely lead to the arrest or extradition of foreign actors charged with conducting state-sponsored cyber operations.[59] U.S. officials sometimes acknowledge these actions as limited, albeit necessary, steps toward achieving international accountability and shaping state behavior. In 2019, then assistant attorney general for national security John Demers called cyber indictments "just a piece of the puzzle."[60]

In search of stronger deterrence, the U.S. government may also combine its public responses with actions taken in private. In his 2020 remarks, Esper said that public attribution should be "on a case-by-case situation, but clearly we have to do more than just play defense and we have to play more of an offensive game." He then referred to Trump's decision to give the military more authority to conduct cyber operations, implying that Washington might undertake cyber counterstrikes against the countries it publicly accuses.[61]

With cyber counterstrikes, unlike sanctions and indictments, U.S. law does not require the government to make any public accusations. Still, all these tools are fundamentally related to public attribution because the U.S. government believes that macro-level deterrence requires their combined, synchronized, and repeated use over time (ideally, in concert with allies). For example, when announcing the public attribution of the Microsoft Exchange hack and other cyber activities to China, a senior U.S. government official twice emphasized that "no one action can change China's behavior in cyberspace."[62]

Public attribution may also aim to achieve macro-level deterrence of other actors beyond the accused state. After all, the public exposure of one state's cyber activities can provide a general global signal of U.S. attribution capabilities and intentions. In 2015, then director of national intelligence James Clapper testified that "most [cyber actors] can no longer assume that their activities will remain undetected. Nor can they assume that if detected, they will be able to conceal their identities. Governmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions."[63] By comparison, discreetly sharing a U.S. attribution privately with the accused state would not send this broader deterrent signal to other countries and actors.

The effectiveness of public attribution for macro-level deterrence is debated in Washington. Critics observe that U.S. public attribution—even combined with indictments, sanctions, cyber counterstrikes, and other actions—have failed to inflict significant costs on the exposed states. These critics note that state-sponsored cyber operations against U.S. entities have grown in number and severity over time. Thus, public attribution and related actions have obviously not achieved a large amount of macro-level deterrence.[64]

On the other hand, the United States has not yet suffered a truly catastrophic cyber attack. This suggests that some degree of macro-level deterrence does exist; perhaps sustaining such deterrence depends, in part, on repeated public demonstrations of Washington's ability to attribute cyber operations. Furthermore, complete macro-level deterrence is too high a bar for public attribution or indeed any U.S. policy tool to achieve, given the powerful incentives that foreign states have to conduct cyber operations. More realistically, Washington can aim for public attribution to make modest but tangible contributions to macro-level deterrence.

An oft-cited example is the 2015 U.S.-China cyber agreement, which established mechanisms for bilateral dialogue and committed both states not to "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[65] Many U.S. analysts believe that a combination of public attribution, indictments, and threatened sanctions helped then U.S. president Barack Obama secure this deal. Moreover, U.S. officials and private cybersecurity firms both reported an overall reduction in Chinese cyber espionage against U.S. targets following the deal.[66] That said, the same types of analysis showed that China eventually resumed its previous level of activity.[67] Some U.S. analysts believe that Washington's actions never adequately deterred Chinese cyber espionage, while others believe the nonbinding political agreement fell apart due to a broader breakdown in bilateral relations.

Influencing Foreign Cyber Actors, Officials, and Organizations

Second, public attribution can aim to deter or disrupt the individual cyber actors, mid-level government officials, and units or companies responsible for conducting cyber operations. Eichensehr calls this "micro-level deterrence," because it targets a foreign government's subordinate personnel and organizations rather than its national leadership.[68] For example, then associate deputy attorney general Sujit Raman said in 2019 that "the prospect of criminal indictment can help deter some cyber actors from engaging in such conduct in the first place."[69] The viability of micro-level deterrence—and the manner in which it might work—will depend in part on the structures and incentives that exist within foreign states' offensive cyber programs.

For some individual cyber actors, public attribution can bring a frightening level of international notoriety and foreclose future opportunities in the legitimate cybersecurity industry. Further, indictments and sanctions can limit travel or financial opportunities. These possibilities may dissuade some individuals from working for their government or accepting certain sensitive taskings. (Other cyber actors, however, may wear these punishments as badges of honor.) And for some mid-level government cyber officials, public attribution indicates their failure to ensure adequate operational security and oversight, which could cause internal embarrassment and draw criticism from superiors. (This assumes the cyber operation was not intended to be discovered.)

The exposed cyber organizations may need to conduct temporary operational stand-downs, internal reviews, or counterintelligence investigations. They may choose to cut ties with publicly named individual cyber actors, viewing them as compromised. Cyber organizations may decide to impose burdensome new oversight measures and make costly changes in tactics or infrastructure to avoid future public attributions. All this creates friction and distrust within a state's offensive cyber ecosystem. Such costs would be too small to achieve macro-level deterrence. But, according to Raman, they "can make it more difficult for states to recruit the manpower and resources for cyber-attacks, and raise the cost of engaging in malicious cyber activity."[70] In other words, public attribution can cause modest, occasional disruptions and inefficiencies for the exposed state.

As with macro-level deterrence, micro-level deterrence could extend to individuals and organizations beyond those exposed in a public attribution, including cyber actors in other states. To this end, U.S. public attribution statements often highlight the United States' "capability to remove the Internet's cloak of anonymity" and the intention to hold state-sponsored hackers accountable "no matter who they are,

where they are, or what country's uniform they wear."[71] In theory, then, the public attribution of a North Korean cyber operation could help convince an Iranian not to join a state-sponsored hacking organization.

On the other hand, many U.S. experts believe that micro-level deterrence and its disruption effects have generally fallen over time. As public attribution has become a more routine event, some foreign state-sponsored cyber actors and units may have come to accept and adapt to the risk of public exposure.

Informing Cyber Defenders

Finally, public attribution can provide information that enables and motivates potential victims and the cybersecurity community to better defend themselves. For example, the White House statement on the Microsoft Exchange hack stated that "by exposing the PRC's [People's Republic of China's] malicious activity, we are continuing the Administration's efforts to inform and empower system owners and operators to act."[72] Some U.S. experts call this "deterrence-by-denial," because better defense can prevent foreign cyber operations from achieving their goals and thus potentially reduce the motivation to conduct them. Even if deterrence-by-denial is not achieved, public attribution can still aim to improve cyber defenses.

The most direct way to "inform and empower" cyber defenders is for the U.S. government to share detailed technical information about malicious cyber operations and actors—for example, malware samples, indicators of compromise, and other tactical signatures. These technical information releases do not inherently require public attribution; however, public attribution can enhance their impact in several ways. Eichensehr notes that "understanding who the attacker is can shed light on intruders' likely targets and goals," helping cyber defenders anticipate and prepare for cyber actors' moves.[73] Public attribution can also illuminate the stakes: potential victims may choose to invest more resources to prevent compromise by a named adversary state. Finally, public attribution can help to capture media coverage and thereby get more cyber defenders to pay attention to a technical release.

The effectiveness of public attribution in achieving deterrent, disruptive, and defensive goals is difficult to assess. An accurate evaluation would require access to detailed intelligence about foreign states' and cyber actors' evolving intentions and reactions to U.S. public attributions. This information, if it exists, is not publicly available. In its absence, independent analysts can use indirect data to assess the efficacy of public attribution. For example, they can examine publicly reported trends in state-sponsored cyber operations to see if public attribution appears to have a demonstrable effect. But public disclosures of cyber operations by private companies and governments provide a very limited, fragmentary view of true trends. Moreover, it is hard to isolate the impact of public attribution from many other causal factors. In sum, the deterrent value of public attribution remains an open question.

International Signaling, Partnerships, Norms, and Laws

Deterrence is not the only goal the United States has for its public attributions. Many experts have highlighted how public attribution can also be used to shape international views, norms, laws, and expectations about the so-called rules of the game in cyberspace. Again, this broad idea can be divided into

three sub-objectives. U.S. officials have embraced each to some degree, although government statements and actions leave some room for interpretation about how Washington understands and prioritizes these different objectives in specific cases.

Signaling to Adversaries

First, public attribution can help communicate to adversaries what kinds of cyber operations the United States considers unacceptable. Given the dearth of clear, strong global norms and laws governing cyber behavior, this sort of signaling is a way to clarify expectations directly among key states, hopefully reducing the likelihood of misunderstanding or conflict. For example, the 2015 Department of Defense Cyber Strategy stated that "the United States used verifiable and attributable data to engage China about the risks posed by its economic espionage. The attribution of this data allowed the United States to express concerns regarding the impact of Chinese intellectual property theft on U.S. economic competitiveness, and the potential risks posed to strategic stability by Chinese activity."[74]

Such signaling does not necessarily require public attribution; discreetly sharing attribution via bilateral diplomatic channels could serve the same function. However, a public attribution broadcasts the message to the entire international community, including other adversaries. For example, the U.S. public attribution of a Chinese cyber operation may also help the Russian government understand what the United States considers unacceptable behavior in cyberspace. Also, public attribution might be taken as a more serious signal than discreet bilaterally shared attribution, because the former is more costly for both the accusing state (it can risk intelligence sources and methods) and for the accused state (it can cause reputational harm).

Rallying Allies and Partners

In recent years, the United States has increasingly sought to undertake public attribution jointly with other states (so-called collective attribution).[75] For example, in 2018, seven nations including the United States publicly attributed the NotPetya cyber attack to Russia.[76] By acting collectively alongside other nations, the United States seeks to magnify the deterrent impacts of its public attributions. Beyond deterrence, joint attributions can provide Washington with a vehicle for building and strengthening international partnerships on cyber issues.

In 2021, the U.S. public attribution of cyber activities by China's Ministry of State Security (MSS) was joined by what the U.S. government called "an unprecedented group of allies and partners — including the European Union, the United Kingdom, Australia, Canada, New Zealand, Japan, and NATO."[77] A senior U.S. administration official suggested that this collective attribution helped to build support among these partners "to enhance and increase information sharing, including cyber threat intel and network defense information with public and private stakeholders, and expand diplomatic engagement to strengthen our collective cyber resilience and security cooperation." Likewise, the official emphasized that "it's the first time NATO has condemned PRC cyber activities," while also noting that "NATO [was also] adopting a new cyber defense policy for the first time in seven years." As this example shows, joint public attribution can help international partners build a shared understanding of cyber threats and provide a rallying point to motivate and organize more concrete collective cyber efforts.

Shaping International Norms and Laws

Scholars frequently argue that public attribution can be used to help develop and reinforce international norms and laws. By exposing otherwise secret cyber operations, public attributions help the international community to "foster agreement on factual reality of what states are doing."[78] And by condemning the exposed cyber activity, the accusing state can express and promote its views on what should be considered irresponsible behavior. For example, John Demers stated in 2020 that "in the past three months alone, the department [of Justice] has charged computer intrusions or taken legal action related to the activities of China, Iran, and North Korea. Each of these cases charged significant and malicious conduct that we have called out in part to reinforce norms of responsible nation state behavior in cyberspace."[79] Over long periods of time, such norms (if expressed in legal terms) might conceivably help to shape customary international law. Conversely, states' failure to publicly expose, attribute, and condemn major categories of cyber operations might result in such operations becoming seen as normatively acceptable and lawful.

On a few occasions, U.S. public attributions have alleged specific violations of international cyber norms, laws, or commitments. U.S. President Joe Biden, in off-the-cuff remarks in July 2021, accused Russia of seeking to influence the 2022 U.S. elections and called it "a pure violation of our sovereignty."[80] That same month, the White House pointed to a newly unsealed indictment of MSS cyber actors, and noted that "much of the MSS activity alleged . . . stands in stark contrast to the PRC's bilateral and multilateral commitments to refrain from engaging in cyber-enabled theft of intellectual property for commercial advantage."[81]

However, those instances are relatively rare. More frequently, U.S. public attribution statements make general condemnations of cyber operations, using terms such as "irresponsible" and "destabilizing," without explicitly claiming that a specific international norm or law was violated. For example, the White House statement on NotPetya called it "reckless" but did not comment on its legality or compatibility with international cyber norms.[82] In such cases, the United States seems unwilling to stake a clear claim about the application of international law and norms to the cyber operation at hand. Instead it offers a more general objection to or criticism of the cyber operation, while preserving room to further develop precise U.S. legal and diplomatic positions over time.[83] Among other reasons, Washington may not yet be ready to constrain itself from conducting similar cyber operations of its own.

In still other cases, U.S. public attribution statements have acknowledged, or at least implied, that the relevant cyber operations did *not* violate any international norms or laws. When James Clapper called China the "leading suspect" for the Office of Personnel Management hack in 2015, he famously added that "you have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute."[84] Though his off-the-cuff remarks attracted controversy in the United States for accepting the Chinese hack as legitimate state behavior, Clapper later affirmed in his memoir that "China had hurt us dearly, but that it hadn't done anything outside the bounds of what nation-states do when conducting espionage."[85] More recently, the 2021 White House statement attributing the SolarWinds breach to Russia called it "malicious," "harmful," and "a national security and public safety concern" but stopped short of alleging any violations of international principles.[86] The United States has so far been reluctant to embrace normative restrictions on national security espionage in cyberspace, although more U.S. experts have begun advocating for such norms.[87]

Domestic Politics and Public Education

Finally, U.S. public attribution may serve domestic purposes. This is an inevitable part of policymaking in democracies (and, to a lesser extent, in non-democracies). While domestic politics can sometimes encourage poor policymaking by U.S. leaders, it can also help to channel the legitimate needs of U.S. constituencies and encourage valuable public discourse.

Domestic Political Motivations

In the wake of a significant cyber incident, U.S. leaders often face domestic political pressure to do something—and, in particular, to take strong action against the perpetrators. If they fail to do so, U.S. leaders may be criticized as weak by the political opposition. In some cases, this pressure may come from the victims themselves. Tim Maurer and Garrett Hinck note that "the March 2016 indictment against a cadre of Iranian hackers was largely in response to demands from big banks for the U.S. to take some kind of public action in response" to Iranian distributed denial-of-service (DDoS) attacks.[88] Additionally, public attribution can help focus domestic political attention on the wrongdoing of an adversary rather than on U.S. cybersecurity failures.

When considering domestic political incentives, it is worth noting that U.S. leaders do not have total control over whether or when such attributions come to light. Private sector attributions or unauthorized leaks by government officials or members of Congress may preempt the U.S. administration. For example, a U.S. senator, not an executive branch official, was the first to openly blame Iran for its DDoS attacks on the financial sector.[89] Mandiant's 2013 "APT 1" report on Unit 61398 of the People's Liberation Army was published more than a year before the Department of Justice unsealed charges against members of that unit.[90] And during the 2020 presidential election, a series of leaks by U.S. officials attributed influence activities to Russia, despite reticence by top Trump administration leaders to publicly acknowledge this attribution.[91] Cases like these may encourage U.S. leaders to quickly publicize cyber attributions because they could be criticized for acting slowly or withholding information from the public if an attribution is later revealed by someone else.

Educating and Galvanizing the Public

Additionally, public attribution can help the U.S. government build domestic political support for many different cyber policies, from greater investments in cybersecurity to more assertive diplomatic action. For the last decade, many senior U.S. national security officials have expressed concern that the American people do not fully appreciate the extent of cyber risks facing the country, and they have sought various ways to raise public awareness.[92] Cumulatively, public attributions create a factual record of cyber threats to U.S. interests. This can help to educate the American people about the breadth, severity, and diversity of cyber threats facing the United States—and, in turn, motivate members of Congress and other political and private sector actors to support policies to address these threats.[93]

Reasons Not to Publicly Attribute

U.S. administrations of both parties have gradually increased their use of public attribution over time. Independent U.S. cyber experts have generally favored this policy, even while they raise questions about its effectiveness in achieving U.S. goals. Still, commentators have identified some potential ways that certain public attributions can be counterproductive or harmful to U.S. interests. These are summarized below, in very rough order of importance.

- The U.S. government does not always have enough confidence in an attribution to justify publicly revealing it.
- Intelligence sources and methods may be compromised or lost. This could spoil opportunities to monitor, defend against, deceive, or disrupt the cyber actor (or other cyber actors).
- Cyber actors, once exposed, may learn from their mistakes and become stealthier.
- Public attribution may create domestic political pressure for a stronger U.S. retaliatory response than the government wants to—or can—undertake.
- Public attribution can cause unwarranted domestic alarm, which may even help adversaries achieve their goals—for example, by sowing doubt about election security.
- Washington may want to avoid bilateral friction during a sensitive period, such as while negotiating with the accused country on a more important topic.
- The accused country may retaliate.
- Quiet diplomacy with the accused state may be more effective in addressing the objectionable cyber behavior.
- U.S. allies and partners may not agree with Washington's decision to publicly attribute a cyber operation.
- If the underlying evidence remains secret, public attribution may fail to convince some audiences.
- Public attribution establishes a precedent that other countries may eventually use to publicly name (and potentially take action against) U.S. government cyber operators.
- Publicly attributing some cyber operations could imply tacit approval of others.

Most of these concerns relate to the merits of public attribution in specific cases, its proper timing, or mechanics. There is little advocacy in the United States for stopping or dramatically reducing the number of public attributions across the board. In fact, the most frequent American criticism of public attribution is that it is insufficient to achieve deterrence and therefore must be accompanied by far stronger cost-imposition measures.

Key Takeaways

Foreign governments like China that object to U.S. public attribution should take account of U.S. objectives and incentives. Understanding what U.S. leaders and officials seek to accomplish and why can help reduce the risks of misinterpretation, promote cyber stability, and potentially facilitate diplomacy. There are several major takeaways:

- **Public attribution is a well-established U.S. policy tool.** Although each U.S. administration chooses to publicly attribute some cyber operations and not others, there is a clear trend toward greater public attribution over time. The U.S. government has multiple, overlapping objectives that often reinforce each other and make public attribution all but inevitable for some major cyber operations.

  U.S. debates about the efficacy of public attribution mostly focus on whether Washington should seek to impose even stronger costs on foreign state sponsors of cyber operations—not whether the U.S. government should restrain the use of tools such as public attribution. Arguments against public attribution tend to be about the specific circumstances and timing; there is little advocacy for abandoning the tool. In the words of Florian Egloff, "The use of public attribution as a means of statecraft in national security policy is here to stay."[94] Indeed, more U.S. allies and partners (and other states, such as Iran) have also increased their use of public attribution in recent years, suggesting a growing international appreciation of its utility.

- **Public attributions do not always have the same objectives.** Although Washington's overall use of public attribution is settled policy, the objectives for each instance seem fluid. Public attributions are considered on a case-by-case basis, and U.S. officials offer varying descriptions of their specific purposes and meanings. Sometimes these messages are ambiguous, suggesting that American policymakers are still working to refine their practices and resolve possible tensions between different policy objectives.

  For example, the U.S. government hopes that public attribution can affirm international norms of responsible behavior in cyberspace. But it also publicly attributes certain cyber operations that do *not* violate international norms, on the grounds that these operations are still hostile and must therefore be deterred. Because U.S. objectives can vary from case to case, observers should carefully parse U.S. government statements and actions for clues about what message Washington is trying to communicate with a specific public attribution.

- **Public attribution is usually part of an integrated U.S. response to cyber operations.** It has become rare for the U.S. government to publicly attribute a cyber operation while taking no other responsive action. American leaders understand that public attribution alone—like other individual U.S. policy tools used in isolation—cannot achieve objectives such as deterrence. That is why Washington generally uses public attribution in concert with other responses, such as sanctions, indictments, technical releases, intelligence sharing, coordinated defense among international partners, and cyber counterstrikes.

In other words, public attribution is not fully discrete from the rest of U.S. cyber response policy. Rather, public attribution should be understood as supporting, and being supported by, other U.S. actions. The United States aims to achieve its objectives by combining multiple policy tools together, sustaining their use over time, and acting in concert with allies and international partners whenever possible.

- **Public attributions accurately reflect U.S. government assessments.** Research for this paper did not identify any U.S. government public attributions that were later proven wrong, let alone any that were deliberately concocted or falsified. In all of the instances examined, the U.S. intelligence community, federal law enforcement, and other agencies appear to have sought in good faith to assess and report who was responsible for cyber operations.[95]

  U.S. leaders choose whether, when, and how to publicize agencies' internal attributions. In the overwhelming majority of cases examined, U.S. leaders' public statements seem to have accurately described U.S. intelligence assessments. To definitively confirm this would require access to classified information. That said, the possibility of leaks, whistleblowing, or contradictory reports by private companies helps to serve as a check on any attempts by U.S. government officials to inaccurately convey cyber attributions.

  The Trump administration, as in many other areas, provided some partial exceptions to this general pattern of truthful cyber attributions. Trump administration officials publicly denied that Russia was supporting the president's reelection, even though U.S. intelligence analysts had assessed the opposite. Additionally, the Trump administration publicly implied that China's rhetorical opposition to U.S. policies was intended to undermine the president's reelection prospects, even though intelligence analysts had assessed otherwise. Neither of these cases involved falsely attributing actions that the accused government did not in fact do; rather, the Russia case involved falsely *denying* an attribution, and the China case involved *mischaracterizing* publicly visible behavior. In both cases, public signs of the distorted intelligence quickly emerged, and the issues were eventually addressed by internal investigators, reported to Congress and the public, and corrected by the Biden administration.[96]

CHAPTER 4

Beyond Public Cyber Attribution: Reflections and Responses

XU MANSHU

In recent years, state authorities and corporations increasingly have publicly attributed cyber incidents to states or other entities.[97] Yet the fact that cyber attacks continue to occur suggests that public attribution is not stopping them. Moreover, public attribution itself causes disputes and tension among major powers, including the United States and China. This chapter seeks to identify approaches that will reduce the risk of escalating confrontation between accusatory state and accused states.

Although there may be many possible intentions and drivers of public attribution, this chapter assumes that the ultimate purpose of attributing states is to stop and prevent cyber incidents. On the basis of this assumption, the chapter aims to explore available options to ameliorate the negative effects of public attribution from the perspectives of technology, politics, and international governance. Specifically, this chapter aims to answer three questions by providing diversified options for decisionmakers to respond to cyber incidents:

1. Technically, how can cyber incidents be responded to effectively?

2. Politically, how can public attributions of cyber incidents be prevented from escalating confrontation?

3. How can the international community jointly combat malicious cyber activities?

The Technical Perspective: Effective Responses Beyond Public Attribution

For research on governmental public attribution as an element of security policy, one can split the public attribution process into two phases: mechanisms that lead to public attribution and what happens after an incident is publicly attributed.[98] Attribution of malicious cyber activity can be focused on a machine, on a specific person pressing the keys that initiate that activity, or on a party that is deemed ultimately responsible for that activity.[99] Herbert Lin argues that which type of attribution is relevant depends on the goals of the decisionmakers involved.

Generally speaking, the machine that initiated the cyber attacks is likely to be identified as technical forensics are relatively accurate. However, some technical indicators themselves are likely to be altered or manipulated by attackers who want to deflect responsibility onto someone else. It is more difficult to trace the activity back to a specific person or party. This demands more technical means and intelligence resources, which are usually not disclosed by the attributer. Reasons for nondisclosure may include preventing the exposure and consumption of intelligence resources (which are often mentioned in statements of public attribution) or covert technical methods in the name of public security and national security (including the use of back doors and vulnerabilities, which may incur international criticism and scrutiny).

It is worth noting that while victims frequently assign responsibility for a cyber attack to one country, the deductive logic of attributing responsibility for cyber attacks to one country has become more complicated. Cyber attacks have changed a great deal and taken on new features.

First, cyber attackers can use the domestic infrastructure of their target country to carry out the attack. For example, in the SolarWinds cyber incidents, the attackers used a cybersecurity management software provider—a U.S. federal contractor—and local U.S. cybersecurity companies as the carrier. This exploitation of trust allowed the attackers to cover up their malicious operations in a legitimate way and enable precision attacks on government agencies and critical infrastructure in the United States.

Second, cyber attacks are more commercial than ever before; an international industry is popping up around them. Advanced persistent threat actors are increasingly making use of widely available commercial tools such as virtual private networks.[100] Many organizations provide ransomware services, with core developers maintaining ransomware and payment sites and recruiting affiliates carrying out attacks and disrupting victim networks. In return, any ransoms paid by victims are split between core groups and affiliates, which typically receive 70–80 percent of the total.

Third, cyber attackers have adopted new tactics. Since the first global outbreak of the NotPetya ransomware attacks in 2017, there have been many new variations of ransomware, and the tactics of ransomware attacks have changed. Some ransomware attackers are increasingly using stolen data for extortion without having a direct impact on systems or businesses. So-called double blackmail has become an important mode of extortion, which not only forces victims to pay a ransom by obtaining decryption tools but also steals data before encrypting and locking the system, thus coercing the victim to pay lest the stolen data be leaked or deleted. Cyber attackers have also recruited corporate insiders, offering high pay for help

with the attack. Consequently, the diversity of malicious nonstate actors—all with differing motives—has resulted in malicious cyber activities occurring more frequently and made accurate attribution more difficult.

Ransomware attacks against the Colonial Pipeline, JBS Foods, and Kaseya in the United States revealed three realities for the target systems. First, energy, healthcare, and educational institutions have become important targets. Hackers exploit the large number of access points and inadequate protection measures on online platforms. Second, there are significant vulnerabilities in critical infrastructure. Finally, the failure to repair high-risk vulnerabilities after disclosure is also an important factor in leaked data, which are often used by ransomware organizations.

Even if cyber attacks could be accurately attributed, it is remarkably difficult to change the behavior of an attacker. Considering the limited resources and time, therefore, it is more practical and effective to prioritize strengthening one's own cyber defense capabilities. Based on the United States' experience, improving cybersecurity defense capabilities and modernization levels may reduce the number of ransomware attacks that seriously affect critical infrastructure businesses.

This chapter, therefore, argues that strengthening cyber defenses may be a more proactive and effective approach than public attribution. To name just a few, the following measures are more practical and efficient steps to take after a cyber attack than public attribution:

1. **Find out the attack mode from the logs of the target system.** The top priorities should be identifying the way that attackers entered the target, the scope of the target being attacked, the computer code used in the attack, and the consequences of the attack—all of which can be collected by the victim's side.

2. **Cut the fund chain.** For example, in 2021, the U.S. Treasury Department announced the first-ever sanctions against a cryptocurrency exchange—the Russian-linked Suex—for facilitating ransom transactions for ransomware gangs and helping them evade sanctions. Suex is registered in the Czech Republic but has no physical presence there. Instead, it operates out of branch offices in Moscow and Saint Petersburg, with other Russian and Middle Eastern locations.[101] The action is aimed at disrupting the ransomware group's main channel for collecting ransoms from victims.

3. **Strengthen legislation and guidelines to improve cyber defense.** It is extremely important to take compulsory measures to report cyber incidents and patch vulnerabilities in order to respond quickly and prevent similar attacks from happening again. For example, after the ransomware attacks in 2021, the Chinese government took new measures to defend against cyber incidents. National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT) issued its "Guide for Preventing Ransomware Attacks,"[102] and the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), and the Ministry of Public Security issued the "Regulations on the Management of Security Vulnerabilities in Network Products" (网络产品安全漏洞管理规定),[103] and the State Council

issued the "Regulations on the Protection of Critical Infrastructure" (关键信息基础设施安全保护条例).[104]

4. More fundamentally, improve cybersecurity capabilities by deploying advanced security technologies. For example, the White House Office of Management and Budget issued its "Zero Trust Cybersecurity Principles." The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released the "Zero Trust Maturity Model" and "Cloud Security Technology Reference Architecture." Together, these documents form a cybersecurity architecture road map for federal agencies at all levels, setting benchmark performance goals for critical infrastructure owners and operators, and implementing the zero-trust security concept of "never trust, always verify" through maturity models as agencies' systems and businesses migrate to the cloud.

These steps are the right way to boost cybersecurity. In addition, the enhancement of cyber defense will increase the difficulty of carrying out cyber attacks, which can stop cyber attackers—to a certain extent.

The Political Perspective: Preventing Public Attribution From Escalating Confrontation Between States

The second step of public attribution—information dissemination—is actually a process of political decisionmaking. Public attribution is a political choice made by the victim state based on its own national interests. But if the public attribution seriously affects the interests of the accused state, it will also likely lead to retaliation. So can cyber attacks actually be stopped by blaming another country? Obviously, the answer is no.

Understanding the internal rationale of waging a cyber attack is critical here. From a technical point of view, two facts emerge. The first is that the interconnectedness of the internet has enabled remote operation of the physical world through cyberspace. The second is that vulnerabilities or back doors in the code of information and communication technology (ICT) products, services, mechanisms, and protocols have become a necessary condition for remote control. Until the security of ICT products and services is improved, cyber attacks by states as well as criminal organizations will never stop. Neither of these technical truths can be eliminated by blaming a single country for a cyber attack. It is the poor quality of ICT products that has created opportunities for cyber attackers of various motivations.

From the perspective of politics and diplomacy, confrontation in cyberspace not only reflects structural contradictions between countries but also increases the intensity. The emergence of cyberspace has given states new tools that are covert, flexible, and relatively low cost and high yield. Cyber intelligence collection, critical infrastructure attacks, information influence operations, have become primary ways for states to confront each other in cyberspace.

Consider, for example, the ongoing cyber conflict between the United States and Russia. In June 2019, Washington announced that it was deploying offensive malware against Russia's power grid to prevent

Russia from implementing selective blackouts in key U.S. states during the 2020 U.S. elections. In late 2020, however, the United States discovered that Russian hackers had developed the ability to hit critical U.S. infrastructure—including power, energy, water, and communications—through the SolarWinds cyber attack. According to FireEye CEO Kevin Mandia's testimony at a congressional hearing in February 2021, the attackers conducted a "dry run" of the attack in October 2019, before the actual attack occurred between March and June 2020.[105] The chronology of the two incidents, as reported by the media, has prompted outside observers to infer that the SolarWinds cyber attack may have been Russia's response to the U.S. Cyber Command's strategic practice of so-called persistent engagement.

On March 8, 2021, White House Press Secretary Jen Psaki said the U.S. government was prepared to take "a mix of actions seen and unseen" in response to Russian cyber attacks, but said the White House would not "publicly discuss certain aspects of our response."[106] On May 7, 2021, the Colonial Pipeline Company, the largest fuel pipeline in the United States, proactively shut down its pipeline system in response to a ransomware attack.[107] On May 10, 2021, the Federal Bureau of Investigation confirmed that "the Darkside ransomware is responsible for the compromise of the Colonial Pipeline networks."[108] President Joe Biden explained that "so far there is no evidence based on, from our intelligence people, that Russia is involved, though there is evidence that the actors, ransomware, is in Russia. They have some responsibility to deal with this."[109] So it might as well be assumed that if the United States military did carry out cyber attacks on Russian military and intelligence systems, the subsequent series of ransomware attacks on the United States could be logically undestood as retaliation by Russia.

Cyber interactions between North Korea and the United States offer another illuminating example. In the wake of the Sony hack, the United States disrupted North Korea's networks and then U.S. president Barack Obama issued an executive order imposing sanctions on ten North Korean individuals and three entities linked to the North Korean government.[110] North Korea did not immediately respond. But by October 2017, FireEye reported that North Korean hackers had successfully used phishing emails to infiltrate the networks of several U.S. electric companies for early-stage reconnaissance and "North Korea linked actors are bold . . . and have little concern for potential discovery and attribution of their operations."[111] In 2020, the U.S. government said North Korean hackers had manipulated the systems of financial institutions in nearly forty countries. The U.S. Departments of State, the Treasury, Homeland Security, and Justice issued a joint statement noting that North Korea is targeting banks in several countries to make fraudulent international transfers.[112]

In these cases, publicly attributing cyber attacks did not change the behavior of the accused states. Rather, public attribution made it more difficult to reach a compromise with the opposing sides and more likely for the adversary to seek revenge. Regardless of the gap between different nations' cyber capabilities, cyber attacks are often the most attractive choice for a state. If a cyber dispute between two countries falls into a cycle of attack and retaliation, political negotiations are a necessary step toward deescalation. These negotiations must go beyond the subject of the cyber attacks themselves and take into account a broad spectrum of national concerns and interests.

For instance, direct mediation between the Chinese and U.S. heads of state helped settle the 2013–2015 cyber espionage dispute between the two countries.[113] U.S.-Chinese relations were strained on the eve

of President Xi Jinping's visit to the United States in 2015 due to the combined effects of the Mandiant report, the Edward Snowden disclosures, the U.S. judicial prosecution of five Chinese military officers, and the U.S. Office of Personnel Management data breach. Under the direct instructions of the two heads of state, the envoys of the two countries conducted urgent visits. Then U.S. national security adviser Susan Rice visited China on August 30, during which the two sides discussed a range of sensitive issues, including cybersecurity. Although the two countries have differences over cyber attacks, official press statements did not mention them.[114] On September 9, 2015, Meng Jianzhu—Xi Jinping's special envoy and a member of the Political Bureau of the Chinese Communist Party (CCP) Central Committee and secretary of the CCP's Central Political and Legal Commission—visited the United States. Two days later, on September 11, the two sides said that they had reached an "important consensus" on prominent issues of cybersecurity.[115] Finally, on September 25, Xi and Obama held a joint press conference to announce a landmark agreement on cybersecurity.[116] Although China had previously rejected the distinction between acceptable national security spying and unacceptable economic espionage,[117] the two sides agreed that "states should not conduct or knowingly support misappropriation of intellectual property" and "ICT cyber security regulations should be consistent with WTO agreements."

The U.S.-Russia summit in June 2021 can also be seen as an important factor in the reduction of blackmail attacks. During talks in Geneva, U.S. President Joe Biden gave Russian President Vladimir Putin a list of sixteen key infrastructure areas, from energy to water, that should be off-limits for malicious cyber activity. The two heads of state also agreed to have cybersecurity experts from both governments "work on specific understandings about what's off-limits and to follow up on specific cases that originate in . . . either of our countries."[118] According to Kommersant's Russian sources, in a few months Moscow and Washington managed to resume cooperation in areas that had been frozen for many years. As a result, the Evil Corp., TrickBot, and REvil cyber groups were hit.[119]

Once the leaders reach a consensus, states can discuss implementation. This requires flexibility. New mechanisms can be established, old approaches can be revived, and cyber issues can be added to traditional security dialogue and consultation mechanisms. If there are cyber attacks involving national security and intelligence, they should be discussed at a very high level through strategic dialogue channels. If cyber attacks involve critical infrastructure protection or the financial sector, they could be addressed through cooperation and consultation mechanisms to combat cyber crimes.

The International Governance Perspective: Combating Malicious Cyber Activities Beyond Collective Public Attribution

Another way to publicly attribute a malicious cyber activity is collectively through an alliance of actors. When a government-led public attribution fails to provide sufficient evidence of blame, the country can choose to cooperate with other governments and lean on the credibility and political influence of a coalition to prescribe responsibility for a cyber incident. In 2017, for example, the ransomware NotPetya spread around the world after attacking Ukraine, causing billions of dollars in damage by infecting companies and governments in Europe, Asia, and the Americas. The governments of the UK, the United States, Denmark, Australia, Canada, and New Zealand all issued public attribution statements within

a week, unanimously blaming the Russian government for NotPetya. In general, establishing a public attribution alliance strengthens the claim of responsibility in cyber conflict (the fundamental objective of a public attribution alliance), promotes collective action by the alliance, and helps to shape international rules in cyberspace.

Collective public attribution may enhance a claim's credibility, but it cannot change the nature of public attribution. Collective public attribution is still a strategic choice made by the states according to their political needs. In essence, they are still deriving their conclusion from the comprehensive analysis of technology and intelligence, and the content is still a new way to package the nonconfidential information such as data forensics and incident response.

Specifically, collective public attribution has not yet solved three major challenges of identifying responsibility in cyber incidents. The first is the uncertainty of cyber attribution—attackers make full use of the anonymity of cyberspace to conceal and mislead their nature. The second is how to attribute the action to personnel in the accused country, which involves the acquisition of overseas information and is thus both complicated and sensitive. The third is how to persuade the public through a confidential attribution process. As a non-legal scholar, I argue that public attribution—including collective public attribution—cannot help a government earn international legitimacy for their retaliatory actions against other countries, nor can it serve as a legitimate basis for exercising collective self-defense in cyberspace. I do hope there will be more professional discussion on this from legal experts.

Fortunately, it is in the common interest of the international community to combat malicious cyber activities. Under the multilateral framework, the international community could work together to establish an international cyber attribution mechanism to jointly combat malicious cyber activities by nonstate actors. This could act as a communication mechanism for resolving cyber disputes between competitors; it may also serve to restrain the behavior of states actors.

First, the international cyber attribution mechanism should aim to avoid misunderstandings and escalating tensions between states by promoting the peaceful settlement of cyber disputes. If the mechanism to attribute malicious cyber activities becomes an avenue for escalation into a "real shooting war,"[120] as Biden has described it, or causes more conflicts than it solves, it will be doomed to failure.

Second, the priority for the international cyber attribution mechanism should be to fight against cyber attacks that disrupt a country's vital services infrastructures. For example, to combat ransomware attacks, which have become a common threat to global cyberspace, the Biden administration has initiated a Counter-Ransomware Initiative and held virtual meetings with thirty countries to address the misuse of virtual currency, laundering ransom payments, disrupting the ransomware ecosystem, and prosecuting cyber criminals.[121]

Third, a technical cooperation mechanism for cyber attribution should be established. Being positioned to jointly crack down on cross-border cyber criminal organizations, the mechanism may facilitate intelligence sharing, investigation and evidence collection of cross-border cyber attacks, and assistance for technical attribution and investigation of major cyber incidents worldwide. For instance, the "Federal

Government Cybersecurity Incident and Vulnerability Response Playbooks,"[122] published by the U.S. Cybersecurity and Infrastructure Security Agency, is worth sharing worldwide; it provides valuable operational procedures and detailed steps for both cybersecurity incidents and vulnerability responses.

Key Takeaways

There is no doubt that finding the source of an attack is at the very core of combating malicious cyber behavior. Due to the particularities of cyberspace, attribution—especially the attribution of malicious behavior—has always been a challenging issue for the international governance of the cyber sector. Technically speaking, publicly attributing responsibility for cyber attacks to one country does not reduce uncertainty in cyberspace as there is no fundamental breakthrough in the architecture of cyberspace and the anonymity of cyberspace has not changed.

Politically, public attribution is a strategic choice made by countries according to their political needs. Some countries even define it as national sovereignty. However, assigning responsibility for malicious cyber behavior to another country will inevitably lead to hostility. Thus, public attribution is likely to increase tensions and provoke hostile interactions between states.

From the perspective of international governance, collective public attribution still does not solve three major challenges about determining responsibility in cyberspace. Therefore, though it may strengthen credibility, it cannot help a government obtain international legitimacy for retaliatory actions against other countries, nor can it serve as the legal basis for exercising the right of collective self-defense in cyberspace.

If the ultimate goal of public attribution is to crack down on competitors, the risk of it causing instability needs to be addressed in a broad political framework across countries. If the ultimate goal of public attribution is to combat malicious cyber activities, there are many more effective measures—whether through technical solutions or international cooperation—that can be taken without increasing political hostility.

CHAPTER 5

Attribution and Characterization of Cyber Attacks

ARIEL E. LEVITE WITH JUNE LEE

Introduction

This chapter aims to provide a schematic and generic description of the nexus between attribution and characterization in cyber attacks. Attribution is when an entity is named as being responsible or accountable for an act—for example, the theft of personnel data from another state's computer networks.[123] Whereas characterization refers to how an entity interprets or understands a digital anomaly detected in one's systems—recognizing the possibility that rather than a malicious cyber intrusion into one's systems, it could be the product of human error, technical failure, or natural events.[124]

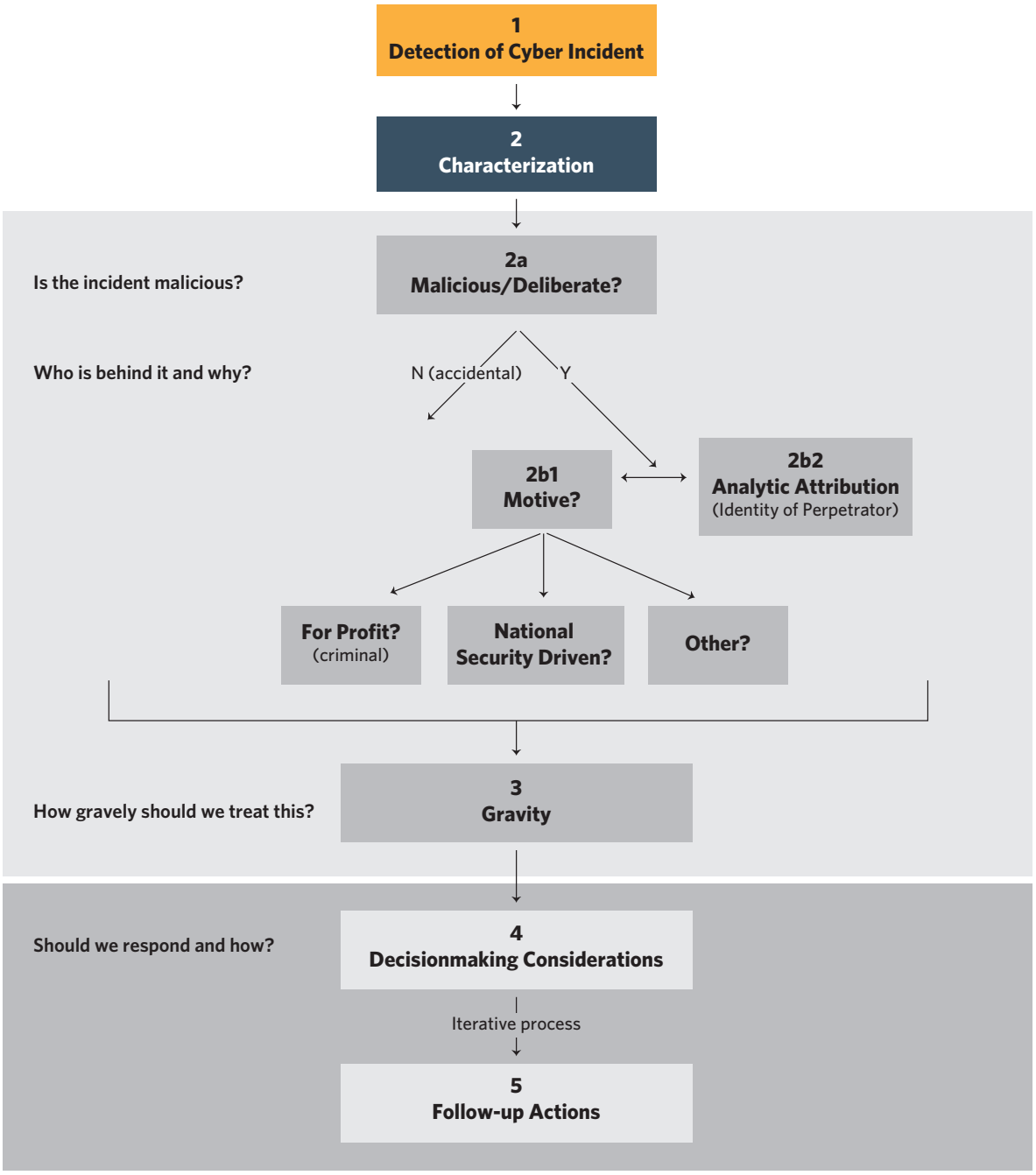
This chapter highlights the centrality of the interaction between these two diagnostic endeavors in the analytic phase following the discovery of anomalies.[125] It further considers how this exchange precedes and subsequently influences any serious policy deliberation of policy responses to cyber attacks. The chapter then considers the interplay between conclusions that emerge from this analytical phase and the framing of the options for response, as well as the policy choices that follow.

Process of Inquiry

The discovery of a serious functional anomaly in one's digital systems (both governmental and corporate) typically leads to a vexing process of inquiry designed to characterize the event and determine its causes and consequences. How different governments conduct such inquiries varies greatly in time, sequence, style, and participants. However, it typically involves certain core functions, processes, dilemmas, and choices.[126] These could be conveniently summarized, for heuristic purposes, as a sequential effort to address a series of core questions to characterize (and interpret) the event. The chart below aims to provide

a comprehensive bird's-eye view of the entire process; the narrative that follows elaborates on key features of every link in this chain.

Characterization and Attribution Sequence



(A more detailed version of this chart appears in the appendix of this chapter.)

Malicious or Deliberate?

Is the detected cyber anomaly the result of malicious action? Or has it been triggered by a technical failure, an innocent human error, or possibly a natural occurrence? On its face, this determination seems like a no-brainer. In practice, though, arriving at a definitive answer may not merely involve considerable time and effort, but also some anxiety until such an answer emerges—especially when the perpetrator of an anomaly tries to mask a malicious action as a technical or human error.

Some publicity may occur during this period, accompanied by confusion, potentially inconsistent statements, and conceivably even a measure of deceit in an effort to buy time and/or shift blame away from (or toward) the incident.[127] Publicity during this phase will likely neither be sought nor welcome; it can be embarrassing and/or can limit policymakers' choices in determining their response.[128] Yet it might be unavoidable, especially if and when private sector entities are involved in either detecting the anomaly or absorbing its effects.

Most importantly, for some actors, the default option might be to treat a cyber anomaly, once discovered, as if it were caused by foul play (at least) until proven otherwise.[129] For others, the opposite may be true. (As, for example, seems to have been the case with Iran's initial discovery of malfunctions in their centrifuge operations that later were attributed to Stuxnet.) Regardless, it must be noted that initially characterizing an event as a possible malicious action makes it more challenging to later credibly dismiss such a misplaced interpretation if and when it is proven to have originated from more benign—if not necessarily less ominous (in terms of consequences)—causes.

In any event, an investigation into the pervasiveness of the phenomenon (where and how widespread is the anomaly) may help determine the root cause of the cyber anomaly and whether it was caused by a malicious action of some sort. Yet we must also acknowledge the real possibility that even a serious and lengthy analysis might fail to remove all uncertainty about the true causes of some cyber anomalies. Suspicion may persist for a long time, especially when vulnerabilities exposed in information technology (IT) systems are traced back to technical or human failures that could either be triggered by unintentional human neglect or attributed to design flaws, deliberately placed bugs, or vulnerabilities.[130]

Motive

Assuming an investigation suggests a deliberate action with malicious intent, it is bound to take a while to assess its true consequences. While the effort to do so is ongoing, the natural next step is to ascertain the motive behind the adversarial action. Was it driven by criminal aims of one kind or another? Is it perhaps an action by a disgruntled employee? Is it a protest by anarchists or another ideological opponent? Or is it motivated by the national security of a foreign power or its proxy? If the latter, two other sets of questions quickly arise, each calling for an elaborate follow-up effort to figure out the precise motive.

The first set of questions aims to establish whether or not the case involves a straightforward cyber espionage operation, such as information collection. If so, is it a typical information collection effort or part of a state-sponsored effort at commercial espionage? Alternatively, is it designed to lay the ground

for an attack—or even carry one out? Or, perhaps, it is intended to communicate a certain message or convey a signal; in which case, what is the message? A related intent would be to shape the perception of the recipient(s) in other ways (that is, an influence operation), begging the question: To what end? Does it intend to sway election results or cast doubt on their veracity? To sow confusion and chaos or foment dissent to weaken an adversary? Additionally, an effort is likely to be made to understand how the perpetrators see their own action: as an unprovoked (cyber) move, a retaliatory action in response to something done to them (be it in the cyber domain or elsewhere), or as a defensive action (preventive or preemptive) to a move the perpetrator expects you to make against them.

The second set of questions digs deeper into the modalities of an attack, seeking to establish whether the perpetrator intended (and tried to design) the attack to be targeted, discriminate, temporary, reversible, and/or one-off. Conversely, the perpetrator may have intended to produce more widespread and/or persistent effects, or at least opened the way (by omission or commission) for these to be followed by (possibly unrelated) others who would seek to leverage the opportunity.

It is important to note that, in recent times, there have been many cases in which the perpetrators (especially those who are agents or proxies of a state) have not tried to mask their actions but have tried to conceal their true intentions.[131] The latter, for example, have presented their actions as ransomware while their true intentions were to cause harm. Naturally, such tactics complicate the characterization and attribution challenge, though it seems doubtful whether such attempts can hold water over time. A thorough investigation of the specific case, additional information (deliberately and unwittingly) released over time by the perpetrators, and considerations of contextual factors (such as geopolitical developments) are likely to ultimately yield critical insights into the underlying motivations of the attackers.

Identity

Another pressing matter is the identity of the perpetrator. And even more importantly, who stands behind them (who could be located far apart nationally, geographically, or institutionally)? And at what level of seniority was the operation approved or, at least, assisted/tolerated? Naturally, the first set of motivation-related questions already begins to touch on these questions, insofar as the effort to characterize an action must factor in the identity of the perpetrator. But often, just as in police investigations of criminal behavior,[132] the process works in reverse order—namely, the likely motivation inferred from an action's parameters provides some clues as to the likely identity of its perpetrator.

Typically, the effort to analytically attribute an action draws on two sources of input: technical forensics and intelligence information. The art and science of cyber forensics has advanced a great deal in recent years; so has the sophistication that goes into concealing the true identity of a perpetrator or even impersonating an attacker's identity, at times going as far as to try to pin blame for an attack on a specific third party.[133] These parallel developments have resulted in an open-ended competition between the two sides.[134] While forensic examinations of tactics and procedures are invaluable in sorting out the identity of cyber attackers, intelligence often remains indispensable to confidently arriving at the identity of the perpetrator and, even more importantly, ascertaining who stands behind them (as well as to quickly respond to such attacks). The odds of attaining such intelligence might be enhanced by

(but not confined to) broad network surveillance, the persistent forward deployment and monitoring of sensors, and especially penetration of adversary networks and trajectories from which such attacks are likely to come.[135]

As we have discovered over the past year, however, these efforts have hardly proved adequate to discover and respond in time to especially sophisticated network intrusions, such as the SolarWinds, Microsoft Exchange, and Colonial Pipeline attacks. Two other factors come into play here. The first is whether the perpetrator or others have taken credit for the cyber action, or categorically denied any culpability for it. As a rule of thumb, both are typically suspect. The role of forensics—as well as intelligence—is to help prove or disprove either one. The second factor is whether the cyber actions are singular or unique; are they distinguishable from others that clearly fit into a broader context, pattern, or the well-recognized modus operandi of a specific actor? The former naturally proves more difficult to pin down with confidence, let alone quickly.

Either way, there is a clear synergy between the two processes of ascertaining the identity of the perpetrator and the motivation behind their action. The ultimate goal of this analytic phase is not merely to identify the perpetrator(s), even if they try to conceal or masquerade their identity, but rather to provide as definitive an answer as possible on two core characterization issues: whether the attack ought to be viewed as a de facto or even de jure hostile state action; and, if so, whether it represents a clear policy choice by the government—rather than the accidental, mistaken, or overly zealous (or corrupt) operation of a state organ or its proxy.[136]

A major obstacle that needs to be overcome in order to arrive at a definitive answer to both questions is the prevalent practice of some states to use proxies or other nonstate agents to undertake cyber attacks on their behalf. In a manner not dissimilar to the historical phenomenon of privateers,[137] states not only work out some arrangements—such as dividing the loot with the proxies, providing them cover and other mutually beneficial arrangements—but at times even empower proxies through provision of some state assistance, such as penetration tools or other material means.[138] In these cases, forensics and intelligence alone may not yield a definitive answer to these questions. And here is where the nature of the regime in which these nonstate operatives reside serves as a useful guiding tool and feeds into the due diligence process of assigning accountability.

As a general point, the more cyber intruders that operate from a territory tightly governed by a regime that effectively surveils also tightly monitors its population, the higher the likelihood that they are—at a minimum—benefiting from acquiescence of its state organs. This probability rises much higher when the state, which enjoys unprecedented police powers over its own cybersecurity and other laws and arrangements, also systematically and consistently fails to investigate and curtail the activities in question in the face of repeated warnings and allegations. This does raise a more fundamental issue regarding how states interpret their own duty of care to prevent cyber attacks from their territories, by their citizens, or employing their nationally based or produced products and services (as well as their international obligation, legal capacity, and operational capability to implement their obligations in this realm).

Gravity

The next phase is determining the gravity of an action. While the preceding phases do feed into and set up a factual (or, at the very least, empirical) foundation on which this question could be addressed, this phase lends itself to a far more subjective determination than the preceding ones. Furthermore, it usually involves many other types of participants as well as considerations. In particular, six additional criteria come into play here to assess and characterize the gravity of an incident. These are:

1. The adversary's aim(s) and intended effect(s).

2. The actual effects of the action (which might be bigger, smaller, more localized, more widespread, more enduring, or more fleeting than the perpetrators may have intended).

3. The targets engaged (such as whether critical infrastructure was attacked).

4. The modalities employed in the attack.

5. The extent to which the operation violated agreed-upon (or, at the very least, desired) norms and other obligations undertaken by the perpetrator.

6. Whether the action represents (or is, at least, likely to become) a broader/bolder pattern of behavior or is merely a one-off action.

We need to bear in mind that these criteria may not all align in the same direction and could potentially produce a mixed evaluation of gravity. Moreover, it is also common to have different individuals and institutions assign different weights to the various indicators of gravity. Further, there is a tendency to address these issues on an ad hoc basis—possibly because of so-called defensive procrastination that is common in high-stress situations—and as part of a calculated strategy to retain a measure of flexibility while waiting for the parameters of the situation to crystallize or mature. Either way, this review often produces a degree of inconsistency and unpredictability in the final judgment of gravity.

Decisionmaking Considerations and Follow-Up Actions

While assessment of gravity (in addition to intent and identity of the perpetrator and their motivation) undoubtedly constitutes an important input into the policy decisionmaking process regarding if and how to respond to the adversarial cyber action, this process has to factor in several additional considerations as well. Especially noteworthy in this context are the following issues, ranging from technical and operational all the way to strategic and political:

1. The level of confidence in the attribution as well as the assessment of the adversary's intent.

2. The extent to which the characterization and attribution rely on sensitive sources and methods that could be compromised if revealed.

3. Whether there are operational benefits associated with keeping the incident and/or its nature/perpetrator secret (such as tracking the perpetrators, feeding them misinformation, or encouraging their complacency).

4. Whether public revelation of the incident (or its specific presentation in a certain light) could become a public or political liability that forces unpalatable policy choices. An alternative consideration is whether covering up the incident or inaction in response could also become such a liability.

5. Whether public revelation of the incident, the identity of the perpetrator, and/or their intention could yield strategic or political benefits. For example, could it influence the adversary's behavior in a desirable direction? Or is it necessary as a step in responding to the attack in certain ways (for example, to lay the ground for imposing sanctions or indicting the culprits)? Or could it be leveraged to enhance one's political standing and agenda?

6. The likely economic and other ramifications of public revelation of the incident and its characterization in certain ways. For example, would public attribution prevent businesses from receiving insurance payments for damages because insurers can then legitimately claim that the cyber event was an act of war and therefore not covered?

7. The response options available for response to the attack (besides public condemnation), and how these might be affected by publicity—or lack thereof—around the event.

8. Whether a response—especially a public one—might trigger a reaction from the perpetrator of the attack (potentially others, too) that might dangerously escalate the situation or create other liabilities.

This undoubtedly is a daunting list of issues to grapple with, consisting of issues that go well beyond deciding whether to publicly acknowledge an attack and whether to attribute the action to a specific, named hostile actor. Officials have to agonize a great deal over whether to publicly characterize an adverse cyber action as a state operation. If so, they also must decide how to portray it (such as, a normal intelligence effort, commercial spying, an armed attack, or even warlike action). Not in the least because such actions may serve more than one purpose or their function may evolve over time. The answers to these questions inform not only how gravely policymakers view an action but also their willingness (or determination) to respond and the direction of such a response.

There obviously are profound consequences that follow each of these choices and ensuing designations. Many strategic, political, and operational considerations—including subjective judgments—affect the ultimate decisions.[139] The nature of this process largely explains why most states and decisionmakers typically opt for an eclectic approach toward public attribution and characterization, even at the expense of some inconsistency in how they approach these issues from one case to another.[140] It also accounts for the considerable variation we observe in how specific they are when they do go public about malicious cyber events, and the unpredictability in the options they pick to publicly name attackers and characterize their actions.[141]

Key Takeaways

This brief review of the process of assessing and debating how to respond to adversarial cyber actions offers a few telling insights:

1. It suggests that the attribution process is, in fact, no more than one (albeit, an important) element in a much broader effort to characterize cyber attacks, debate their significance, and agonize over how one ought to respond to them.

2. This process inevitably weaves together many considerations beyond the capacity to establish who has carried out the attack and toward what end.

3. The sheer complexity of the calculus that determines whether, when, and how to go public about such an attack makes it unreasonable to expect a consistent public characterization and attribution policy to emerge that would hold firm across time, space, and circumstances.

4. The weight of the considerations that affect the choices on public attribution and characterizations also implies that it would be difficult to externally lobby policymakers inclined to go public to refrain from so doing, unless they are offered a credible alternative that would go a long way toward addressing core interests and concerns.

5. These factors hold true not merely for government officials but also for some corporations that provide digital services and platforms for their customers. For example, some such actors may consider it part of their duty of care not only to inform their customers about attacks and breaches but also to dissuade perpetrators from sustaining such conduct.[142] Other private sector players may be inclined to release such information as part of an effort to brandish their cybersecurity credentials. Still others may conversely feel that their corporate interest would be best served by refraining from attributing attacks to their current or prospective customers.

Notwithstanding the inherent inconsistency in decisions on whether and how to go public about cyber intrusions, four clear patterns emerge from analysis of the track record of Western governments in handling public characterization and attribution of cyber attacks:

1. They are generally reluctant to go public about these events unless they feel compelled to do so because the event is serious enough or already in the public domain, and they can point to some process of managing and responding to the event.

2. When senior government officials do elect to publicly acknowledge adversary cyber attacks, they more often than not characterize events as state action without actually (and certainly not initially) naming the culprit, even when they have already reached a high level of confidence about the identity of the perpetrator. This is likely because it allows decisionmakers time to consider how to respond to such events, not in the least to leave some elbow room to explore quiet diplomacy to dissuade the adversary from undertaking further incursions.

3. When they do go a step further to name the culprits, government officials not only seem confident about their judgment but also conscious of the requirement to back it up by publicly releasing some details and taking some measures in response.

4. Some U.S. allies, who are otherwise reluctant to call out cyber attackers, may nevertheless engage in public attribution out of deference to U.S. requests for them to do so.

These trends suggest that the three cumulative requirements—to concede publicly that an adversary has managed to penetrate sensitive digital networks, to back up assertions about the character and identity of the perpetrator(s), and to take some action(s) in response—seem to dampen (though not eliminate) the enthusiasm for going public in general and for making false or unsubstantiated allegations, in particular.

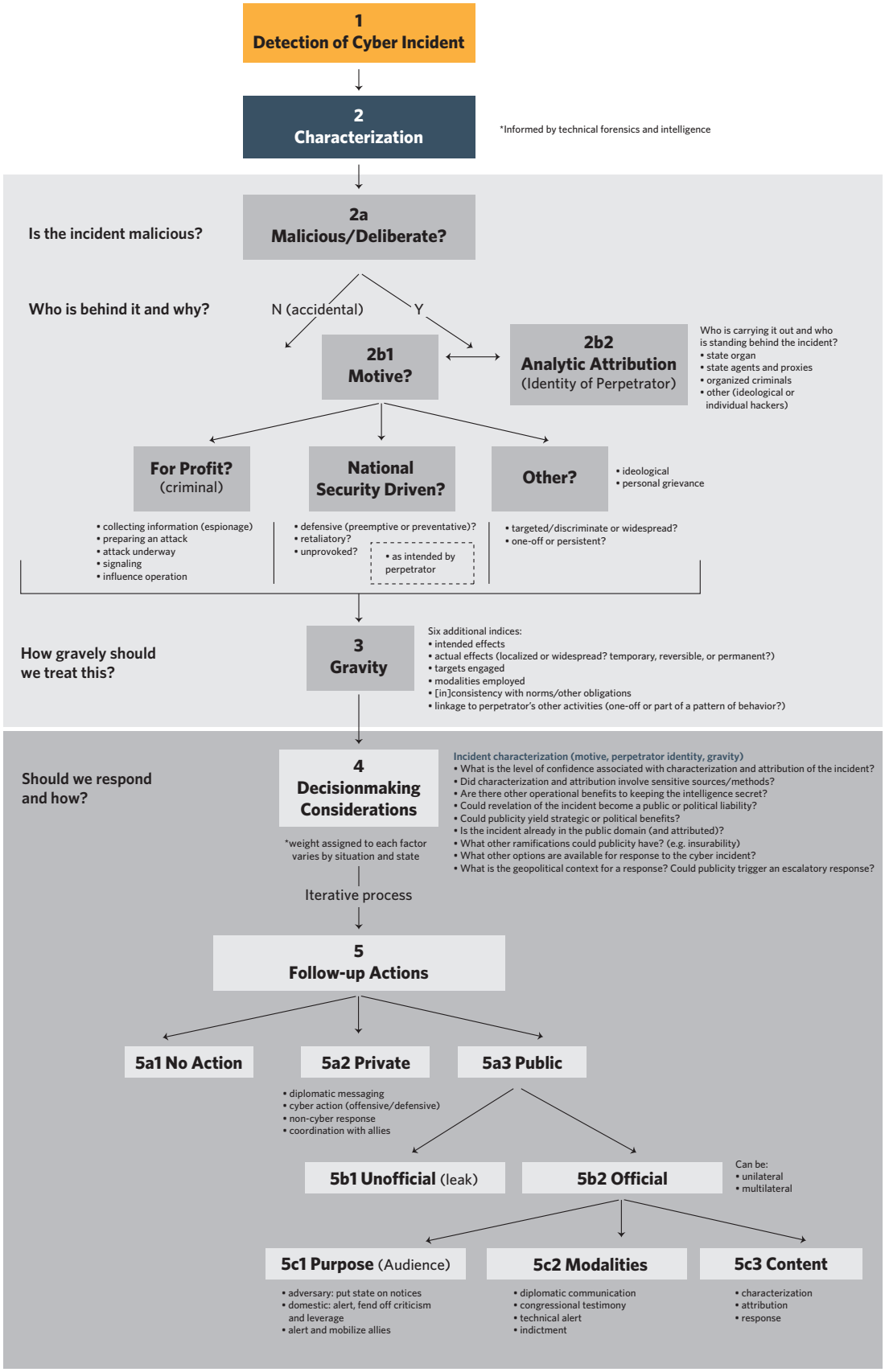
Going forward, two issues are worth exploring further.

The first is whether an official policy of public attribution does indeed serve the national interests of states that undertake them, at least insofar as shaping the behavior of their cyber adversaries is concerned. And if the answer to this question is less than universal and clear cut (as this chapter's analysis implies), what type of developments might alter the incentive structure for governments to engage in public attribution? In particular, can ascendancy of the "duty of care" of nation-states in cyberspace be effectively expanded to comprise prevention, investigation, and prosecution of perpetrators of attacks operating from their territory, that are their national citizens, or homegrown enterprises? If so, might it present a credible alternative to official public attribution toward those states that adopt this norm?

Second, since this chapter solely considers official attribution and characterization by governments, it implicitly draws attention to a closely related issue: the rationales that underlie public attribution by private sector entities and what role they might play in civilizing cyberspace. This issue is worthy of separate discussion.

Appendix

Characterization and Attribution Sequence



CHAPTER 6

A Chinese Perspective on Public Cyber Attribution

LU CHUANYING

When cybersecurity firm Mandiant released its bombshell report "APT1: Exposing One of China's Cyber Espionage Units" in February 2013, it was perhaps the earliest and most high-profile case of public cyber attribution in China-U.S. relations.[143] More than one year later, the U.S. Justice Department's indictment of five Chinese army officers for their alleged involvement in the economic espionage exposed in the Mandiant report marked a major escalation in the fight between the two great powers over cyber theft.[144]

Since then, publicly accusing China for purported cyber activities that threaten U.S. economic interests and national security has become a U.S. policy priority. Federal departments, cybersecurity firms, industry groups, think tanks, and media outlets have all released their accounts of Beijing's so-called malicious cyber operations, portraying the different aspects of a threat that is growing in scale and scope. In stark contrast, to date, China's government has not launched or engaged in any public cyber attribution, except in the case of the Edward Snowden revelations, when Beijing joined others to condemn Washington's extensive government surveillance scheme.

Washington's increased use of public attribution and Beijing's relative passivity reflect their differing perceptions of the divisive issue. A closer examination of the factors driving the two great powers' different approaches will deepen our understanding of public attribution as a foreign policy instrument and its implications for the broader bilateral relationship. A better understanding of the issue may also help move Beijing and Washington closer to some consensus or norms regarding cyber stability.

Public Attribution: An Emerging International Security Issue

Public attribution, as it relates to cyberspace, is a recent phenomenon whose purposes, effectiveness, and consequences are the subject of heated debate. Most countries—including those with formidable cyber capabilities like China, France, and Russia—have refrained from explicitly and publicly attributing

cyber attacks to specific foreign state-affiliated actors. Many of the most high-profile public accusations by governments have so far been made by the U.S.-led Five Eyes intelligence alliance (comprising Australia, Canada, New Zealand, the UK, and the United States) against major ideological adversaries like China, Russia, Iran, and North Korea.[145] Though public attributions of cyber intrusions have increased in the last decade, calling out foreign cyber actors and holding their governments accountable remains a limited policy tool preferred only by a small number of countries because the attribution process is fraught with problems.

First, besides the accusing and the accused parties, public attribution involves multiple cyber actors whose roles, motivations, and behavioral patterns are difficult to ascertain. As a new contested issue in great power competition, public attribution has drawn a significant amount of popular and media attention. Initiators of public attribution can be either government entities or nongovernmental actors that specialize in cyber affairs. Government agencies make accusations against other governments or their proxies for what is described as a state-sponsored malicious cyber intrusion. Nongovernmental accusers may include cybersecurity companies, media outlets, think tanks, or victims of cyber attacks who make attributions for their own reasons or on public interest grounds. On the receiving end of public attribution could be nation-state governments, state-backed hackers, or cyber-criminal gangs. Indiscriminate treatment of the diverse actors involved in public attribution has generated considerable discord and cast the effectiveness of the practice into question.

Government-initiated attributions are more serious and rigorous processes involving considerable amounts of technical and operational information. If public attributions are followed by criminal charges, governments will release even more details to buttress the evidence. In some cases, the accused may raise legitimate questions about evidentiary integrity when the accuser chooses to withhold key information to protect its intelligence sources and methods.

Nongovernmental attributions are more problematic. Cybersecurity companies usually rely on threat intelligence, technical releases, and databases to bolster their cases. Some of them may be capable and prudent, but the less reputable ones may also exaggerate to advertise their attribution capabilities. Accusations initiated by the media and think tanks are generally less convincing as these entities are less technically capable and may need to rely on data or claims provided by others. In some instances, the evidence they've produced has been flawed and misleading.[146] (That said, some think tanks and journalists have become adept at open-source intelligence analysis, and journalists have sometimes conducted valuable on-the-ground investigations.)

Second, there is little agreement on evidentiary standards between the attributor and the accused. The search for perfect proof is futile for a number of reasons. To begin with, cyber forensics is much more difficult than real-world investigations because cyber crimes are virtual and, in many cases, transnational. From the accused state's point of view, the prevailing model of public attribution—associating a cyber intrusion with a state-sanctioned hacking group—has not been convincing enough. When the attributor withholds critical details to protect sources, the accusations invite doubt.

Then there is the problem of legitimacy and credibility. Unlike in real-world court trials, where cross-checking and cross-examination are possible, public attributions of cyber attacks are usually a one-way street; the effective plaintiff's accusations are met with the defendant's resistance and denial. The accused will invariably question the validity of whatever allegedly impeccable evidence the accuser presents.

Public attribution, whether to governments or hacking groups, imposes reputational costs on the accused. Like a defendant in court, the accused will scrutinize every piece of information along the chain of evidence for any possible flaws. If public attribution implicates a foreign state's intelligence agency, the government on the receiving end of the accusation will likely not admit to the charges no matter how compelling the evidence may be. No country has ever acknowledged their intelligence services' involvement in any kind of cyber attack. Washington has never admitted responsibility for the infamous Stuxnet and Flame cyber operations that are widely understood to be part of a broader collaborative effort, known as Operation Olympic Games, between the United States and Israel.[147] In the early days of the PRISM scandal, the U.S. National Security Agency's director downplayed the nature and scope of the government surveillance program at a congressional hearing.[148]

Last but not least, power asymmetry also creates differing perceptions of public attribution. Western attributors—particularly the United States—lead the world in terms of intelligence and internet capabilities. Washington is able to bolster its cases with information and services provided by internet companies, domain name system organizations, and financial agencies within its territory. The accused state, with no ready access to such information and services, may come to a different conclusion. The attributor may call out the accused for the latter's hypocrisy as the accuser believes that the presentation of evidence, no matter how convincing or how substantial, does not change the factual reality of the intrusions and the culpability of the accused. In some cases, the accused would deny the accusation but quietly stop the cyber operations. But presenting persuasive evidence is still necessary—if evidence becomes optional, the threshold for public attribution will be lowered, making it no different from nongovernmental attribution. Audiences will need to learn which attributors are more trustworthy and which attributors are less trustworthy.

Third, the accused has difficulty in fathoming the motives behind public attribution. Compared with the accuser, the accused lags behind in attribution capabilities and experience, and may struggle to understand why the accuser has chosen to go public when existing open channels of communication could be used to express the accuser's concerns. As the accused sees it, public attribution is an exercise in coercive diplomacy, a calculated move to name and shame the accused government. This perception may further undermine the accused state's confidence in bilateral dialogue on cyber issues.

Moreover, the accused may wonder if there are ulterior motives behind the public attributions. As there are no widely agreed international norms of cyber operations, why would the United States accuse others of conducting cyber intelligence activities that Washington has never renounced? While the U.S. government may choose to attribute cyber intrusions that it describes as threatening U.S. national security, news outlets tend to portray cyber operations as irresponsible and illicit followed by moralistic lecturing.

Chinese-U.S. Divergences on Public Attribution

Beijing is also struggling to understand Washington's strategic rationale for public attribution. The United States is the world's leading proponent and practitioner of public attribution but, as Beijing sees it, Washington lacks both consistency and clarity in purpose and tactics.

Three motivations seemingly drive the U.S. public attribution campaign against China. First, Washington aims to establish cyber norms of acceptable behavior—for example, certain targets should be off-limits for cyber intrusions. Beijing and Washington agreed in 2015 that cyber operations should not be conducted to gain commercial advantage.[149] Developing cyber norms also means making cyber operations more professional, as some American cyber experts proposed to reduce backdoors in cyber operations after the Microsoft Exchange hack.[150] Second, Beijing thinks that U.S. public attributions are a prelude to follow-up measures such as indictments and sanctions against alleged Chinese perpetrators. Third, Washington may choose to make public accusations for political purposes. For example, the Office of the Director of National Intelligence has warned of possible Chinese and Russian influence operations in the run-up to U.S. elections.[151]

As Beijing sees it, the above three motivations are contradictory and create confusion. When it comes to developing cyber norms, Beijing insists that it has adhered to the bilateral consensus; U.S. accusations, in some cases, have amounted to a unilateral stretch of the consensus regarding cyber norms. Beijing hopes to sign a more extensive agreement that commits both to refrain from cyber operations against each other.[152] But Washington views cyber operations as a sovereign right it will never renounce, leading Beijing to believe that Washington wants to circumscribe China's cyber operations while preserving its own freedom of action in cyberspace.

Public attribution on domestic legal grounds is also problematic. States conduct cyber operations to collect intelligence not for criminal purposes. In practice, the United States cites domestic laws to justify legal actions against intelligence-gathering cyber operations. For example, when the Justice Department indicted five Chinese soldiers on cyber espionage charges, it cited such U.S. legal provisions as 18 U.S.C. § 1030 (a)(2)(c), 1030 (a)(5)(A), and 1030 (b), which concern computer fraud, theft of personal identities, economic espionage, and theft of trade secrets.[153] In international law, cyber espionage is considered legally dubious while mainstream views maintain that it is acceptable.[154] Cyber operations conducted under the so-called responsible state behavior framework may not be in line with U.S. domestic law but are not inconsistent with international obligations. U.S. accusations that China has violated bilateral consensus are seen in China as unjustified and the United States' moralistic lecturing only exposes its cyber double standard, as Washington engages in cyber operations of a similar nature.

As for public attribution as a kind of prewarning, Beijing regards it as even more irresponsible and counterproductive. The U.S. Office of the Director of National Intelligence released two reports in the run-up to the 2020 presidential election. The first one warned of possible Chinese interference through cyber operations,[155] while the second one recanted the first's claims.[156] As Beijing sees it, irresponsible U.S. actions have tarnished China's international image. In another example, the U.S. Justice Department claimed that China had stolen U.S. data on COVID-19 vaccines. In fact, the alleged evidence it presented only revealed that certain Chinese hackers had been probing the computer networks of U.S. vaccine makers for possible bugs.[157] The glaring inconsistency between charges and evidence exaggerated China's cyber threat, imposed enormous reputational costs, and undermined Beijing's confidence in bilateral cooperation amid the coronavirus pandemic.

Nongovernmental attribution creates even greater confusion. Nongovernmental actors like cybersecurity firms and news outlets feel even less constrained in making public accusations against China. The motivations that drive their attributions are even more complicated and diverse, making the process

even more flawed. The media tends to broaden public attribution into a smear campaign using naming and shaming tactics. It also tries to sway public opinion and government policy by portraying Beijing as a growing malicious cyber actor. Chinese observers believe cybersecurity firms usually exaggerate cyber threats in public attribution to market their capabilities for commercial gains.

Nongovernmental attributions are also fraught with problems. U.S. print and online media have published no shortage of threat assessments that associate Chinese hackers with cyber activities backed by the Chinese government. A report by the Center for Strategic and International Studies examined over 800 cyber incidents and described more than 200 of them as China-related.[158] A number of these news reports made public accusations without presenting any evidence; some are pure hearsay and do not stand up to scrutiny. A Bloomberg article in October 2018 reported that China had planted spyware in Supermicro products to facilitate cyber intrusions.[159] This widely circulated article later turned out to be built on disputed claims, as one of Supermicro's business partners, Apple, wrote a letter to the U.S. Congress, calling the story false.[160]

Though these accusations may not have been sanctioned by the U.S. government, they have hurt China's reputation nonetheless by dragging Beijing into a dilemma of sorts. If China chooses to refute and debunk every unfair charge against it, it would have to devote considerable attention and resources. If it chooses to ignore them, the accusers may feel emboldened and double down on public attribution. China's international discursive power lags far behind that of the United States and other Western countries. Continued Western public accusations, many of which are flawed and ill-grounded, will only deepen bilateral strategic distrust and the Chinese public's disapproval of Western media.

As some Chinese analysts see it, even if the U.S. government did not support nonofficial public attributions, it has acquiesced to them. For example, sometimes media attributions have cited government officials to bolster their cases. In many high-profile accusations, government actions followed media revelations, like the indictment of the five officers in the wake of the 2013 Mandiant report.[161] In another example, the U.S. government forged a partnership with the private sector in the run-up to the 2020 election to guard against possible external interference. Nonofficial public attribution may put the accusing government in a bind, forcing it to take more robust actions to push back against purported Chinese offensive cyber operations. If nongovernmental attributions become a major tool to tarnish China's image, it will further undermine Beijing's willingness to conduct bilateral cybersecurity dialogue for consensus building because China's good-faith engagement will have little to no effect on the intensity of nonofficial public attribution campaigns.

Recommendations for Chinese-U.S. Dialogue on Public Attribution

Beijing and Washington rarely see eye to eye on public attribution, but it is an increasingly prominent issue in the bilateral relationship. As the initiator of many high-profile accusations, the United States seeks to derive strategic benefits from public attribution and chooses to turn a blind eye to many of its downsides. China has been on the receiving end of public attributions, many of which it thinks are unfair and unjustified. Beijing tends to set a high threshold for making public accusations and to put each case under a microscope.

Information asymmetry can make a case that appears convincing to the United States look deeply flawed from Beijing's perspective. And in the absence of substantive communication on technical specifics, divergences of opinion only increase. Perceptional gaps and structural problems have only amplified bilateral discord over the issue. Moreover, politicization, interest groups' influence, and the lack of evidentiary standards have made public attribution a major hurdle to Chinese-U.S. cooperation in cyberspace. The following recommendations would help lessen the tensions and foster greater cyber strategic stability.

1. **Reconsider the effectiveness of public attribution and its wider implications for bilateral relations**. Past practices have proven that intergovernmental cooperation is the cornerstone of cyber strategic stability between Beijing and Washington, but irresponsible public attribution has undermined this stability and thrown bilateral cyber interaction into greater uncertainty. Chinese-U.S. cyber relations should not be defined by disputes over public attribution. Instead, both sides should increase government-to-government dialogue to build a more comprehensive framework to address broader cybersecurity issues.

2. **If public attributions must continue, conduct them prudently and in line with agreed-upon standards**. Public attribution should not be used as a tool for geostrategic competition to add another layer of uncertainty to great power rivalry. The United States should consider allowing for a buffer period before attributions go public, during which Washington and Beijing can increase communication to build trust. It should also guide and limit counterproductive nonofficial public accusations and establish clear evidentiary standards to reduce politicization and internationalization of public attribution.

3. **Establish a multilateral and multiparty regime for public attribution within the United Nations framework**. The regime could be modeled after the International Atomic Energy Agency to mobilize international resources and skills to strengthen the legality, legitimacy, and effectiveness of public attribution and deter truly harmful cyberattacks.

4. **Increase dialogue and communication on public attribution**. As mentioned earlier in this chapter, public attribution is an emerging international security issue over which Beijing and Washington have contested for many years, with each insisting on their own positions and approaches. Continued engagement on the issue both at the policymaker and scholarly levels could help narrow some of the gaps and stabilize bilateral cyber relations.

Conclusion and Recommendations

GEORGE PERKOVICH AND LU CHUANYING

In this conclusion, we will not attempt to summarize the preceding chapters or the discussions between our two groups. Rather, we briefly present here the essence of U.S. and Chinese perspectives on issues related to public attribution, as we have understood them through our discussions. This unavoidably is interpretive and oversimplified; we hope it gives readers a quick sense of key issues.

Perhaps more importantly, our dialogue and improved understanding of the different interests and perspectives of actors in the two countries have led us to make shared recommendations of steps that could be taken to reduce the tensions emanating from cyber operations and reactions to them. These seven recommendations appear at the end of this chapter.

Observations

The United States and China view cyber operations conducted by the other as one of the most serious—and most stubbornly persistent—threats to their national security. Contesting such operations is made difficult by the lack of enforceable international laws or widely supported norms that clearly define what types of cyber activities should be considered unacceptable. Major states have divergent views on key categories of cyber behavior and have different interpretations of even the handful of norms supported by the United Nations Group of Governmental Experts. Even if they did agree on behavioral standards, they would find it difficult to monitor and enforce them. The United States itself has resisted efforts to broadly prohibit some types of cyber intrusions and potential attacks. For now, espionage is not illegal and states increasingly use digital tools and networks to spy on each other. Cyber operations to conduct sabotage or military attacks are also on the rise and becoming more likely. Moreover, the dividing lines between cyber espionage and more offensive forms of cyber actions are so blurred that they are difficult to delineate and enforce.

Thus, the international community—including the United States and China—is closer to the beginning than to the conclusion of efforts to clarify, at least bilaterally, what types of cyber behavior should be deemed illegitimate or irresponsible.

Seeing no real progress in defining and agreeing on standards of cyber behavior or in greatly reducing such threats in the foreseeable future, U.S. leaders have come to rely on modest, readily available tools like public attribution to shape actors' behaviors. American officials are particularly inclined to make public accusations when they feel the counterpart government has not responded constructively to private communications. They hope that a long-term campaign of public attribution—ideally undertaken with allies and combined with other actions like sanctions, indictments, and cyber-forward engagement and counterstrikes—might help to deter some cyber operations and rally the support of domestic and global audiences.

While concrete results may be hard to prove, the risks of public attribution often seem even lower to U.S. officials. Thus, Washington has used public attribution more and more frequently, including with allies. In some cases, the United States has done this in response to alleged Chinese cyber operations that harm U.S. interests but don't necessarily violate any international laws, norms, or commitments. Stealing intellectual property for commercial purposes (which China, the United States, and the rest of the G20 have agreed not to do) is particularly unacceptable to Washington. Sloppy, indiscriminate cyber espionage is also unacceptable, because it leaves back doors and other vulnerabilities open for criminals to exploit. The United States seeks to use public attribution inter alia to try to motivate others to diminish such activities.

Chinese officials, experts, and media submit that many U.S. allegations of Chinese cyber actions are plain wrong. They imply that the United States interprets the 2015 understanding between Chinese President Xi Jinping and then U.S. president Barack Obama differently than China. Chinese officials and observers see hypocrisy, double standards, and a lack of legal basis for many U.S. public attributions. This reinforces the feeling that this so-called issue is simply part of the U.S. effort to contain China and undermine its government. The United States is almost always the accuser and China almost always the accused. In this position, China will naturally be more sensitive to any flaws, limitations, or harms of public attribution.

Chinese officials invoke international law to position the United States as the wrongful actor. They say that U.S. public statements fail to provide sufficient evidence to prove Chinese guilt. Nor does the United States provide sufficient evidence and legal basis to hold the Chinese government responsible for cyber operations that allegedly emanate from Chinese territory or fingertips on keyboards. When a state accuses another of cyber aggression and establishes a basis for potential countermeasures, the international community should demand public evidence of wrongdoing by the accused state. Chinese observers submit that the United States rarely provides much evidence; instead, it makes "ill-substantiated" attributions that are ineffective and destabilizing. Chinese experts further argue that China has thus far largely refrained from engaging in public attribution because its attribution capabilities were inferior to the United States and they were reluctant to make unsubstantiated allegations, notwithstanding their conviction that the United States is aggressively engaged in cyber actions against China.

Of course, there are major technical challenges in identifying who authorized a detected cyber operation and legal challenges in defining the circumstances in which a government should be held legally accountable for such actions. But, according to China, the United States avoids these issues because its main motivation is to politically oppose China.

U.S. law enforcement and intelligence agencies, in particular, may issue public attributions without due heed to the diplomatic fallout. Chinese experts further submit that some private U.S. companies are even more reckless, publishing shaky allegations either because they are doing the U.S. government's bidding or are seeking to attract money and attention. (However, Chinese cybersecurity companies have recently begun publicly accusing others of operations against China, which suggests the quality and role of cybersecurity businesses in this area is becoming more widely accepted.)

Against this background, Chinese experts submit that China is bound to dismiss unsubstantiated U.S. allegations of irresponsible or illegitimate Chinese cyber actions. This skepticism and resistance will intensify if Washington refuses to reassure China that the United States will abstain from cyber operations that threaten the core apparatus of the Chinese state and military command and control. Moreover, Chinese observers argue that public attributions have been ineffective: case in point, cyber attacks continue. Worse than being ineffective, public attribution inflames relations between the accuser and the accused. This reduces the prospects for constructive diplomacy on cyber issues and raises the risk of retaliatory cyber operations by the accused state. The United States would be better off focusing its energy on improving its own cybersecurity while working collaboratively with China and others to tackle international challenges like ransomware.

Americans might respond that the Chinese government controls its cyberspace well enough to know the truthfulness of U.S. accusations, even if the Chinese media and public do not. And Chinese officials understand that no country would give up its best sources and methods of intelligence in another country. Moreover, the gravity and record of major cybersecurity businesses such as Microsoft, Mandiant, and CrowdStrike should sufficiently justify why they must warn their clients and others of threats to their systems so that they can update them and take further steps to enhance cybersecurity. Thus, the United States finds much of China's argumentation to be an attempt to evade responsibility and redirect blame to the United States.

Yet so long as the United States is making accusations outside of the international legal system and without sufficient evidence to hold the Chinese government accountable, Chinese observers will question the United States' intention in launching unilateral accusations: Are they to warn against cyber operations? To simply point fingers at China? Or to ease domestic pressure? This further highlights the need for both states to strengthen communication and cooperation in public attribution. Only by figuring out "what kind of cyber action is unacceptable, what kind of evidence is convincing, what kind of signal can clarify intentions" can public attribution strengthen the two states' cyberspace relationship rather than destabilize it.

One area that seems especially critical for the two parties to discuss is the distinction between intelligence collection operations (whose goal is data exfiltration) and operations that are designed to affect the performance of systems or data. While some of the former could still be contentious (based on their intended purpose and modalities) the latter hold the greatest prospect for triggering unintended escalation.

Looking ahead, it seems that, if left unattended, the festering frictions between the United States and China in general and cyberspace in particular are more than likely to worsen. They may even contain the seeds of serious potential for unintended escalation. This holds especially true when both parties seem bent on expanding their competing activities in other domains including maritime, space, nuclear, and conventional force projection. Unless and until they acknowledge each other's concerns—privately at high levels or publicly—and establish agreed-upon processes for addressing them, tensions over cyber operations and public attribution of responsibility will grow.

Recommendations

From these analyses and arguments, we propose seven recommendations.

All participants in our discussions recognize that relations between China and the United States are now so strained that neither side is eager to take bold steps to establish mutual limits on their competition. Therefore, we have developed modest initiatives that would not require either side to redefine or change their core interests, but which could indicate both sides' willingness to collaborate on matters where it is mutually beneficial to do so. Taking such steps could build confidence not only between China and the United States but also between the rest of the world and these two major digital powers.

To ease the way toward implementing the recommendations below, it would be beneficial if the U.S. and Chinese governments conducted sustained high-level dialogue that could build on the 2015 Xi-Obama understanding and clarify standards of behavior that both would follow. Both sides should study and discuss events that have transpired since then.

1. Clarify Behavior Standards in Cyberspace

As a general norm, **countries should be clearer and more explicit in characterizing the standards they are accusing others of violating in any given instance**. Is it international law? An agreed (or desirable) international norm? A bilateral agreement? Or is it an attempt to punish the other for undermining a core national interest?

U.S. officials and others might resist such clarifications for a variety of reasons. Some factions hold little regard for international law and do not want to affirm its importance. Many want to retain the widest freedom of action for the United States in this domain and do not want to buttress standards that could be used by China or anyone else against the United States in the future. However, there are good reasons to think that both counties as digital economic superpowers would have more to lose from the absence of any rules or standards than from increased clarity on them. Indeed, the United States intensely seeks to make China adhere to its previous political commitment against stealing intellectual property for commercial purposes, for example, while China wants more assurances that the United States won't use cyber tools to interfere in its internal affairs or undermine its national security. Perhaps some common ground could be found in espousing a bilateral norm that prohibits both sides from employing covert means to undermine each other's political order.

2. Improve Cyber Attribution Capabilities

In the same vein, **countries would benefit from improving their governments' and businesses' capabilities to attribute intrusions and other operations** so that they can more specifically hold each other to account for alleged violations of standards or rules that their leaders would then need to respect themselves. For example, improved attribution capabilities could facilitate more useful dialogue between U.S. and Chinese officials in specific cases and more broadly in developing shared standards of responsible or irresponsible behavior. The growth of Chinese cybersecurity companies and recent reporting of alleged foreign cyber operations in the Chinese press suggest the potential here.[162]

3. Sustained Dialogue, Dispute Management, and Confidence-Building Measures

With a clearer understanding of each side's expectation of what standards of behavior the other will follow and more balanced capacity to credibly attribute alleged violations of such standards, the United States and China would have a better basis for **sustained dialogue, dispute management, and confidence-building measures**. These objectives would be served well by U.S. officials refraining from using harsh language to publicly criticize China's cyber conduct, especially when it relates to espionage and other activities that the United States itself conducts or wishes to retain the freedom to carry out.

Without moralizing, Washington can still "complain" about or "protest" the fact of adversary cyber operations, even if these don't violate a standard the United States would apply to itself. Washington generally believes its adversaries are strategic aggressors and the United States is a noble victim, so the United States only hacks because the bad guys first threatened U.S. security. The U.S. government is free to use cyber attributions as part of that larger public argument, but it might be more credible, more diplomatically effective, and less destabilizing to forgo protesting when no wider standard of behavior has been violated.

Alternatively, the United States could do as some other countries and many cybersecurity businesses have done and announce that an observed intrusion or an attack was state-sponsored and that it is confident it knows which state. The United States could say further that it has taken or will take action in response, without publicly declaring the name of the state. This would not stop media and other nongovernmental actors from naming the alleged country, but Chinese authorities and audiences need to understand that the state does not have the monopoly on "truth" or its disclosure in democracies. If, over time, Chinese officials did not engage constructively on these issues and unacceptable operations against the United States continued unabated, Washington could resume more explicit public attribution.

From China's point of view, the United States has gained superior cyber powers that far surpass China's. In contrast to China's professed defensive cyber strategy, the United States is believed to have become increasingly offensive, with its declared policies of "persistent engagement" and "defending forward." Judging from current cyber relations between the two states, China sees itself as weaker and less secure in cyberspace. So it is hard for China to understand why the stronger United States insists on singling China out as the top adversary undermining its cybersecurity. China is still willing to sign a binding agreement with the United States to restrain from carrying out cyber attacks against each other. But China perceives

that the United States is unwilling to accept Beijing's proposal. This gives China reason to suspect that Washington's aggressive public attribution strategy is not to address cybersecurity but to sensationalize the issue for political ends.

4. Define Norms of Responsible Cyber Tradecraft

To build on and reinforce all the points above, the United States and China, bilaterally and/or multilaterally, could be more realistic and constructive if they sought to **define norms of responsible (or irresponsible) cyber tradecraft**. Diplomats and others focus on norms to prohibit actions, but it's at least as important to recognize that some forms of espionage and defense preparation will continue or even intensify. Norms for responsible (or irresponsible) conduct could help reduce the risk of unintended effects on targeted networks and beyond, minimize collateral damage, and minimize opportunities for cyber criminals to exploit tools, among other benefits.

To develop and agree to such norms, cyber operators from both countries would need to be involved. Senior leaders would need to be more informed about technical details of offensive operations (for espionage and potential military conflict) than is often the case. Reflecting the analytic processes that occur when a state is characterizing an intrusion or attack, norms would be based on the recklessness one ascribes to what was targeted, the effects that resulted, or the modalities that were used (such as how easily they could propagate).

5. Explore Alternative Approaches

Recognizing that public attribution has not significantly reduced the problem of cyber intrusions (as seen from the United States) but has created other problems (as seen from China), **the two could explore an alternative approach**. The objecting state could convey that it would share objections privately to officials of the suspected state if there was an agreement that officials of the suspected state would then investigate and report back to the objecting state the results, along with steps that have been taken to prevent similar future operations.

Such communications could be made through a designated official channel or new non-official channels that are acknowledged by the relevant government leaderships. This could involve the suspected state taking corrective (and, if warranted, punitive) actions that would assuage the objector's concerns in ways that could be observed using its national technical means. States would expect reciprocity, of course. If a buffer period of private consultation did not demonstrate good will in a specified amount of time, the suspected state should not be surprised if the objecting state then went public. However, the objecting state should provide evidence proportionate to the severity of the retaliatory actions it plans to take. Viewed from Washington, it seems unrealistic to expect the United States to desist from public attribution and instead adopt such an alternative approach without credible assurances that its privately communicated expressions of concerns would be heeded by China.

6. Identify Consequences for Unsubstantiated Countermeasures

Nationally, bilaterally, and multilaterally, more thought and discussion should be devoted to the question of **what consequences an accusing state should face if it carries out countermeasures against a state on the basis of allegations that are not substantiated**. (Similar discussion would be warranted regarding consequences the accused state would be liable to face if the allegations against it are substantiated and it fails to take appropriate actions to stop such actions forthwith.) The papers and discussions in this project highlight the great difficulties of creating a formal mechanism for international attribution when states, understandably, will not be willing to reveal sources and methods beyond cyber forensics. The difficulties of proving attribution to an international audience need not preclude a state from taking countermeasures or acting in self-defense, but the rest of the world has a legitimate interest in discouraging mistaken reprisals and the escalation of instability.

7. Establish an International Coordination Mechanism Against Ransomware

As an early confidence-building measure, **the United States and China could establish an international coordination mechanism to combat ransomware attacks**. Ransomware is among the most serious cyber challenges that both countries face but is not a major source of bilateral friction, so it is a logical starting point for early cooperation. A counter-ransomware effort could be narrowly tailored, so that neither side feels its participation is legitimizing other objectionable aspects of its counterparts' cyber strategy and behavior. Such cooperation might yield tangible benefits with little costs, help to build bilateral confidence in the cyber domain, and encourage other countries to take stronger action against ransomware as well.

Notes

1 Nan Tian, "Military Expenditure," in *SIPRI Yearbook 2021: Armaments, Disarmament and International Security* (Oxford: Oxford University Press, 2021), https://www-sipriyearbook-org.ceip.idm.oclc.org/view/9780192847577/sipri-9780192847577-chapter-008.xml#; and "GDP Based on PPP, Share of World," International Monetary Fund, 2021, https://www.imf.org/external/datamapper/PPPSH@WEO/OEMDC.

2 "Law of the Sea Convention," U.S. Department of State, accessed February 28, 2022, https://www.state.gov/law-of-the-sea-convention/.

3 "Final Substantive Report," conference room paper, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly, March 10, 2021.

4 Ibid.

5 "Incidents at Sea Agreement," U.S. Department of State, signed May 1972, accessed February 28, 2022, https://2009-2017.state.gov/t/isn/4791.htm.

6 Elizabeth Rosenthal with David Sanger, "U.S. Plane in China After It Collides With Chinese Jet," *New York Times*, April 2, 2001, https://www.nytimes.com/2001/04/02/world/us-plane-in-china-after-it-collides-with-chinese-jet.html.

7 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House, 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/; and Steve Holland and Doina Chiacu, "U.S. and Allies Accuse China of Global Hacking Spree," Reuters, July 20, 2021, https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/.

8 "Protecting People in Cyberspace: The Vital Role of the United Nations in 2020," Global Forum on Cyber Expertise, Microsoft, December 2019.

9 "Bilateral Military Agreements Between NATO Member States and the Soviet Union on the Prevention of Incidents," European Leadership Network, accessed on February 28, 2022, https://www.europeanleadershipnetwork.org/bilateral-military-agreements-between-nato-member-states-and-the-soviet-union-on-the-prevention-of-incidents/.

10 Heajune Lee, "Strategic Publicity?: Understanding US Government Cyber Attribution," thesis, Stanford Digital Repository, Spring 2021, https://purl.stanford.edu/py070wt8487.

11 Harold Koh, "International Law in Cyberspace," *Harvard International Law Journal Online* 54 (December 2012). Accessed at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers.

12 Florian Egloff, "Public Attribution of Cyber Intrusions," *Journal of Cybersecurity* 6, no. 1 (Fall 2020): https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454.

13 For chart illustrations covering the period of 2015–2020 verifying this deduction, see: Garrett Derian-Toth et al., "Opportunities for Public and Private Attribution of Cyber Operations," *Tallinn Paper Series* no. 12 (2021): 8–9. Not surprisingly, top five countries that made the most use of public attributions are all from Five Eyes alliance, and China, Russia, Iran and North Korea have been identified as the responsible actors for 75 percent of all state-sponsored offensive cyber operations.

14 Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," *Journal of Strategic Studies* (Spring 2021): https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117.

15 "A Guide to Cyber Attribution," U.S. Office of the Director of National Intelligence, September 14, 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

16 Some have noted that different purposes of public attribution relate to different levels of evidence. See: Kristen Eichensehr, "The Law & Politics of Cyberattack Attribution," *U.C.L.A. Law Review* 67, no. 3 (July 2020): 19–36, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3453804.

17 It is a long-debated question as to when does cyber operations fall within the meaning of "armed attack" in the language of Article 51 of UN Charter. See, for example, Priyanka Dev, "'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," *Texas International Law Journal* 50, no. 2 (2015): 381–401.

18 Lorraine Finlay and Christian Payne, "The Attribution Problem and Cyber Armed Attacks," *American Journal of International Law Unbound*, 113, (2019): 202–6.

19 United Nations, General Assembly Draft Resolution, "Developments in the Field of Information and Telecommunications in the Context of International Security," para. 10, U.N. Doc. A/C.1/73/L.27, October 22, 2018, available at: https://undocs.org/A/C.1/73/L.27.

20 Quoted phrase appeared in the first statement of the U.S. position on evidentiary issues, See: Brian J. Egan, "International Law and Stability in Cyberspace," *Berkeley Journal of International Law*, no. 35, (2017): 177. Regarding legal underpinnings of evidentiary issues in cyber attribution, "the U.S., British, French, and Dutch efforts to block the development of customary international law on attribution" have been criticized as "shortsighted." See: Eichensehr, "The Law and Politics of Cyberattack Attribution," 521–98.

21 "Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries," UN International Law Commission, 2001, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

22 "Responsibility of States for Internationally Wrongful Acts," United Nations General Assembly, A/RES/56/83, January 28, 2002, available from https://undocs.org/en/A/RES/56/83.

23 James Crawford, *State Responsibility: The General Part* (Cambridge: Cambridge University Press, 2013), 146–54.

24 *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, 1986 ICJ Merits, ICJ Report.

25 *Prosecutor v. Tadic*, Appeals Chamber, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ICTY-94-1-AR72, 1995.

26 Scott Shackleford and R. Andres, "State Responsibility for Cyberattacks: Competing Standards for a Growing Problem," *Georgetown Journal of International Law* 42 (2010): 971, 987.

27 Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press, 2020), 88.

28 *Prosecutor v. Tadic*, paras. 131, 137.

29 *The Corfu Channel Case (United Kingdom v. Albania)*, 1949 ICJ Merits, ICJ Report, https://www.icj-cij.org/en/case/1.

30 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed.* (Cambridge: Cambridge University Press, 2017), Rule 6. doi:10.1017/9781316822524. The rule reads: "State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."

31 "Report on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (Advanced Copy)," UN Group of Governmental Experts, May 28, 2021, Norm 13(c). The norm reads: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."

32 This last element may get us back to the dilemma of lack of primary rules on cyber obligations.

33 Lahmann, *Unilateral Remedies to Cyber Operations*, 91.

34 See: "Report on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (Advanced Copy)," UN Group of Governmental Experts, para. 71(g).

35 "Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries," UN International Law Commission, commentaries, Chapter V, 8.

36 Peter Margulies, "Sovereignty and Cyberattacks: Technology's Challenge to the Law of State Responsibility," *Melbourne Journal of International Law* 14 no. 155 (Winter 2014): 296.

37 Lahmann, *Unilateral Remedies to Cyber Operations*, 93–97.
38 Ibid., 71.
39 Eichensehr, "The Law & Politics of Cyberattack Attribution," 559–62.
40 See, for example, the Land, Island and Maritime Frontier Dispute (El Salvador/Honduras), ICJ Judgment of September 11, 1992, para. 248; see also, Sovereignty over Pedra Branca/Pulau Batu Puteh, Middle Rocks and South Ledge (Malaysia/Singapore), ICJ Judgment of May 23, 2008, para. 86.
41 See: Eichensehr, "The Law & Politics of Cyberattack Attribution," 576–86.
42 See: Eichensehr, "The Law & Politics of Cyberattack Attribution," 571–72.
43 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1–2, (2015): 32.
44 See, for example, MJ Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent," *Military Law Review*, no. 201 (2009): 1.
45 See, for example, Presidential Policy Directive/PPD-20, White House, October 2012, p. 7.
46 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, Rule 71, para. 23.
47 "Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries," UN International Law Commission.
48 See, for example, "Report on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (Advanced Copy)," UN Group of Governmental Experts, para. 71(g).
49 "Understanding on Rules and Procedures Governing the Settlement of Disputes," World Trade Organization, annex 2 of the WTO Agreements.
50 Sasha Romanosky and Benjamin Boudreaux, "Private-Sector Attribution of Cyber Incidents," *International Journal of Intelligence and CounterIntelligence* (Fall 2020): 463–93, https://www.rand.org/pubs/external_publications/EP68257.html. Romanosky and Boudreaux's figures are confirmed by unpublished data compiled by June Lee, Carnegie Endowment for International Peace.
51 The taxonomy and examples in this paper are heavily indebted to the following sources, among others cited: Martha Finnemore and Duncan B. Hollis, "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity," *European Journal of International Law* 31, no. 3 (August 2020), 10.2139/ssrn.3347958; Florian J. Egloff, "Public Attribution of Cyber Intrusions," *Journal of Cybersecurity* 6, no. 1 (2020), 10.1093/cybsec/tyaa012; Kristen Eichensehr, "The Law & Politics of Cyberattack Attribution," *U.C.L.A. Law Review* 67, no. 520 (2020), https://papers.ssrn.com/abstract=3453804; Romanosky and Boudreaux, "Private-Sector Attribution of Cyber Incidents"; Garrett Hinck and Tim Maurer, "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity," *Journal of National Security Law and Policy* 3, no. 10 (Winter 2020), https://jnslp.com/wp-content/uploads/2020/05/Criminal-Charges-as-a-Response-to-Nation-State-Malicious-Cyber-Activity.pdf; and June Lee, "Strategic Publicity?: Understanding US Government Cyber Attribution," Stanford University, 2021.
52 This paper focuses specifically on U.S. government public attributions to state-affiliated actors. It does not consider, for example, attributions to non-state-affiliated cyber criminals.
53 "National Cyber Strategy of the United States of America," White House, September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
54 Romanosky and Boudreaux, "Private-Sector Attribution of Cyber Incidents."
55 "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," Department of Justice, news release, March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.
56 Kristen Eichensehr, "The Law & Politics of Cyberattack Attribution."
57 Mark Esper, "Remarks by Secretary Esper in a Media Availability, U.S. Strategic Command," U.S. Department of Defense, speech transcript, February 20, 2020, https://www.defense.gov/News/Transcripts/Transcript/Article/2090285/remarks-by-secretary-esper-in-a-media-availability-us-strategic-command/.
58 Tim Maurer and Garrett Hinck, "Persistent Enforcement."
59 Ibid.
60 Derek B. Johnson, "DOJ Official Says 'Name and Shame' is One Piece of the Puzzle," *Business of Federal Technology*, January 18, 2019, https://fcw.com/articles/2019/01/18/demers-doj-cyber-shame.aspx.
61 Mark Pomerleau, "After Tug-of-War, White House Shows Cyber Memo to Congress," Fifth Domain, March 13, 2020, https://www.fifthdomain.com/congress/2020/03/13/after-tug-of-war-white-house-shows-cyber-memo-to-congress/.
62 "Background Press Call by Senior Administration Officials on Malicious Cyber Activity Attributable to the People's Republic of China," White House, July 19, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/19/background-press-call-by-senior-administration-officials-on-malicious-cyber-activity-attributable-to-the-peoples-republic-of-china/.
63 James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," February 26, 2015, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

64 Jack Goldsmith and Robert D. Williams, "The Failure of the United States' Chinese-Hacking Indictment Strategy," Lawfare, December 28, 2018, https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.
65 "Fact Sheet: President Xi Jinping's State Visit to the United States," White House, fact sheet, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States.
66 "Update 1- U.S. Accuses China of Violating Bilateral Anti-Hacking Deal," Reuters, November 9, 2018, https://www.reuters.com/article/usa-china-cyber-idUKL2N1XK06K. In 2018, senior NSA official Rob Joyce stated that the quantity of Chinese cyber espionage operations had dropped "dramatically" since the 2015 agreement, though he also said that China hacking went "well beyond the bounds today of the agreement."
67 David E. Sanger and Steven Lee Myers, "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology," *New York Times,* November 29, 2018, https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.
68 Eichensehr, "The Law & Politics of Cyberattack Attribution."
69 Sujit Raman, "The Rule of Law in the Age of Great Power Competition in Cyberspace," U.S. Department of Justice, prepared remarks, May 21, 2019, https://www.justice.gov/opa/speech/associate-deputy-attorney-general-sujit-raman-delivers-remarks-aba-rule-law-initiative.
70 Ibid.
71 "Chinese Military Personnel Charged With Computer Fraud, Economic Espionage and Wire Fraud for Hacking Into Credit Reporting Agency Equifax," U.S. Department of Justice, press release, February 10, 2020, https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.
72 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House, 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/.
73 Eichensehr, "The Law & Politics of Cyberattack Attribution."
74 "The DoD Cyber Strategy," U.S. Department of Defense, 2015, https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/dod_cyber_2015.pdf.
75 Erica Lonergan, "That Makes This Attribution of Chinese Hacking Different," Carnegie Endowment for International Peace, July 22, 2021, https://carnegieendowment.org/2021/07/22/what-makes-this-attribution-of-chinese-hacking-different-pub-85023.
76 Stilgherrian, "Blaming Russia for NotPetya was Coordinated Diplomatic Action," ZDNet, April 11, 2018, https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.
77 "Background Press Call by Senior Administration Officials on Malicious Cyber Activity Attributable to the People's Republic of China," White House.
78 Eichensehr, "The Law & Politics of Cyberattack Attribution."
79 "DOJ Press Conference Transcript October 19: Charges Against Russian Officers," Rev.com, October 19, 2020, https://www.rev.com/blog/transcripts/doj-press-conference-transcript-october-19-charges-against-russian-officers.
80 Joe Biden, "Remarks by President Biden at the Office of the Director of National Intelligence," White House, July 27, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/.
81 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House, 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/.
82 "Statement From the Press Secretary," White House, February 15, 2018 https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.
83 Nick Beecroft, "To Condemn Chinese Hacks, Hate the Game Not Just the Players," Carnegie Endowment for International Peace, July 23, 2021, https://carnegieendowment.org/2021/07/23/to-condemn-chinese-hacks-hate-game-not-just-players-pub-85025.
84 Julianne Pepitone, "China Is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper," NBC News, June 25, 2015, https://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881.
85 Florian J. Egloff, "Public Attribution of Cyber Intrusions."
86 "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government," White House, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.
87 Perri Adams, Dave Aitel, George Perkovich, and JD Work, "Responsible Cyber Offense," *Lawfare*, August 2, 2021, https://www.lawfareblog.com/responsible-cyber-offense.
88 Maurer and Hinck, "Persistent Enforcement."

89 Ellen Nakashima, "Iran Blamed for Cyberattacks on U.S. Banks and Companies," *Washington Post*, September 21, 2012, https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html.

90 William Wan and Ellen Nakashima, "Report Ties Cyberattacks on U.S. Computers to Chinese Military," *Washington Post*, February 19, 2013, https://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html?wprss&google_editors_picks=true.

91 Jon Bateman, "American Voters Deserve Facts on Outside Influence on This Election," *Hill*, July 26, 2020, https://thehill.com/opinion/national-security/509099-american-voters-deserve-facts-on-outside-influence-on-this-election.

92 Adam Stone, "How Leon Panetta's 'Cyber Pearl Harbor' Warning Shaped Cyber Command," Fifth Domain, https://www.fifthdomain.com/opinion/2019/07/30/how-leon-panettas-cyber-pearl-harbor-warning-shaped-cyber-command/; Aaron Boyd, "DNI Clapper: Cyber Bigger Threat Than Terrorism," *Federal Times,* February 4, 2016, https://www.federaltimes.com/management/2016/02/04/dni-clapper-cyber-bigger-threat-than-terrorism/; Brian Fung, "Cyberattacks Are the Number-One Threat to the Global Financial System, Fed Chair Says," CNN, April 12, 2021, https://www.cnn.com/2021/04/12/business/jerome-powell-cyberattacks-global-threat/index.html; and Aruna Viswanatha and Dustin Volz, "FBI Director Compared Ransomware Challenge to 9/11," *Wall Street Journal,* June 4, 2021, https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003.

93 D. Howard Kass, "CISA Needs More Money, Lawmakers Tell House Appropriations Committee," MSSPAlert, May 3, 2021, https://www.msspalert.com/cybersecurity-markets/americas/cisa-budget-needs/.

94 Florian J. Egloff, "Public Attribution of Cyber Intrusions."

95 "A Guide to Cyber Attribution," Office of the Director of National Intelligence, September 14, 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

96 Ellen Nakashima, "Political Appointees, Career Analysts Clashed Over Assessments of Russian, Chinese Interference in 2020 Election," *Washington Post*, January 8, 2021, https://www.washingtonpost.com/national-security/russia-china-election-interference-intelligence-assessment/2021/01/08/7dc844ce-5172-11eb-83e3-322644d82356_story.html; and National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

97 Florian J. Egloff and Andreas Wenger, "Public Attribution of Cyber Incidents," CSS Analyses in Security Policy, no. 244, Spring 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse244-EN.pdf.

98 Florian J. Egloff, "Contested Public Attributions of Cyber Incidents and the Role of Academia," *Contemporary Security Policy* 41, no. 1 (Fall 2019): 55–81, https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677324.

99 Herbert Lin, "Attribution of Malicious Cyber Incidents," Hoover Institution, 2016, https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

100 Mariam Baksh, "NSA Cyber Chief Warns Hackers Increasingly Use Commercial Tools to Stay Hidden," NextGov, September 29, 2021, https://www.nextgov.com/cybersecurity/2021/09/nsa-cyber-chief-warns-hackers-increasingly-use-commercial-tools-stay-hidden/185733/.

101 Sergiu Gatlan, "US Sanctions Cryptocurrency Exchange Used by Ransomware Gangs," Bleeping Computer, September 21, 2021, https://www.bleepingcomputer.com/news/security/us-sanctions-cryptocurrency-exchange-used-by-ransomware-gangs.

102 "Guide for Preventing Ransomware Attacks," CNCERT, August 11, 2021, https://www.cert.org.cn/publish/english/115/2021/20210811180857408105025/20210811180857408105025_.html.

103 Catalin Cimpanu, "Chinese Government Lays Out New Vulnerability Disclosure Rules," *Record*, July 14, 2021, https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/; see also http://www.gov.cn/zhengce/zhengceku/2021-07/14/content_5624965.htm.

104 "Regulation to Strengthen Protection Over Critical Information Infrastructure," State Council of China, 2021, https://english.www.gov.cn/policies/latestreleases/202108/17/content_WS611b8062c6d0df57f98de907.html.

105 Scott Ferguson, "House SolarWinds Hearing Focuses on Updating Cyber Laws," Data Breach Today, February 26, 2021, https://www.databreachtoday.com/house-solarwinds-hearing-focuses-on-updating-cyber-laws-a-16078.

106 Lauren Feiner, "U.S. Reportedly Prepares Action Against Russia After Major Cyberattack," CNBC, March 8 2021, https://www.cnbc.com/2021/03/08/us-prepares-to-take-action-against-russia-after-major-cyber-attack.html.

107 "Colonial Pipeline Cyber Incident," U.S. Office of Cybersecurity, Energy Security, and Emergency Response, press release, accessed March 3, 2022, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

108 "FBI Statement on Compromise of Colonial Pipeline Networks," FBI National Press Office, press release, May 10, 2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks.

109 Edward Helmore and Joan E Greve, "Biden Says 'No Evidence' Russia Involved in US Pipeline Hack but Putin Should Act," *Guardian*, May 10, 2021, https://www.theguardian.com/us-news/2021/may/10/colonial-pipeline-shutdown-us-darkside-message.

110 "Letter – Imposing Additional Sanctions With Respect to North Korea," White House, press release, January 2, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/letter-imposing-additional-sanctions-respect-north-korea

111 "North Korean Actors Spear Phish U.S. Electric Companies," *FireEye*, October 11, 2017, https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html.

112 "CISA, TREASURY, FBI And USCYBERCOM Release Cyber Alert on Latest North Korea Bank Robbing Scheme," Cybersecurity and Infrastructure Agency, press release, February 05, 2021, https://www.cisa.gov/news/2020/08/26/cisa-treasury-fbi-and-uscybercom-release-cyber-alert-latest-north-korea-bank.

113 Manshu XU and Chuanying LU, "China–U.S. Cyber-Crisis Management, *China International Strategy Review* 3, (Summer 2021): 97–114, http://link.springer.com/article/10.1007/s42533-021-00079-7.

114 Edward Wong, "National Security Adviser Meets With Chinese President Before His U.S. Visit," *New York Times*, August 28, 2015, https://www.nytimes.com/2015/08/29/world/asia/susan-rice-xi-jinping-china.html.

115 "U.S., Chinese Officials Meet on Cyber Security Issues: White House," Reuters, September 12, 2015, https://www.reuters.com/article/idUSKCN0RC0S420150913.

116 Ministry of Foreign Affairs of China. Outcome list of President Xi Jinping's state visit to the United States, 2015. See https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml.

117 Elizabeth Thomas, "US-China Relations in Cyberspace: The Benefits and Limits of a Realist Analysis," E-International Relations, August 28, 2016, https://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/.

118 Sean Lyngaas, "Biden Says He Gave Putin List of 16 Sectors That Should Be Off-Limits to Hacking," Cyberscoop, June 16, 2021, https://www.cyberscoop.com/biden-putin-summit-russia-geneva/.

119 Elena Chernenko, "Axis Against Evil," Newspaper, *Kommersant,* No. 176, September 29, 2021, p. 6, https://www.kommersant.ru/doc/5007866

120 Nandita Bose, "Biden: If U.S. Has 'Real Shooting War' It Could Be Result of Cyber Attacks," Reuters, July 28, 2021, https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/.

121 "White House Brings 30 Nations Together for Counter-Ransomware Even," Cisomag, October 14, 2021, https://cisomag.eccouncil.org/white-house-brings-30-nations-together-for-counter-ransomware-event/; "Joint Statement of the Ministers and Representatives From the Counter Ransomware Initiative Meeting," White House, October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

122 "New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks," Cybersecurity and Infrastructure Agency, November 16, 2021, https://us-cert.cisa.gov/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability.

123 Herbert Lin, "Attribution of Malicious Cyber Incidents," Hoover Institution, 2016, https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

124 Ben Buchanan, *The Cybersecurity Dilemma* (Boston, MA: Oxford Scholarship Online, 2017), https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012.

125 Microsoft's "Digital Defense Report" provides an illustrative example of the interaction of these two analytic processes. See: "Microsoft Digital Defense Report," Microsoft, October 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

126 See Egloff and Smeets for a recent effort to conceptualize consistent factors constraining and enabling states' public attribution practice. Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," *Journal of Strategic Studies* (Spring 2021), https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117.

127 Jon Bateman's contribution to this volume highlights some of the effects publicity may have on government official's decisionmaking. See Jon Bateman, "The Purposes of U.S. Government Public Cyber Attribution."

128 Note that public attribution through press leaks is either directed by senior government officials (*plant* of classified information) or unauthorized by government (*leak* by an official acting independently). See: David E. Posen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review* 127, no. 2 (Winter 2013), https://harvardlawreview.org/2013/12/the-leaky-leviathan-why-the-government-condemns-and-condones-unlawful-disclosures-of-information/.

129 Ben Buchanan elaborates on the "cybersecurity dilemma"—the challenge of assessing states' intent in cyberspace means that actions taken for defensive reasons may be misinterpreted and inadvertently lead to escalation. See: Buchanan, *The Cybersecurity Dilemma*.

130 An interesting case in point is the UK's National Cyber Security Centre report on Huawei 5G network equipment, that in contrast with widespread U.S. assertions established that the security flaws uncovered originated in serious engineering flaws and inadequate security culture. See: "Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2018," Government of the UK's official website, July 19, 2018, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018.

131 "Microsoft Digital Defense Report," Microsoft, 47–69.
132 Renze Salet, "Framing in Criminal Investigation: How Police Officers (Re)construct a Crime," *Police Journal: Theory, Practice, and Principles* 90, no. 2 (Fall 2016): 128–42, https://journals.sagepub.com/doi/full/10.1177/0032258X16672470.
133 Ellen Nakashima, "Russian Spies Hacked the Olympics and Tries to Make It Look Like North Korea Did It, U.S. Officials Say," *Washington Post*, February 24, 2018, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.
134 Heajune Lee, "Strategic Publicity?: Understanding US Government Cyber Attribution," Stanford Digital Repository, Spring 2021, https://purl.stanford.edu/py070wt8487.
135 For discussion of the alleged utility of forward defense strategy in defending the United States against cyber attacks, see: Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.
136 Luca Follia and Adam Fish, *Hacker States* (Cambridge, Massachusetts: MIT Press, 2020), https://mitpress.mit.edu/books/hacker-states.
137 For a fascinating discussion of the privateering analogy to cyberspace proxy actions see: Florian J. Egloff, "Cybersecurity and the Sage of Privateering," Carnegie Endowment for International Peace, October 16, 2017, https://carnegieendowment.org/2017/10/16/cybersecurity-and-age-of-privateering-pub-73418.
138 Tim Maurer, *Cyber Mercenaries* (Washington, DC: Cambridge University Press, 2018), https://www.cambridge.org/core/books/cyber-mercenaries/B685B7555E1C52FBE5DFE6F6594A1C00.
139 Egloff and Smeets, "Publicly Attributing Cyber Attacks."
140 Florian J. Egloff, "Public Attribution of Cyber Intrusions," *Journal of Cybersecurity* 6, no. 1 (Fall 2020) https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454.
141 Lee, "Strategic Publicity?"
142 "Microsoft Digital Defense Report," Microsoft.
143 Dan McWhorter, "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant*, February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
144 Michael S. Schmidt and David Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times:* May 19, 2014, https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html.
145 Garrett Derian-Toth et al., "Opportunities for Public and Private Attribution of Cyber Operations," NATO Cooperative Cyber Defence Centre of Excellence, 2021, https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf.
146 Jordan Robertson and Michael Riley, "New Evidence of Hacked Supermicro Hardware Found in US Telecom," Bloomberg, October 9, 2018, https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom.
147 Some officials, speaking on the condition of anonymity, admitted such actions were firstly developed during the George W. Bush administration. See: Ellen Nakashima and Joby Warrick, "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say," *Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.
148 Byron Acohido, "NSA Chief Alexander Defends PRISM, Deflects Hecklers," *USA Today*, accessed December 3, 2021, https://www.usatoday.com/story/cybertruth/2013/07/31/nsas-alexanders-defends-prism-deflects-hecklers/2604533/.
149 Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace," *Diplomat*, January 19, 2017, accessed December 3, 2021, https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/.
150 James A Lewis, "Toward a More Coercive Cyber Strategy," Center for Strategic and International Studies, 2021, https://www.csis.org/analysis/toward-more-coercive-cyber-strategy.
151 Philip Ewing, "Election Security Boss: Threats to 2020 Are Now Broader, More Diverse," NPR, January 22, 2020, https://www.npr.org/2020/01/22/798186093/election-security-boss-threats-to-2020-are-now-broader-more-diverse.
152 Chen Dongxiao, Lu Chuanying, Sun Haiyong, and Jiang Xudong, "Competition Without Catastrophe: A New China-U.S. Cybersecurity Agenda," SIIS, February 2021, http://www.siis.org.cn/Report/3656.jhtml.
153 "18 U.S. Code § 1030 - Fraud and Related Activity in Connection With Computers," Legal Information Institute, accessed March 3, 2022, https://www.law.cornell.edu/uscode/text/18/1030.
154 James Crawford and Simon Olleson, *The Nature and Forms of International Responsibility* (Oxford, UK: Oxford University Press, 2003), 415–449.
155 James A. Lewis, "Toward a More Coercive Cyber Strategy," Center for Strategic and International Studies, 2021, https://www.csis.org/analysis/toward-more-coercive-cyber-strategy.
156 "Foreign Threats to the 2020 US Federal Elections," National Intelligence Council, March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

157 "Congressional-Executive Commission on China, Annual Report, 2020," U.S. Department of Justice, December 2020, https://www.justice.gov/eoir/page/file/1366421/download.

158 "Significant Cyber Incidents," Center for Strategic and International Studies, November 5, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

159 Jordan Robertson and Michael Riley, "New Evidence of Hacked Supermicro Hardware Found in US Telecom," Bloomberg, October 9, 2018, https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom.

160 Sebastian Moss, "Apple Denies Chinese Spy Chip Claims in a Letter to US Congress," Data Centre Dynamics, October 8, 2018, https://www.datacenterdynamics.com/en/news/apple-denies-chinese-spy-chip-claims-letter-us-congress/.

161 Schmidt and Sanger, "5 in China Army Face U.S. Charges of Cyberattacks."

162 Emilio Iasiello, "Chinese Company Outs U.S. Cyber Espionage and Sends a Message," OODA Loop, March 2, 2022, https://www.oodaloop.com/archive/2022/03/02/chinese-company-outs-u-s-cyber-espionage-and-sends-a-message/; and Pierluigi Paganini, "CIA Hacking Unit APT-C-39 Hit China Since 2008," Security Affairs, March 4, 2020, http://securityaffairs.co/wordpress/98885/apt/cia-hacking-china.html.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Nuclear Policy Program

The Carnegie Nuclear Policy Program works to strengthen international security by diagnosing acute nuclear risks, informing debates on solutions, and engaging international actors to effect change. The program's work spans deterrence, disarmament, nonproliferation, nuclear security, and nuclear energy.

Shanghai Institutes for International Studies

Founded in 1960, the Shanghai Institutes for International Studies(SIIS) is a government-affiliated high-caliber think tank dedicated to informing government decision-making by conducting policy-oriented studies in world politics, economics, foreign policy, and international security. SIIS maintains intensive and extensive exchanges and cooperation with research institutions at home and abroad, bolstering China's international influence and soft power.

SIIS boasts an authorized size of 106 full-time research fellows and staff, including 60% senior fellows. SIIS was ranked one of the top ten Chinese think tanks In 2006, and one of the top ten global think tanks (non-American) in 2008. SIIS comprises six institutes and six research centers, namely, the institute for global governance studies, the institute for foreign policy studies, the institute for world economic studies, the institute for international strategic studies, the institute for comparative politics and public policy, the institute for Taiwan, Hong Kong& Macao Studies, the center for American studies, the center for Asia-Pacific Studies, the center for Russian and Central Asian Studies, the center for West Asia and Africa studies, the center for European studies, and the center for maritime and polar studies. SIIS has also set up six in-house research platforms, i.e., the research base on people's diplomacy of Shanghai, center for the study of Chinese diplomatic theory and practice, center for world politics and political parties, center for China-South Asia cooperation, center for BRI and Shanghai studies, and center for international cyber governance. In addition, SIIS is an institutional member of the Shanghai International Strategic Studies Association and the Shanghai International Relations Association.

Research Center for Global Cyberspace Governance

The Research Center for Global Cyberspace Governance is a think tank specialized on the topics of cybersecurity and global cyberspace governance, with the purpose of exploring the global cybersecurity landscape and national cybersecurity strategies, while promoting the creation of global cyberspace governance mechanisms. The Research Center for Global Cyberspace Governance was founded in December 2018 in a joint effort by the Shanghai Institutes for International Studies, the PLA National Defense University, Fudan University, Nanjing University, Xiamen University, the Shanghai Academy of Social Sciences and others.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org

上海国际问题研究院
SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES

en.siis.org.cn