Institutionalizing Transnational Cyber Attribution
Internet Governance Project

Abstract

Authoritative attribution of cyberattacks to nation-state actors requires more than purely technical solutions. New institutions are needed to develop the credibility and procedural checks and balances that can take attribution beyond one nation pointing its finger at one of its adversaries. This white paper explores the attribution challenge, reviews proposed models for new institutions, and sketches an agenda for future research.

Keywords—attribution; cybersecurity; forensics; governance; internet; international

Institutionalizing Transnational Cyber Attribution:
A survey and research agenda

Karl Grindal, Brenden Kuerbis, Farzaneh Badiei, Milton Mueller

Introduction

After the United States blamed China for the Office of Personnel Management intrusion in 2015, China called speculation on their involvement neither "responsible nor scientific."[1] They subsequently suggested it was "imperative to stop groundless accusations, [and] step up consultations to formulate an international code of conduct..."[2] The U.S. - China exchange raises a critical question: what qualifies as "groundless accusations," and what would "responsible and scientific" attribution of nation state-sponsored attacks look like? The incident raised another question as well: what is the current U.S. process for attribution, and is it achieving its aims?

The authors have maintained a consistent interest in addressing the challenges of attribution in cyberspace through new transnational institutions. This topic has been explored through presentations on the need for an International Attribution Organization at RightsCon 2018, a lightning talk at the North American Network Operators' Group (NANOG), a lecture at the Institute for Information Security & Privacy, our past blog posts on the subject, and in forthcoming research papers.[3] Throughout this research we have maintained that authoritative attribution of cyberattacks to nation-state actors requires more than purely technical solutions. New institutions are needed to develop the credibility and procedural checks and balances that can take attribution beyond one nation pointing its finger at one of its adversaries. This document will explore the attribution challenge, review proposed models for new institutions, and sketch an agenda for future research. The authors' expertise in the development of transnational institutions in the domain name space has direct policy relevance to this case, as a new institution may be needed to hold offensive actors responsible and deter future cyber attacks.

The role of cyber attribution in deterrence and accountability

One can defend against a cyber attack but without attribution, attackers lack a deterrent. At best, secure systems increase the time needed to find a vulnerability to a point beyond that which the attacker is

[1] "Cyber Intrusion into U.S. Office of Personnel Management: In Brief" (Washington D.C.: Congressional Research Service, July 17, 2015), https://fas.org/sgp/crs/natsec/R44111.pdf.
[2] Ibid.
[3] "A Global Cyber-Attribution Organization: Thinking it through," *Internet Governance Project blog*, June 4, 2017. "Defusing the Cybersecurity Dilemma Game through Attribution and Network Monitoring." *Internet Governance Project* blog, April 13, 2018. "Beyond Mapping the Cybersecurity Landscape: A Look into the Evolution of Cybersecurity Governance Structures," paper presented at International Studies Association, March, 2018.

willing to spend. Without proper incentives to restrain malicious attacker behavior, be they state or non-state, it's unreasonable to expect the present situation to change.

Accurate attribution requires experienced threat intelligence and digital forensics experts. While governments and threat intelligence groups will attribute attacks to specific intrusion sets, sometimes even linking these to specific actors, there is no internationally recognized forensic process with an evidentiary based level of confidence. Rather, attribution is more often than not based on limited evidence and the reputation of the attributing entity. Considering that both attributing groups and attackers could be based anywhere in the world, without a recognized standard and institutionalized process for attribution can we expect a global coalition to implement sanctions?

There is an important distinction between identifying intrusion sets and assigning them to an adversary or "threat group," and linking this adversary with a known state or non-state actor. Robert Lee refers to the latter as "true attribution."[4] This two part distinction can be compared to Herb Lin's model, developed in the paper *Attribution of Malicious Cyber Incidents,*[5] which uses three levels of attribution: machines, human operators, and the ultimate party responsible. In Mandiant's 2013 attribution of APT-1 to the China PLA Unit 612398[6] all three levels of Lin's model are described. At the lowest level would be IP addresses associated with command and control servers. Next, is attribution to a human operator; the Mandiant report identifies a persona who went by the alias "ugly gorilla," but associated this with the real person Wang Dong. Ultimately though, the report is attributing APT-1 to China's Peoples Liberation Army and hence the Chinese state.

Defining an ultimate responsible party can be particularly challenging when it comes to state involvement. Even when a person is clearly identified as being in the attributed country, it is not necessarily clear from the forensics whether that person was a contractor or an employee, or whether they were operating under express instructions or on their own. Jason Healey's Spectrum of State Responsibility acknowledges that states employ hackers, contract out hacking, encourage hacking, or permit its use within their jurisdiction, each level representing a different degree of state responsibility.[7]

The challenge of authoritative attribution to nation-state actors

Technical intelligence builds on past incidents to create intrusion sets, that is the set of tools, infrastructure or tactics, techniques and procedures (TTPs) from previous attacks that are grouped together and associated with a common actor. This process has some general standardization by convention and predictive success, but there is no one correct method. Accordingly, SANS in 2010 noted that:

---

[4] Robert M. Lee. "The Problems with Seeking and Avoiding True Attribution to Cyber Attacks." *SANS DFIR* (blog), March 4, 2016.
[5] Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 2, 2016).
[6] Benjamin Wittes, "Mandiant Report on 'APT1,'" *Lawfare* (blog), February 20, 2013.
[7] Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

> There is no rule of thumb or objective threshold to inform when linked intrusions should become a campaign. The best measure is results: if a set of indicators effectively predict similar intrusions when observed in the future, then they have probably been selected properly.[8]

This predictive modeling creates important questions around the degrees of confidence, and how threat intelligence firms respond to novelty. Assuming an incident is correctly associated with an intrusion set, how is this intrusion set linked to a specific actor? Information like common language, activity during specific hours, the choice of targets, and level of complexity are often used to associate an incident group with a specific responsible threat actor. But this type of attribution extends beyond a purely technical association. The reuse of certain TTPs can complicate this attribution. For example, the vulnerability EternalBlue is reported to have been developed by the NSA, but was later exploited by Russia, North Korea, and Iran.[9]

Models of attribution help digital forensics to structure collected intelligence and compare it to known intrusion sets. Examples of these include, the Diamond Model of Intrusion Analysis developed by Caltagirone and Pendergast[10], and the Q-model developed by Thomas Rid and Ben Buchanan.[11] Both the Diamond Model and Q-model acknowledge the need for a nontechnical dimension to attribution. In the diamond model, the nontechnical dimension is described by the relationship between the victim and adversary. The strategic dimension of the Q-Model is described as a "function of what is at stake politically."[12]

While the political dimension of attribution might be quantified, it is necessarily relational, a product more of political science or intelligence studies than computer science. As sanctions or other disincentives are used to punish offensive cyber operations, we might expect cyber operations to adjust by taking steps to disguise their identity. The CIA's leaked Marble Framework, for example, has been described as providing the capability to change the language of the source code from English to another language like Russian or Farsi.[13] Meanwhile, cyber tools invented by one country are being reused by another. This suggests a technical race between forensic experts and counter-forensic obfuscation, but also an inequity of attribution based on state capability. Inequalities in attribution capabilities is said to have played a role in the breakdown of the UN Group of Governmental Experts on Developments in the Field of Information

---

[8] *Security Intelligence, Defining APT Campaigns.* SANS blog, June 21, 2010.
[9] Adam Segal. "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat." *Council on Foreign Relations* (blog), June 19, 2018.
[10] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intrusion Analysis," May 7, 2013, 61.
[11] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37. While this paper contains some excellent analysis of the problem of attribution, the "Q model" is not really a model in the social science sense but more a graphic representation of the authors' ideas.
[12] *Ibid.*
[13] Matt Burgess, "WikiLeaks Drops 'Grasshopper' Documents, Part Four of Its CIA Vault 7 Files," *Wired Magazine* (blog), May 7, 2017.

and Telecommunications in the Context of International Security (UN GGE).[14] While this obfuscation might serve powerful states well in the short term, it does little to mitigate the long term damage of offensive cyber attacks.

The attribution processes today

Preliminary research by IGP has started to categorize the origin and characteristics of publicly attributed incidents. This work builds on the Council on Foreign Relations dataset of state-sponsored cyber-incidents from 2005 to the present.[15] Reviewing 82 incidents identified by CFR between 2016 and the first quarter of 2018 (Table 1), we coded each case, identifying whether a state(s) and/or private actor(s) made a public attribution, as well as details related to the attribution including timing and outcome.

While publicly disclosed incident databases can be criticized as being just the tip of the iceberg, and two years of data based on a single dataset is certainly not conclusive, several interesting initial observations can be made. First, the vast majority of incidents (70, or 85%) resulted in some form of public attribution, with only 12 incidents (15%) not being attributed to a perpetrator. A small number of incidents, 7 (9%), were attributions involving both government(s) and private actor(s). These public attributions may have involved coordinated action between state and non-state actors (e.g., Wannacry), or attributions published

Table 1: Incident attributions made by actor type

	Year			
Actor type	2016	2017	2018 1Q	Grand Total
No attribution made	6	5	1	12
Both government(s) and private actor(s)	4	3		7
Government(s)	7	7	1	15
Private actor(s)	12	26	10	48
Grand Total	**29**	**41**	**12**	**82**

by non-state actors citing anonymous government sources, or what appeared to be separate attributions made independently (e.g., DNC hacks). Fifteen incidents (18%) were attributions made by government(s), including where identified government officials informally "named and shamed" alleged perpetrators, or

[14] Michael Schmitt, & Liis Vihul. (2017). International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. Retrieved August 17, 2018, from https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/

[15] Adam Segal and Alex Grigsby, "New Entries in the CFR Cyber Operations Tracker: Q1 2018," Council on Foreign Relations, April 23, 2018. The Council on Foreign Relations is not the only entity collecting and publishing cyber-incident data. Another example is the Dyadic Cyber Incident and Dispute Dataset by Valeriano and Maness (2015), as well as incident data collected by the New America Foundation. Methodological questions can be raised where differences occur between these datasets, e.g., in what is considered a state-sponsored "incident", or an attribution to a specific perpetrator.

formally accused them in official statements, reports, sanctions or indictments. The largest number of attributions have been made by private actors, a category that includes threat intelligence organizations, network security companies and news media organizations. The importance of these actors in attribution is evident from the number of attributions made by them, which seems to be nearly doubling every year. It also highlights the need for a standardized attribution process.

New developments in advancing attribution technology

Within the private sector and academia, research into attribution technologies has advanced, with promising technologies set to significantly improve forensic confidence. New areas of research include Artificial Intelligence, monitoring campaigns from start to end, and improved monitoring of infrastructure. Our colleagues at Georgia Tech, Manos Antonakakis and Michael Farrell at the Institute for Internet Security & Privacy, are investigating attribution as part of the Rhamnousia project.[16] This project is connecting diverse datasets to fuel new algorithmic attribution methods, that will expedite the process of attribution. These and other research efforts will increase the speed, confidence, and breadth of potential attribution, and represent dramatic improvements to digital forensics. But they will also raise questions about reproducibility (e.g., data collection) and the interaction with other legal and political attribution processes.

The need to develop legitimate attribution processes

While attribution technology is advancing, it does not and cannot eliminate the need for a legitimate process through which the technical attribution outcomes can be used to attribute an attack to a responsible party. Such a process has not been implemented, nor have the current processes been studied in detail. Attribution technologies focus on identifying specific machines and showing a pattern of behavior, not on identifying an organization or state. At some point, the evidence has to be assessed and independently reviewed, and that cannot be carried out through technological means alone. Even with next generation research on attribution, technology can only be used to establish technical attribution. A decision to blame a responsible party and impose sanctions on the identified attacker has to take place through a nontechnical process.

States may conclude the attribution process by filing an indictment against the perceived offender or offenders. This state-led process may ultimately lead to the identified attackers and sanctions might be imposed on them. In the United States, such indictments have usually been brought to a grand jury.[17] While some US allied countries have welcomed such procedures,[18] a perception of a lack of due process could hamper the credibility of attribution more broadly. The proceedings of grand juries are not open to the public, and the accused are not given a chance to defend themselves nor to provide evidence. Should

[16] John Toon, "$17 Million Contract Will Help Establish Science of Cyber Attribution," *Georgia Tech Research, Horizons* (blog), November 29, 2016.

[17] As indictments are filed as felony charges at the federal level, it has to be argued in front of a grand jury. For a specific indictment on hackers which took place through a grand jury process, see these documents.

[18] For example after the US Department of Justice indicted attributed a set of cyberattacks to Iranian hackers, backed by the Iranian revolutionary guard, the UK issued a statement supporting the US efforts in carrying out attribution.

an attribution process punish the accused while their guilt remains unproven through the procedures of a domestic court? If attribution is to transcend a technical meaning to carry legal weight, how should the accused respond? Any attribution process will need to answer these questions.

Proposals for a Domestic Attribution Organization

While technology could transform attribution, so could organizational changes. International forums like the European Union and NATO have not fully integrated their members' cyber capabilities. Cyber attribution capability remains concentrated in a few nation states and distributed across many private sector actors, some of whom may be clients or contractors of nation-states. States have made efforts at the national level to undertake cyber attribution through bureaucratic and judicial processes without a global standard. In the United States today, one of the last steps of this attribution process falls on the Secretary of Treasury's determination, in consultation with other cabinet officials, as to whether or not to freeze the actor's US-based assets.

The NSA's general counsel, Glenn Gersell, has suggested revising the national cyber strategy to centralize the attribution function into a single agency, implying that the NSA could play a leading role.[19] While this might best represent the current state of affairs, placing an attribution organization in a capable but secretive organization of a single nation-state would present unique challenges. The NSA does not have a great track record effectively managing disclosures or public communications. Nor is it likely to inspire trust in other countries.

Alternatively, Rosenzweig[20] and Shackelford[21] have proposed a National Cyber Safety Board in the United States, similar to an attribution organization that investigates the cause (e.g., network security flaws, human factors) and effects of an incident, and makes recommendations based upon findings. It is not explicitly performing attribution, although who is responsible might be inferred from the findings. But this model is confined to the national level. The most interesting and challenging issues in attribution are international.

The proposed *Cyber Deterrence and Response Act of 2018*, an attempt by the US Congress to codify into law two Executive Orders (13694 and 13757) which focus on punishing foreign actors engaging in significant malicious cyber-enabled activities, would place authority in the "President, acting through the Secretary of State," to determine which actors are engaged in, responsible for, or complicit in state-sponsored cyber activities. However, it leaves out any details about how this determination should occur. And here again, as an entirely unilateral initiative, the attributions made under this framework are unlikely to have global legitimacy.

The United States may be unique in having the number of independent agencies with cyber responsibilities that it does. While the above proposals relate to organizational structure, perhaps the

[19] Glenn S. Gerstell, "How We Need to Prepare for a Global Cyber Pandemic" NSA news release (April 9, 2018).
[20] Paul Rosenzweig, "The NTSB as a Model for Cybersecurity," R Street Shorts (May 9, 2018).
[21] Shackelford, Scott, and Austin Brady. "Is It Time for a National Cybersecurity Safety Board?" *Albany Law Journal of Science and Technology*, January 12, 2018.

glaring absence from these plans is how results will be communicated. While the proposal for a National Cyber Safety Board implies it would produce a report, what would distinguish this from today's private sector produced threat intelligence reports?

These proposals suggest that the degree of centralization, checks and balances, and the importance of expertise are all critical questions in the attribution space. However, these domestic solutions are insufficient to address the global nature of cybersecurity attacks. Sanction mechanisms, domestic rules, and executive orders in one country will not be perceived as legitimate and neutral by third party countries. This could reduce their willingness to participate in joint efforts, thereby allowing inter-state rivalries to limit collective action that would protect the Internet.

Proposals for a Transnational Attribution Institution

A Transnational Attribution Institution (TAI) could serve as a neutral global platform in which to perform authoritative public cyber-attributions. The TAI would be an independent entity or set of processes whose attribution decisions would aspire to be widely perceived as *unbiased*, *legitimate and valid*, even among parties who might be antagonistic (such as rival nation-states). Various proposals have been put forward with different scopes of activity, organizational structures, levels of stakeholder involvement, and evidentiary standards to potentially achieve such a process. Four of the leading attribution proposals use markedly different descriptions for this project. Microsoft describes their proposal as "a public-private forum to address attribution;"[22] the Atlantic Council called for a multilateral "attribution and adjudication council for cyber attacks rising to the [legal] level of 'armed conflict'";[23] a RAND study called for a "Global Cyber Attribution Consortium" of nonstate actors;[24] a Russian think tank called for an "independent, international cyber court or arbitrage method that deals only with government-level cyber conflicts."[25]

The International Attribution Organization proposed in the Microsoft Digital Geneva Convention, and its subsequent articulation,[26] is one such proposal that has been widely touted. This proposal included language that suggested that an independent attribution organization should 1) span the public and private sector while including civil society and academia 2) both investigate and serve an information sharing role and 3) resemble the International Atomic Energy Agency (IAEA). The initial proposal contained significant ambiguity as to whether or not this is describing a multistakeholder or multilateral model.

---

[22] Scott Charney, "Cybersecurity Norms for Nation-States and the Global ICT Industry," *Microsoft on the Issues* (blog), June 23, 2016.
[23] Jason Healey et al., "Confidence-Building Measures in Cyberspace: A Multiskeholder Approach for Stability and Security" (Washington, D.C.: Atlantic Council, November 2014).
[24] John Davis et al., *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND Corporation, 2017), https://doi.org/10.7249/RR2081.
[25] Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," *Council on Foreign Relations* (blog), February 23, 2018.
[26] Scott Charney et al., "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms" (Microsoft Corporation, June 2016).

The Atlantic Council's 2014 *Confidence Building Measures in Cyberspace* report proposes a multilateral "attribution and adjudication council for cyber attacks rising to the [legal] level of 'armed conflict'."[27] While the scope is only limited to incidents that rise above an international legal threshold, Healey et al. suggests that these assessments should result in the application of an enforcement mechanism. The organization, like the Digital Geneva Convention draws on the IAEA for inspiration, but also the Biological Weapons Convention and Nuclear Nonproliferation Treaty.

RAND's Stateless Attribution Report draws on both Atlantic Council's and Microsoft's work, but suggests that "an attribution organization should be managed and operated independently from states." Their report also differs from the Atlantic Council report in suggesting that an enforcement role is not needed. While the RAND Report classifies the Atlantic Council proposal as including nonstate actors in collaborative investigations, this seems to confuse organizational management and support. As the Atlantic Council's proposal makes use of private sector data and expertise as a multilateral entity, the RAND proposal does not explain how nonstate actors would assist targeted states without their involvement.

The Chernenko et al. paper presents an interesting contrast to the IAEA model for attribution. While not denying the significance of private sector actors, the Chernenko et al. proposal is explicitly state based, recommending an "independent, international cyber court...that deals only with government-level cyber conflicts"[28] This scoping is less expansive than the Microsoft proposal, but more inclusive than the Atlantic Council's, covering government-level cyber conflict which would include those below the threshold of armed conflict.

Each proposal offers different scopes of activity for a cyber attribution organization and pushes for dramatically different structures (e.g., multilateral vs. nongovernmental, or hierarchical vs. networked). And while the RAND Report[29] makes powerful arguments as to why states have conflicting incentives to participate in an attribution organization and cautions against their membership in any Consortium, none of the above proposals explicitly consider the incentives for private actors to participate in the forensic process. IGP is tracking TAI proposals and critiquing their viability, but believes more research is needed before a consensus can form.

Challenges to proposed models (challenges of collective action in attribution)

Three major challenges are likely to present themselves in the creation of a transnational attribution institution; these include geopolitical conflict, building independent capability, and private sector participation. These challenges overlap with, but are more institutional than, those challenges identified by the RAND study: effective attribution and persuasive communication. Efficacy and communication will be contingent on the breadth of participation of public and private entities and their willingness to be

[27] Healey, note 21 above.
[28] Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms."
[29] Davis et al., *Stateless Attribution*.

transparent with the evidence. As with any political challenge, getting collective action from actors with competing interests presents a challenge.

Adversarial geopolitical relationships are likely to extend to any international forum. The advantage of such forums is that by joining the forum the participants agree to adhere to the constitutive as well as procedural rules, even when they disagree over the particulars. The neutrality of international bodies is often established through the professionalism of participants: either a technical independence as described in the RAND study or a judicial independence might claim to embody this ethos. Should states as political actors be involved, as described by the Atlantic Council proposal, a majoritarian ethos might be needed to result in collective action. A consensus based solution proposed in the Microsoft Digital Geneva Convention research, could certainly face challenges acquiring unanimity.

In addition to the geopolitical challenges of managing an organization are those of creating trustworthy assessments. The Organisation for the Prohibition of Chemical Weapons (OPCW) manages to maintain global trust in its forensics with an independent laboratory, whose work it supplements with a network of over 20 certified laboratories[30] distributed across numerous national jurisdictions. While the same strategy might help to supplement the capability of an attribution based organization, building this capability will require financial resources. Finding dedicated financial resources for a TAI, might create their own challenges. Would a country finance an organization tasked with rooting out its espionage operations, what incentives are there for the private sector?

The cyberspace domain is uniquely defined by private sector participation and ownership of the core infrastructure. In this respect, Microsoft's Digital Geneva Convention is served well by including the private sector, but creates a potential contradiction by drawing on the example of the International Atomic Energy Agency. We can imagine an independent, member state-funded international organization, like that of the IAEA. Or by empowering the "the private sector, academia and civil society,"[31] is Microsoft suggesting a multistakeholder model? At face value, it appears that governments will set the rules, while private actors will lend their services and data, but nothing is stated about how these interests might be aligned. If a subset of private sector cyber security firms have advanced forensic capability equaling or exceeding that of most states, why would they participate in a monopsony attribution organization? Presumably, they would have to be compensated. Alternatively, if access to the Internet's infrastructure allows an investigation to backtrack the origins of an attacker, what process should enable the acquisition of relevant evidence? Should this layer of attribution include partnerships with national law enforcement or permit international inspections? Either way, this potentially burdens the private sector and has implications for global privacy.

[30] "Lab Receives OPCW Recertification." *Lawrence Livermore National Laboratory* (blog), February 8, 2013. https://www.llnl.gov/news/lab-receives-opcw-recertification.

[31] Scott Charney et al., "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms" (Microsoft Corporation, June 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

Research agenda going forward

At present, threat intelligence firms and national security agencies are the primary producers of cyber forensics and attribution. While ideal models for attribution and novel policy proposals were described above, too little is known about the current state of affairs. Modeling of state(s) behavior in attribution should also incorporate the role of private actors.[32] A research agenda going forward should attempt to better understand the process of attribution, and, based on empirical research and the current state of attribution, provide novel institutional designs and processes that go beyond merely replicating the current international organizations. This might include exploring research questions like:

- How effective is attribution at initiating an international response?
- How does the public and state response to attribution differ based on whether the forensic assessment comes from the private sector, state intelligence, law enforcement, or second hand media reporting?
    - Are there different accepted levels of confidence?
    - How does the level of public transparency differ?
- How do geopolitical rivalries undermine the confidence placed in attribution?
- Is a hierarchically-organized institution really needed to align participant incentives, or can a more loosely organized form of networked governance or market satisfice?
- How would different visions for attribution address the concerns of stakeholders, distribute costs, and get off the ground?

With a better understanding of the present state of attribution, we can better seek to define governance based solutions. This paper has described a number of competing visions for an attribution based organization. Without greater clarity on the trade-offs inherent to each, political capital might be saved and more efficiently directed at a workable solution.

IGP will continue to explore these questions, and to seek a better understanding of how governance models might help build global trust in forensic evidence so that responsible parties can be held accountable. Despite the capacity of advanced threat actors, the need to protect intelligence sources and methods, and conflicting nationalistic biases we believe that global consensus is possible.

[32] Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(11), 2825–2830. http://doi.org/10.1073/pnas.1700442114

References

Burgess,M. “WikiLeaks Drops ‘Grasshopper’ Documents, Part Four of Its CIA Vault 7 Files,” Wired Magazine (blog), May 7, 2017, https://www.wired.co.uk/article/cia-files-wikileaks-vault-7.

Caltagirone, S. Andrew Pendergast, and Christopher Betz, “The Diamond Model of Intrusion Analysis,” May 7, 2013, 61.

Charney, S et al. “From Articulation to Implementation: Enabling Progress on Cybersecurity Norms” (Microsoft Corporation, June 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

Charney, S “Cybersecurity Norms for Nation-States and the Global ICT Industry,” Microsoft on the Issues (blog), June 23, 2016, https://blogs.microsoft.com/on-the-issues/2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/.

Chernenko, E., Demidov, O., and Lukyanov, F. “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms,” Council on Foreign Relations (blog), February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Davis II, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. (2017). *Stateless Attribution*. RAND Corporation.

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(11), 2825–2830. http://doi.org/10.1073/pnas.1700442114

Finklea, K., Christensen, M. D., Fischer, E. A., Lawrence, S. V., & Theohary, C. A. (2015, July). Cyber Intrusion into US Office of Personnel Management: In Brief. Congressional Research Service https://fas.org/sgp/crs/natsec/R44111.pdf.

Gerstell, G. “How We Need to Prepare for a Global Cyber Pandemic” (April 9, 2018), https://www.nsa.gov/news-features/speeches-testimonies/speeches/09Apr2018-gerstell-cyber-pandemic.shtml.

Healey, J ed., A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013).

Healey, J et al., “Confidence-Building Measures in Cyberspace: A Multiskeholder Approach for Stability and Security” (Washington, D.C.: Atlantic Council, November 2014),

http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.

Internet Governance Project, "Defusing the Cybersecurity Dilemma Game through Attribution and Network Monitoring.", blog, April 13, 2018. https://www.internetgovernance.org/2018/04/13/defusing-cybersecurity-dilemma-game-attribution-network-monitoring/

Lee R. "The Problems with Seeking and Avoiding True Attribution to Cyber Attacks." SANS DFIR (blog), March 4, 2016. https://digital-forensics.sans.org/blog/2016/03/04/the-problems-with-seeking-and-avoiding-true-attribution-to-cyber-attacks/.

Lin H, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 2, 2016), https://papers.ssrn.com/abstract=2835719.

Rid., T and Buchanan., B. "Attributing Cyber Attacks," Journal of Strategic Studies 38, no. 1–2 (January 2, 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

Rep. Ted Yoho, "Cyber Deterrence and Response Act of 2018," H.R. 5576 § (2018), https://www.congress.gov/bill/115th-congress/house-bill/5576/text.

Rosenzweig, P. "The NTSB as a Model for Cybersecurity," R Street Shorts (R Street, May 9, 2018), https://www.rstreet.org/2018/05/09/the-ntsb-as-a-model-for-cybersecurity/.

Michael Schmitt, & Liis Vihul. (2017). International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. Retrieved August 17, 2018, from https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/

Security Intelligence, Defining APT Campaigns (2010) https://digital-forensics.sans.org/blog/2010/06/21/security-intelligence-knowing-enemy

Segal, A,. "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat." Council on Foreign Relations (blog), June 19, 2018. https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat.

Segal, A., Grigsby, A., "New Entries in the CFR Cyber Operations Tracker: Q1 2018," Council on Foreign Relations, April 23, 2018, https://www.cfr.org/blog/new-entries-cfr-cyber-operations-tracker-q1-2018.

Toon, J. "$17 Million Contract Will Help Establish Science of Cyber Attribution," Georgia Tech Research, Horizons (blog), November 29, 2016, http://www.rh.gatech.edu/news/584327/17-million-contract-will-help-establish-science-cyber-attribution.

Wittes, B. “Mandiant Report on ‘APT1,’” Lawfare (blog), February 20, 2013, https://www.lawfareblog.com/mandiant-report-apt1.

Collected Resources

July 6, 2018

Original Sources:

Jack Goldsmith. “The Significance of Panetta’s Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks.” *Lawfare* (blog), October 15, 2012. https://www.lawfareblog.com/significance-panettas-cyber-speech-and-persistent-difficulty-deterring-cyberattacks.

Jason Healey. “Beyond Attribution: Seeking National Responsibility for Cyber Attacks.” Atlantic Council, Cyberstatecraft Initiative, January 2012. https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf .

Robert M. Lee. “The Problems with Seeking and Avoiding True Attribution to Cyber Attacks.” *SANS DFIR* (blog), March 4, 2016. https://digital-forensics.sans.org/blog/2016/03/04/the-problems-with-seeking-and-avoiding-true-attribution-to-cyber-attacks/.

Rid, Thomas, and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37. https://doi.org/10.1080/01402390.2014.977382.

IGP Work

Kuerbis, Brenden. “Defusing the Cybersecurity Dilemma Game through Attribution and Network Monitoring.” *Internet Governance Project* (blog), April 13, 2018. https://www.internetgovernance.org/2018/04/13/defusing-cybersecurity-dilemma-game-attribution-network-monitoring/.

Mueller, Milton. “A Global Cyber-Attribution Organization – Thinking It Through.” *Internet Governance Project* (blog), June 4, 2017. https://www.internetgovernance.org/2017/06/04/a-global-cyber-attribution-org/.

Data

Adam Segal, and Alex Grigsby. “New Entries in the CFR Cyber Operations Tracker: Q1 2018.” Council on Foreign Relations, April 23, 2018. https://www.cfr.org/blog/new-entries-cfr-cyber-operations-tracker-q1-2018.

Theory Development

Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. “The Diamond Model of Intrusion Analysis,” May 7, 2013, 61.

Central Intelligence Agency. “A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis,” March 2009.

Jason Healey. “Innovation on Cyber Collaboration: Leverage at Scale.” Washington, D.C.: Atlantic Council, May 2018. http://www.atlanticcouncil.org/images/publications/Innovation-Cyber-WEB.pdf.

———. “The Argument for Mapping Cyber Response.” *The Cipher Brief* (blog), June 19, 2018. https://www.thecipherbrief.com/column_article/argument-mapping-cyber-response.

Nikolas Pitropakis, Emmanouil Panaousis, Alkiviadis Giannakoulias, George Kapakis, Rodrigo Diaz Rodriguez, and Panayiotis Sarigiannidis. “An Enhanced Cyber Attack Attribution Framework,” n.d.

Nunes, Eric, Paulo Shakarian, Gerardo I. Simari, and Andrew Ruef. “Argumentation Models for Cyber Attribution,” July 2016. https://arxiv.org/pdf/1607.02171v1.pdf.

Shakarian, Paulo, Gerardo I. Simari, Geoffrey Moores, and Simon Parsons. “Cyber Attribution: An Argumentation-Based Approach.” In *Cyber Warfare*, edited by Sushil Jajodia, Paulo Shakarian, V.S. Subrahmanian, Vipin Swarup, and Cliff Wang, 56:151–71. Cham: Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-14039-1_8.

Models for Attribution Institutions

Paul Rosenzweig. “The NTSB as a Model for Cybersecurity.” R Street Shorts. R Street, May 9, 2018. https://www.rstreet.org/2018/05/09/the-ntsb-as-a-model-for-cybersecurity/.

Solomon, Howard. “RightsCon Report: Universities Should Form Cyber Attribution Network.” *IT World Canada* (blog), May 18, 2018. https://www.itworldcanada.com/article/rightscon-report-universities-should-form-cyber-attribution-network/405399.

Shackelford, Scott, and Austin Brady. “Is It Time for a National Cybersecurity Safety Board?” *Albany Law Journal of Science and Technology*, January 12, 2018.

Chernenko, Elena, Oleg Demidov, and Fyodor Lukyanov. “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms.” *Council on Foreign Relations* (blog), February 23, 2018. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Davis, John, Benjamin Boudreaux, Jonathan Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael Chase. *Stateless Attribution: Toward International Accountability in Cyberspace*. RAND Corporation, 2017. https://doi.org/10.7249/RR2081.

Gerstell, Glenn S. “How We Need to Prepare for a Global Cyber Pandemic.” presented at the The Cipher Brief Threat Conference, Sea Island, Georgia, April 9, 2018. https://www.nsa.gov/news-features/speeches-testimonies/speeches/09Apr2018-gerstell-cyber-pandemic.shtml.

Healy, Jason, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd. “Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security.” Washington, D.C.: Atlantic Council, November 2014. http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.

Microsoft

Charney, Scott. “Cybersecurity Norms for Nation-States and the Global ICT Industry.” *Microsoft on the Issues* (blog), June 23, 2016. https://blogs.microsoft.com/on-the-issues/2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/.

Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze, and Paul Nicholas. “From Articulation to Implementation: Enabling Progress on Cybersecurity Norms.” Microsoft Corporation, June 2016. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

McKay, Angela, Jan Neutze, Paul Nicholas, and Kevin Sullivan. “International Cybersecurity Norms.” Microsoft Corporation, 2014. http://aka.ms/cybernorms.

Strategic Dimension of Attribution

Adam Segal. “The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat.” *Council on Foreign Relations* (blog), June 19, 2018. https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat.

Office of the National Counterintelligence Executive. “Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage,” October 2011. http://www.dni.gov/reports/20111103_report_fecie.pdf.

Government Funded Research

Carnegie Mellon Software Engineering Institute. “SEI Seeks Participants for Cyber Intelligence Study Sponsored by Office of the Director of National Intelligence.” *PR News Wire* (blog), November 16, 2018. https://www.prnewswire.com/news-releases/sei-seeks-participants-for-cyber-intelligence-study-sponsored-by-office-of-the-director-of-national-intelligence-300558050.html.

Models of Attribution in Other Domains

OPCW Conference of the States Parties. “OPCW Decision.” The Hague, Netherlands: Organisation for the Prohibition of Chemical Weapons, February 2, 2018. https://www.opcw.org/fileadmin/OPCW/CSP/C-I/en/C-I_DEC.13_Rev.1-EN.pdf.

OPCW Technical Secretariat. “Summary of the Report on Activities Carried out in Support of a Request for Technical Assistance by the United Kingdom of Great Britain and Northern Ireland.” The Hague, Netherlands: Organisation for the Prohibition of Chemical Weapons, April 12, 2018. https://www.opcw.org/fileadmin/OPCW/S_series/2018/en/s-1612-2018_e___1_.pdf.

Government Action

Boyd, Aaron. “Senate Wants More Cyber Intelligence.” *Nextgov* (blog), May 7, 2018. https://www.nextgov.com/cybersecurity/2018/05/senate-wants-more-cyber-intelligence/148010/.

James Van De Velde. “The Short-Sightedness of Obama-Era Cyber Operations Policy.” *The Cipher Brief* (blog), June 21, 2018.

https://www.thecipherbrief.com/column_article/short-sightedness-obama-era-cyber-operations-policy.

Response to Russian Hacking

Raphael Satter. “Russian Hackers Posed as IS to Threaten Military Wives.” *AP News*. May 8, 2018. https://apnews.com/4d174e45ef5843a0ba82e804f080988f.

John Markoff, and Andrew E. Kramer. “U.S. and Russia Differ on a Treaty for Cyberspace.” *The New York Times*. June 27, 2009. https://www.nytimes.com/2009/06/28/world/28cyber.html.

Michael Birnbaum. “In These Cyber War Games, the Fictional Foe Launching Attacks Sounds a Lot like Russia.” *The Washington Post*. May 4, 2018. https://www.washingtonpost.com/world/europe/in-these-cyber-war-games-the-fictional-foe-launching-attacks-sounds-a-lot-like-russia/2018/05/03/06494f8c-47cb-11e8-8082-105a446d19b8_story.html.

Ng, Alfred. “Dutch Government to Drop Kaspersky Lab, Citing Security Concerns.” *CNet* (blog), May 14, 2018. https://www.cnet.com/news/dutch-government-to-drop-kaspersky-lab-citing-security-concerns/.

Response to Iran Hacking

Bowden, John. “US Fears More Iranian Cyberattacks after Exit from Iran Deal: Report.” *The Hill* (blog), May 11, 2018. http://thehill.com/policy/technology/387372-us-fears-more-iranian-cyberattacks-after-exit-from-iran-deal-report.

Greenberg, Andy. “The Iran Nuclear Deal’s Unraveling Raises Fears of Cyberattacks.” *Wired Magazine* (blog), May 9, 2018. https://www.wired.com/story/iran-nuclear-deal-cyberattacks/.

Kovacs, Eduard. “Industry Reactions to Iran Cyber Retaliation Over U.S. Nuclear Deal Exit.” *SecurityWeek* (blog), May 10, 2018. https://www.securityweek.com/industry-reactions-iran-cyber-retaliation-over-us-nuclear-deal-exit.

McKeon, Amanda. “Iran Retaliation Likely After Nuclear Deal Dropped.” *Recorded Future* (blog), May 14, 2018. https://www.recordedfuture.com/podcast-episode-56/.

Gundert, Levi, Sanil Chohan, and Greg Lesnewich. “Iran’s Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations.” Recorded Future, May 9, 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf.

Corporate Action

Chris, Bing. “FireEye Denies ‘hack Back’ Claims Detailed in New Book.” *Cyberscoop* (blog), June 25, 2018. https://www.cyberscoop.com/fireeye-hack-back-david-sanger-book/.

FireEye. “Doing Our Part – Without Hacking Back.” *FireEye.Com* (blog), June 25, 2018. https://www.fireeye.com/blog/executive-perspective/2018/06/doing-our-part-without-hacking-back.html.

GaTech Actions

Toon, John. “$17 Million Contract Will Help Establish Science of Cyber Attribution.” *Georgia Tech Research, Horizons* (blog), November 29, 2016. http://www.rh.gatech.edu/news/584327/17-million-contract-will-help-establish-science-cyber-attribution.

———. “Faster Detection, Cleanup of Network Infections Are Goals of $12.8 Million Project.” *Georgia Tech Research, Horizons* (blog), May 14, 2018. http://www.rh.gatech.edu/news/606177/faster-detection-cleanup-network-infections-are-goals-128-million-project.

Other Sources

“20 Russian High-Profile Organizations Attacked by Spy Malware in Coordinated Op – FSB.” *RT* (blog), July 30, 2016. https://www.rt.com/news/353990-russia-cyber-attack-hackers/.

Bajak, Frank. “Correction: Cyberattack Fighter-Detained Story.” *U.S. News & World Report* (blog), May 17, 2018. https://www.usnews.com/news/best-states/wisconsin/articles/2018-05-16/british-cybersecurity-expert-heads-to-court-in-malware-case.