# Cyber Attribution: Can a New Institution Achieve Transnational Credibility?

Milton Mueller

Karl Grindal

Brenden Kuerbis

Farzaneh Badiei

## 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 US-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 raises another question as well: what is the current US process for attribution, and is it achieving its aims? This paper argues that authoritative attribution of cyberattacks to nation-state actors requires more than purely technical solutions. New, credible institutions are needed to develop procedural checks and balances that will make attribution more than one nation pointing its finger at an adversary. 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 led by non-state actors in critical Internet resources 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 amount of time it takes an attacker to find a vulnerability to a point beyond that which the attacker is willing to spend. Without proper incentives to restrain malicious attacker behavior, be they state or non-state, it is unreasonable to expect the present situation to change.

**Milton L Mueller** is Professor at the Georgia Institute of Technology (Atlanta, USA) in the School of Public Policy. He is the author of Will the Internet Fragment? (Polity, 2017), Networks and States: The global politics of Internet governance (MIT Press, 2010) and Ruling the Root: Internet Governance and the Taming of Cyberspace (MIT Press, 2002) are acclaimed scholarly accounts of the global governance regime emerging around the Internet.

Accurate attribution requires experienced threat intelligence and digital forensics experts advising decision-makers. While governments and threat intelligence groups will attribute attacks to specific intrusion sets, sometimes even linking these to specific actors, no internationally recognized forensic process with an evidentiary based level of confidence exists. Rather, attribution is often based on limited evidence and the reputation of the attributing entity. How can we expect a global coalition to implement sanctions when attributing groups and attackers could be based anywhere in the world, and there is no recognized standard or institutionalized process for attribution?

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." [3] This two-part distinction can be compared to Herb Lin's model, developed in the paper *Attribution of Malicious Cyber Incidents*, [4] which uses three levels of attribution: machines, human operators, and the ultimately responsible party. In Mandiant's 2013 attribution of APT-1 to the Chinese People's Liberation Army (PLA) Unit 612398 [5] all three levels of Lin's model are described. At the lowest level would be the IP addresses associated with command and control servers. Next is attribution to a human operator–the Mandiant report identifies a person who went by the alias "ugly gorilla" and associated this alias with the real person Wang Dong. Ultimately, the report attributed APT-1 to the PLA hence, the Chinese state.

Defining the ultimately responsible party can be particularly challenging when it comes to state involvement. Even when a person has been clearly identified as being inside or a citizen of the attributed country, it may not be clear from the forensics whether that person is a contractor, or an employee operating at the behest

THE CYBER DEFENSE REVIEW

Karl Grindal is a Ph.D. Student at the Georgia Institute of Technology's School of Public Policy and partner with the Internet Governance Project. Karl previously served as a Senior Analyst at Delta Risk LLC and as the Executive Director of the Cyber Conflict Studies Association (CCSA), a non-profit dedicated to advancing a research agenda on cyber conflict.

of their national government or operating 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, and each variation comes with a different degree of state responsibility. [6]

### The challenge of authoritative attribution to nation-state actors

Technical intelligence builds upon past incidents to create intrusion sets, or, the set of tools, infrastructure or tactics, techniques and procedures (TTPs) established during 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:

> 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 predicts similar intrusions when observed in the future, then they have probably been selected properly. [7]

This predictive modeling creates important questions around the degrees of confidence regarding attribution, 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 a common language, activity during specific hours, choice of targets, and the level of complexity of attack 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. [8]

**Brenden Kuerbis** is a Postdoctoral Fellow at the Georgia Institute of Technology, School of Public Policy and a former Fellow in Internet Security Governance at the Citizen Lab, Munk School of Global Affairs, University of Toronto. His research focuses on the governance of Internet identifiers, and the intersection of cybersecurity with forms of Internet governance.

Models of attribution help digital forensics to structure collected intelligence and compare it to known intrusion sets. An example is the Diamond Model of Intrusion Analysis developed by Caltagirone and Pendergast. [9] The so-called "Q-model" developed by Thomas Rid and Ben Buchanan contains some excellent analysis of the problem of attribution although it is a graphic representation of the authors' ideas rather than a scientific model. [10] Both approaches, however, 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." [11]

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. [12] 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 are said to have played a role in the breakdown of the United Nations (UN) Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. [13] 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 CYBER
DEFENSE REVIEW

**Farzaneh Badiei** is a postdoctoral researcher at the Georgia Institute of Technology, School of Public Policy and the Executive Director of Internet Governance Project. She holds a Ph.D. in law and economics from Hamburg University Germany.

### The attribution processes today

Preliminary research by Georgia Tech's Internet Governance Project has started to categorize the origin and characteristics of publicly attributed incidents. This work builds on the Council on Foreign Relations (CFR) dataset of state-sponsored cyber-incidents from 2005 to the present. [14] 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.

| Actor type | Year | | | |
|---|---|---|---|---|
| | 2016 | 2017 | 2018 IQ | 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** |

Table 1. Incident attributions made by actor type

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 by non-state actors citing anonymous government sources, or what appeared to be separate

attributions made independently (e.g., the Democratic National Committee hacks). Fifteen incidents (18%) were attributions made by government(s), including where identified government officials informally named alleged perpetrators, or 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.

The incident data also allow important distinctions to be made. Table 2 (below) shows attributions made to threat group(s) or state sponsor(s) by the actor type making the attribution. The total number of attributions made differs from the number of incidents (Table 1, previous page) as more than one entity in different actor types may be implicated per incident. Consistent with the incident observations above, private actors made substantially more attributions to both threat groups (31 versus 5) and state sponsors (38 versus 13) than did governments. Most attributions made by government(s) were made to a state sponsor. These attributions included the United States and allied countries accusing Iran, Russia and North Korea, as well as the United States implicating itself. As noted previously in Table 1 (previous page), governments made attributions in 15 incidents. Table 2 shows that governments attributed those incidents to state sponsors 13 times.

Governments (in this case, the US) attributed an attack to a threat group five times; in three of those times, the attribution was to both a threat group (APT28, APT 29, Lazarus) and an alleged state sponsor (Russia, North Korea). Only twice did a government (in this case, Switzerland) limit its accusation to a threat group (Turla), although a

| Attribution made by (actor type) | Incidents attributed to threat group | Incidents attributed to state sponsor |
|---|---|---|
| Both government(s) and private actor(s) | 4 | 3 |
| Government(s) | 5 | 13 |
| Private actor(s) | 31 | 38 |
| **Grand Total** | **40** | **58** |

Table 2. Attributions made by actor type to actor type

state sponsor was suspected. However, despite the appearance, a Chi-Square test concludes there is no significant difference between actor type regarding whom (threat group or state sponsor) they attribute incidents. Neither group is more likely, or perhaps better suited, to make attributions to a specific type of actor.

### *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 are investigating

attribution as part of the Rhamnousia project. [15] This project is connecting diverse datasets to fuel new algorithmic attribution methods which will speed up attribution. These and other research efforts will increase the speed, confidence, and breadth of potential attribution and represent dramatic improvements to digital forensics for their sponsors. But if individual states hoard this knowledge, they may not improve the general credibility of public attributions. Such military-funded efforts 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 must 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. The decision to blame a responsible party and impose sanctions on the identified attacker must 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 US, such indictments have usually been brought to a grand jury. [16] While some US-allied countries have welcomed such procedures, [17] 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 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 organizations like the European Union (EU) and North Atlantic Treaty Organization (NATO) have not fully integrated their members' cyber capabilities. Cyber attribution capability remains concentrated within 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 US 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 to freeze the actor's US-based assets.

The NSA's general counsel, Glenn Gerstell, 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. [18] While this might improve the current state of affairs, placing an attribution organization in a capable but secretive organization of a single nation-state would present unique challenges. While the NSA is a robust organization, it lacks an effective public affairs piece that impactfully manages disclosures or public communications. This aspect would help to inspire public confidence in its mission as well as trust from other countries.

Alternatively, Rosenzweig [19] and Shackelford [20] have proposed a National Cyber Safety Board in the US, something 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 responsibility 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 U.S. Congress to codify into law two Executive Orders (13694 and 13757) that focus on punishing foreign actors for 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. Even within the US, without a transparent process and evidence, attribution would be subject to question.

The US may be unique in having the number of independent agencies with cyber responsibilities. While the above proposals relate to organizational structure, perhaps the 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, transparency, 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;" [21] the Atlantic Council called for a multilateral "attribution and adjudication council for cyber-attacks rising to the [legal] level of 'armed conflict'"; [22] a RAND study called for a "Global Cyber Attribution Consortium" of non-state actors; [23] a Russian think tank called for an "independent, international cyber court or arbitrage method that deals only with government-level cyber conflicts." [24]

The International Attribution Organization proposed in the Microsoft Digital Geneva Convention, and its subsequent articulation, [25] is one such proposal. This proposal included language suggesting 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 this is describing a multi-stakeholder or multilateral model.

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'." [26] 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 implying that an enforcement role is not needed. While the RAND Report classifies the Atlantic Council proposal as including non-state 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 non-state 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" [27] This scoping is smaller 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 [28] 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. The Internet Governance Project (IGP) is tracking TAI proposals and critiquing their viability but believes more research is needed before a consensus can form.

Finally, a recent development highlights the growing demand for and stakes of neutral and widely accepted attribution. In late 2018, Mondelez International, Inc. filed a complaint against Zurich American Insurance Company. [29] In it, Mondelez sought relief for Zurich's alleged breach of its contractual obligations to Mondelez under an all-risk property insurance policy covering "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction ....". Zurich has asserted that the NotPetya attack, which caused damages more than $100M to Mondelez, was launched by a state-based actor and therefore excluded from the policy. Mondelez claims that Zurich bears the burden of proving the applicability of the exclusion. While numerous Western governments publicly accused the Russian government of launching NotPetya, Russia has steadfastly denied its responsibility. [30] However the court rules, it is unclear how the standard of proof will be met and what institution will provide it.

### 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, the challenges of effective attribution and persuasive communication identified by the RAND study. Efficacy and communication will be contingent on the breadth of participation of public and private entities and their willingness to be transparent with the evidence. As with any political challenge, obtaining 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 technical independence as described in the RAND study or 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. The consensus-based solution proposed in the Microsoft Digital Geneva Convention would undoubtedly face challenges.

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 [31] distributed across numerous national jurisdictions. The same strategy might help to supplement the capability of an attribution-based organization.

Finally, building this capability will require financial resources. Finding dedicated financial resources for a TAI would create its own set of challenges. Which country will agree to 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 was served well by including the private sector, but this thrust was undermined by the way it drew upon the model of the International Atomic Energy Agency. Was Microsoft proposing an independent, member state-funded international organization, like that of the IAEA? Or by empowering the "the private sector, academia and civil society," [32] was it suggesting a multi-stakeholder 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 cybersecurity firms has 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.

*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. [33] 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 existing international organizations. This might include exploring research questions like:

- How effective is attribution at initiating an international response?

- How do the public and state responses to an 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 gain momentum?

With a better understanding of the present state of attribution, we can better seek to define governance-based solutions. This paper has described several 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 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.

# 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-theissues/

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-coop-eration-cybersecurity-andadapting-cyber-norms.

Davis II, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M.S. (2017). *Stateless Attribu-tion*. 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-cyberpandemic.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" (Wash-ington, D.C.: Atlantic Council, November 2014), http://www.atlanticcouncil.org/images/publications/Confidence-Build-ing_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-gameattribution-net-work-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-withseeking-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, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advancecy-ber-norms/.

Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.

Security Intelligence, Defining APT Campaigns (2010) https://digitalforensics. sans.org/blog/2010/06/21/security-intelli-gence-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-reuseadvanced-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-operationstracker-q1-2018.

Toon, J. "$17 Million Contract Will Help Establish Science of Cyber Attribution," Georgia Tech Research, Horizons (blog), No-vember 29, 2016, http://www.rh.gatech.edu/news/584327/17-million-contract-will-help-establish-science-cyber-attribution.

Volz, D, & Sarah Young. 2018, "White House Blames Russia for 'reckless' NotPetya Cyber Attack." *Reuters*. https://www.reuters.com/article/us-britain-russia-cyber-usa/white-houseblames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ.

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

## NOTES

1. "Cyber Intrusion into U.S. Office of Personnel Management: In Brief" (Washington D.C.: Con-gressional Research Service, July 17, 2015), https://fas.org/sgp/crs/natsec/R44111.pdf.

2. Ibid.

3. Robert M. Lee. "The Problems with Seeking and Avoiding True Attribution to Cyber Attacks." *SANS DFIR* (blog), March 4, 2016.

4. Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 2, 2016).

5. Benjamin Wittes, "Mandiant Report on 'APT1,'" *Lawfare* (blog), February 20, 2013.

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

7. Security Intelligence, Defining APT Campaigns. SANS blog, June 21, 2010.

8. Adam Segal. "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat." *Council on Foreign Relations* (blog), June 19, 2018.

9. Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intru-sion Analysis," May 7, 2013, 61.

10. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015), 4–37.

11. *Ibid.*

12. Matt Burgess, "WikiLeaks Drops 'Grasshopper' Documents, Part Four of Its CIA Vault 7 Files," *Wired Magazine* (blog), May 7, 2017.

13. Michael Schmitt, & Liis Vihul. (2017). International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, retrieved August 17, 2018, https://www.justsecurity.org/42768/international-cyber-lawpoliticized-gges-fail-ure-advance-cyber-norms/.

14. Adam Segal and Alex Grigsby, "New Entries in the CFR Cyber Operations Tracker: Q1 2018," Council on Foreign Rela-tions, 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 be-tween these datasets, e.g., in what is considered a state-sponsored "incident", or an attribution to a specific perpetrator.

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

16. 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 indict-ment on hackers which took place through a grand jury process, see these documents.

17. 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.

18. Glenn S. Gerstell, "How We Need to Prepare for a Global Cyber Pandemic," NSA news release (April 9, 2018).

19. Paul Rosenzweig, "The NTSB as a Model for Cybersecurity," R Street Shorts (May 9, 2018).

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

21. Scott Charney, "Cybersecurity Norms for Nation-States and the Global ICT Industry," *Microsoft on the Issues* (blog), June 23, 2016.

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

23. John Davis et al., *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND Corporation, 2017), https://doi.org/10.7249/RR2081.

24. Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," *Council on Foreign Relations* (blog), February 23, 2018.

25. Scott Charney et al., "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms" (Microsoft Cor-poration, June 2016).

26. Healey, note 21 above.

## NOTES

27. Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms."

28. Davis et al., *Stateless Attribution.*

29. Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.

30. Volz, Dustin and Sarah Young. February 15, 2018. "White House Blames Russia for 'reckless' NotPetya Cyber Attack." *Reuters,* https://www.reuters.com/article/us-britain-russia-cyber-usa/white-house-blames-russia-forreckless-notpe-tya-cyber-attack-idUSKCN1FZ2UJ.

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

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

33. Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, at-tribution, 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.