Working Paper

Private Sector Attribution of Cyber Incidents

Benefits and Risks to the U.S. Government

Sasha Romanosky, Benjamin Boudreaux

National Security Research Division

WR-1267-OSD
February 2019

For more information on this publication, visit www.rand.org/pubs/working_papers/WR1267.html

Published by the RAND Corporation, Santa Monica, Calif.

Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government

DRAFT

Sasha Romanosky
sromanos@rand.org
RAND Corporation

Benjamin Boudreaux
bboudrea@rand.org
RAND Corporation

Abstract

Over the past decade, private sector cyber security companies have developed advanced capabilities that enable them to attribute malicious cyber activity to nation-states or state-sponsored actors. These capabilities may even rival those of some government intelligence agencies, and present new challenges because historically in the U.S. only the Federal government had the ability to link hostile actions with foreign actors. It is therefore unclear whether this growing trend of private sector attribution of cyber incidents represents a benefit or a liability for the U.S. Government (USG) and its cybersecurity and diplomatic efforts. In this Article, we address four related questions. First, what is the purpose of attribution, both for private sector companies, and the USG? Second, what benefits and risks does private sector attribution bring to the USG? Third, what are the relative capabilities of each stakeholder? And fourth, how should the USG collaborate with the private sector going forward? In order to answer these questions, we begin with a brief overview of cyber attribution. We then examine attribution reports from the private sector, the USG, and a dataset of publicly known state-sponsored cyber activity. Finally, we present the results of qualitative research in which we interviewed 15 senior subject matter experts from the intelligence community, law enforcement, the National Security Council staff, academics, and private sector threat intelligence companies. We conclude with insights from this analysis.

Keywords: cyber attribution, threat intelligence, APT, cyber attack, cyber incident, thematic saturation

Acknowledgements: We would like to thank Lilian Ablon, Sina Beaghley, Megan Doscher, Alex Grigsby, Jamil Jaffer, Martin Libicki, Mårten Mickos, Christopher Porter, Elizabeth Petrun Sayers, Christopher StMyers, Lori Uscher-Pines, Darius Wiles, and each of our anonymous participants for their comments and insights. We would also like to thank two anonymous colleagues who provided insights during the early stages of this project.

This research was sponsored by the Office of the Secretary of Defense and conducted within the Cyber and Intelligence Policy Center of the RAND National Defense Research Institute, a federally funded research and development center (FFRDC). The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Introduction

In a blog post in June 2016, the threat intelligence company CrowdStrike attributed the breach of the Democratic National Committee's (DNC's) networks to two groups of cyber actors closely linked to the Russian government.[1] The DNC had requested CrowdStrike's assistance and gave it permission to share the results of their attribution finding with the public. CrowdStrike explained that part of what motivated the publication of their finding was to "help protect even those who do not happen to be our customers" (Alperovitch, 2016).

Several months later in October, and a month before the US presidential election, the U.S. government (USG) made its own public attribution through a joint statement by the Department of Homeland Security (DHS) and the Director of National Intelligence (DNI). In this joint statement, the USG claimed that it was "confident" that the breach was directed by "senior most officials" of the Russian government.[2] Although the statement did not include any evidence or technical details, it was followed by a DHS/FBI Joint Analysis Report (JAR) called "GRIZZLYSTEPPE" that offered technical details about the malicious tools.[3] The GRIZZLYSTEPPE report, however, included a broad range of vague indicators, some not necessarily relevant to the DNC hack, and was widely criticized by the information security community as "sowing confusion about the hackers' identities."[4] In January 2017 in the waning days of the Obama administration, the U.S. government intelligence community released a coordinated report that situated the DNC breach as part of a broader Russian disinformation campaign.

In Congressional hearings, senior USG leaders were asked in detail about the methods they employed to arrive at their attribution. In response, former FBI director James Comey noted they could not offer details without revealing sensitive sources and methods, but explained that the FBI experts analyzed the forensic and other technical details provided by CrowdStrike ("we got the forensics from the pros that they hired").[5] Former DHS Secretary Johnson added that "the DNC did not feel it needed DHS' assistance at that time…they don't want our help, they have CrowdStrike."[6]

This case depicts a variety of dynamics emerging from the growth of private sector firms that attribute malicious cyber incidents to nation state actors, and how these capabilities interact with USG activities and interests. First, it speaks to the motivations behind publicly attributing a cyber incident, both for private companies, as well as the USG. For example, CrowdStrike's attribution may have been intended to help other potential victims, but it also generated extensive media attention that raised CrowdStrike's public profile in a growing cyber threat marketplace. On the other hand, the USG must balance a range of interests in its public attribution, including its responsibilities for domestic cybersecurity, intelligence collection, deterrence in cyberspace, and an effective foreign policy. Second, attribution of the DNC breach demonstrates that there are opportunities for the USG to leverage private sector capabilities, but also that there are risks with the government now not always having a preeminent role in this space. For

[1] As CrowdStrike noted, "on rare occasions, a customer decides to go public with information about their incident and give us permission to share our knowledge of the adversary tradecraft with the broader community" (Alperovitch, 2016).
[2] See https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national. Last accessed July 26, 2018.
[3] See https://www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity. Last accessed July 26, 2018.
[4] See https://www.cyberscoop.com/dhs-election-hacking-grizzly-steppe-iocs/. Last accessed July 26, 2018.
[5] See http://transcripts.cnn.com/TRANSCRIPTS/1703/20/cnr.07.html. Last accessed July 26, 2018.
[6] See https://www.politico.com/story/2017/06/21/dnc-no-help-homeland-security-hacks-239800. Last accessed July 26, 2018.

example, CrowdStrike had the capabilities to disclose the breach months before the USG, and its attribution might have pressured the USG to offer its own attribution or otherwise respond to the Russians responsible. Third, in part because of its extensive cyber forensics capabilities and direct access to the victim's network, a high-profile victim of a major nation-state actor (the DNC) relied on the capabilities of a private firm for assistance rather than the Federal government. This raises the question of who may have better capabilities and under which conditions be able to collect information and associate an incident with an attacker. Fourth, perhaps in part because of the close connections between the FBI and CrowdStrike (the President of CrowdStrike is a former senior FBI official), the two entities participated in a valuable and growing form of public-private cooperation through CrowdStrike's sharing of forensic analysis.[7]

Each of those four points, we argue, present emerging tensions, but also opportunities for the USG as it seeks to navigate and further understand its role, and the role of the private sector in cyberspace. Therefore, in this Article, we seek to answer the following four questions:

1. What is the purpose of attributing a cyber incident to a nation-state, or nation-sponsored individual or entity, both for private sector and the USG?
2. What are the risks and benefits of private sector attribution of cyber incidents for the USG and its agencies, such as the intelligence community and law enforcement?
3. What are the relative capabilities for reaching high confidence attributions between private companies and the USG?
4. What opportunities exist for collaboration between these groups going forward?

While this discussion is presented in the context of the USG (including law enforcement, the intelligence community, network defense entities, and foreign policy community) we want to stress how the issues raised are likely to impact the governments of *any* country that confronts malicious cyber activity.

We begin by providing an overall context for attribution and describe generally what is cyber attribution. We then examine the stakeholders that are making attribution claims, and we perform analysis of a dataset of publicly known state-sponsored cyber activity. Finally, we present the results of qualitative research in which we interviewed 15 subject matter experts from the intelligence community, law enforcement, the National Security Council staff, academics, and private sector threat intelligence companies. We conclude with insights from this analysis.

What is Attribution of Cyber Incidents?

Cyber attribution is the process by which evidence of a malicious cyber activity is collected, analyzed, and associated to an originating party (i.e. the attacker).[8] Since the first rigorous threat intelligence report in 2013 which sought to attribute a collection of cyber intrusions of U.S. companies to the Chinese military, there has been a growing body of literature concerning the technical challenges of attributing a cyber incident to an individual or government entity (Rid and Buchanan, 2015; Lin, 2016). In addition, other scholarship has addressed particular strategic, legal and ethical issues that arise when entities seek to attribute cyber events (Anderson, 2018; Eichensehr, 2017; Guerrero-Saade, 2015; Edwards et al 2017). The current state of affairs is complicated enough that there have even been numerous proposals to

[7] See https://www.crowdstrike.com/shawn-henry/. Last accessed July 24, 2018.
[8] By "malicious cyber activity" (or simply "cyber incident") we consider any computer-enabled malicious activities, intended to compromise the confidentiality, integrity, or availability of computing devices. This includes espionage operations.

standardize attribution reports or even create new international or private-sector led organizations whose mission is to attribute malicious cyber activity (Davis et al, 2017; Microsoft's Cyber IAEA[9]; Atlantic Council Attribution Council[10]). Others have also developed analytic models to help frame attribution procedures. For instance, the Diamond Model uses graph theory to formally characterize the distinct components of a cyber incident, and track any developments of those characteristics over time (Caltagirone, 2013), while the Q model takes a conceptual and strategic approach to help analysts better understand intrusion activity (Rid, 2015). Lin (2017) distinguishes between three types of attribution, each requiring increasing forms and degrees of evidence: attribution to the machine, to the human, and to the party.

For the purpose of this Article, however, we consider two main types of attribution: technical and political as shown in Figure 1. *Technical attribution* is the act of associating software, computer, or networking artifacts with a cyber incident. The body of evidence collected for technical attribution may include computer log entries, network traffic, malicious software (malware), file timestamps, or other modifications to computing hardware or software.

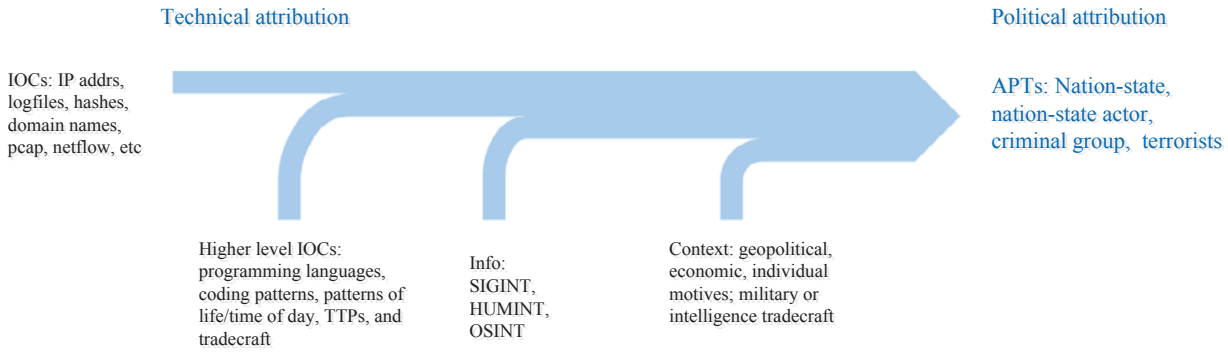


Figure 1: Attribution diagram[11]

Additional evidence that can be brought to bear may include all-source intelligence which can include signals intelligence (SIGINT) intercepted communications, and human intelligence (HUMINT) from well-positioned human sources. In general, advanced SIGINT and HUMINT were historically only available to highly-sophisticated nation-states, however, threat intelligence companies (and other non-governmental organizations) are now developing their own capabilities that may rival nation-states capabilities (Weinbaum et al, 2017). Open source intelligence (OSINT) based on publicly available information may also help in attribution. This type of evidence is available for all stakeholders and includes activities such as surfing Darknet sites, leveraging publicly available websites, blogs, document repositories, and otherwise studying the behavior and tactics of cyber threat actors. Together, these additional sources help achieve higher levels of attribution confidence.

---

[9] See https://blogs.microsoft.com/eupolicy/2016/07/08/the-role-of-cybernorms-in-preventing-digital-warfare/. Last accessed July 26, 2018.

[10] See http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf. Last accessed July 26, 2018.

[11] This Sankey flow diagram is a notional description of how pieces of information are combined to create various forms of attribution. We recognize that these information types are not exhaustive, nor always available during attribution. Further, the arrows suggest a strictly linear progression toward political attribution, which we recognize is not always the case.

The most challenging type of attribution, *political attribution,* requires understanding the geo-political context and motives of potential attackers, such as information about the threat group's governance, financial or reputational gains. Together, this information is incorporated in order to associate an incident or campaign to the particular threat actor - commonly referred to as an advanced persistent threat (APT) - responsible for tasking, directing, or controlling the operation.[12]

Unsurprisingly though, attribution is rarely a straightforward exercise. An investigator will likely not have all the necessary information, and even if she does, the evidence may be misleading. Technical indicators can be re-used, marred by incomplete data, false flag and deception trickery, and forensic difficulties (Porter, 2016; Bishop et al 2009; Bartholomew and Andres Guerrero-Saade, 2016).[13] All-source intelligence may not be available or may provide conflicting evidence. Political attribution is also difficult since political motives are not always clear and can be purposely obscured to create confusion.[14] For example, states regularly use proxy and non-government actors to conduct cyber operations, with these actors being directed, controlled, and monitored by official state authorities to varying degrees (Healey, 2011; Maurer, 2018). The relevant government might be aware of these operations and thus might bear some legal or other responsibility to prevent them, but might also be able to create sufficient distance to muddy a judgment.[15] Indeed, states might even benefit from the plausible deniability that these dynamics create—see e.g. Russian denials that they were responsible for the 2007 Estonian DDoS claiming that these were patriotic hackers rather than officials acting on behalf of the Russian government. Lastly, political attribution might not ever be reached with analysis of a single incident, and instead might require analyzing an incident in relation to other incidents leveraging similar tactics, techniques and practices (TTPs).

What is Known About Publicly Attributed Cyber Incidents?

We now seek to understand and characterize the types of attribution statements and reports that have been made about malicious cyber activity. In short, we address the questions: what does cyber attribution look like, and who is making it?

We address these questions by examining three datasets of attribution information from the private sector, the USG, and an independently curated source of state-sponsored cyber incidents. As discussed below, the unit of "attribution" can differ across each of these datasets. For the private sector, attribution reports may identify a piece of malware, or cyber incident(s), which may or may not be connected to a threat group (an APT). On the other hand, attribution statements from the USG attribute states or individuals (in the case of indictments) to specific incidents against the U.S., while the third dataset seeks to associate *all* known state-sponsored cyber incidents.

---

[12] While many definitions may exist, we consider an APT to refer to a sophisticated cyber actor who invests extensive resources (time, attention, toolsets, infrastructure) to conduct malicious cyber operations. An APT may or may not be under the direct control of a nation-state.

[13] As in the case of multiple attackers allegedly behind the Sony data breach, "South Korea alternately blamed North Korea for the attack as well as China—since an IP address in China appeared to be part of the campaign. Officials later retracted the allegations", https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/. See also http://deadline.com/2014/12/is-the-chinese-armys-cyber-squad-behind-the-sony-attack-1201325918/. There are a myriad of other examples of malicious actors using attack infrastructure, code, or techniques used by other attackers with the intention of confounding attribution. Documents last accessed July 24, 2018.

[14] An example of this is the Cyber Caliphate incident against TV5Monde that was originally attributed to the Islamic State, but was later determined to be Russian.

[15] See Tallinn Manual 2.0 discussion of legal responsibility of states for cyber actions emanating from their territory.

Attribution by the Private Sector

In the discussion below we examine threat reports from 5 of the leading threat intelligence companies. While there are many other very capable firms that track and report privately on APT groups, we limit our analysis to those firms that are most vocal in producing *publicly available* attribution reports, namely, (listed in alphabetical order): Cisco, CrowdStrike, Dell SecureWorks, Fireye, and Kaspersky.

The "Thing" Being Attributed

Part of the reason attribution is confusing is that companies attribute incidents to different things. In some cases, the "thing" being attributed is malware (as in the case of trojans,[16] remote access tools[17] or exploits[18]), or a particular attack (as in the case of botnet attacks or ransomware[19]), or *campaigns* of related attacks (as with a number of identified North Korean incidents by Group 123).[20] Or it could be a nation state, a state-sponsored entity, or a criminal group.[21] For the purpose of this Article, however, it is the latter group of threat actors (states, state-sponsored entities, and criminal groups), collectively referred to as APTs, with which we are mainly concerned.[22]

These APTs are differentiated from historic and simpler actors or attacks that may simply deface or DDoS a website, or crash a networking device. Instead, APTs are generally characterized by being deliberate in their choice of victims, using custom-built malware which may exploit zero-day vulnerabilities, operate slowly and deliberately over months or years, and are able to adapt to an organization's network defense and hunt teams (FireEye, 2018b). Specifically, FireEye defines APTs as, "distinct set of cyber tools, techniques, and procedures (TTPs) that are employed directly or indirectly by a nation-state or a sophisticated, professional criminal organization for cyber espionage or the long-term subversion of adversary networks."[23] Similarly, Kaspersky defines them as, "concerted, stealthy, ongoing attacks against specific organisations — in contrast to speculative, isolated, opportunistic incidents that make up the bulk of cybercriminal activity."[24]

As described above, the general practice is to associate APTs to specific countries or state-sponsored groups (in addition to terrorist and criminal groups). For example, CrowdStrike takes a very adversary-based approach to attribution, stating that their, "primary focus is to track adversaries associated with

---

[16] See p45, https://www.accenture.com/t20170928T145132Z__w__/hk-en/_acnmedia/PDF-61/Accenture-Cyber-Threat-Scape-Report.pdf. Last accessed July 13, 2018.
[17] See https://www.crowdstrike.com/blog/adwind-rat-rebranding/ or https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html. Last accessed July 12, 2018.
[18] See https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/. Last accessed July 12, 2018.
[19] See https://www.crowdstrike.com/blog/gameover/. Last accessed July 12, 2018.
[20] See https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html. Last accessed July 13, 2018.
[21] Or sometimes Kaspersky Labs uses a name to refer to both an APT and a Trojan, as in the case of BLACKENERGY, https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/, or an APT and backdoor, https://securelist.com/minidionis-one-more-apt-with-a-usage-of-cloud-drives/71443/. Last accessed July 13, 2018.
[22] See also Florian Roth's comments at https://medium.com/@cyb3rops/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263 who describes these problems with naming conventions. Last accessed July 17, 2018.
[23] See http://www2.fireeye.com/rs/848-DID-242/images/fe-rpt-regional-atr-emea.pdf. Last accessed July 13, 2018.
[24] See https://securelist.com/threats/apt-advanced-persistent-threats-glossary/?utm_source=securelist&utm_medium=blog&utm_campaign=termin-explanation. Last accessed July 13, 2018.

nation-state actors and monitor their activity,"[25] and when naming threat groups, the intention is that the name, "designates both the adversary's nation-state and the group they targeted."[26]

Further, some companies seek to publicly call out specific individuals who allegedly carried out the cyber incident (i.e. Lin's (2007) *attribution to the person*). For example, FireEye's Mandiant began this trend with its APT1 report describing Chinese exfiltration of corporate information from the U.S where it used a number of techniques to connect cyber activity with individual(s) from the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, or Unit 61398 (Mandiant, 2013). Not to be outdone, CrowdStrike sought to connect the individual 'cpyy' of PUTTER PANDA to 12th Bureau of the 3rd Department of the GSD through "unintentional backgrounds in images of his dormitory and images of his office."[27]

On the other hand, Cylance specifically does not focus on disclosing information about the humans conducting a cyber incident. As they state in Operation Cleaver, "all personally identifiable information about the members of Operation Cleaver has been withheld. We don't care who the adversary is, where they work or reside, who they're dating or what party photos they upload to Facebook – all we care about is preventing campaigns like Operation Cleaver from negatively affecting the real world" (Cylance, 2014).

Kaspersky very deliberately does not attribute those APT groups to any particular state actor or criminal group because of the potential for false or misleading indicators.[28] However, they may sometimes refer to APT names used by other companies, which have been associated to nation-states.

How Many Named APTs Are There?

It is difficult to know with much precision how many APT groups any given private company is tracking and *when* they were formally named. For example, even though FireEye claims to track thousands of threat actors (FireEye, 2018b), not all reports are available to the public, and even when they are - in our experience - company websites make it difficult to locate the reports.

Based on publicly available information from company websites and reports, as well as additional opensource information, we can begin to estimate the number of named APT groups from these most vocal companies. While we have tried to be complete in our analysis, the numbers provided below are estimates and subject to measurement error for many of the reasons previously discussed. It is *not* our intention to suggest that the total number of named APTs is a measure of capability, either by the company, or the threat actors. We merely present the numbers below in order to provide the reader with an understanding of the scope and scale of APT naming by the private sector, as compared with the USG (discussed in a later section).

[25] See https://www.crowdstrike.com/blog/whois-anchor-panda/. Last accessed July 11, 2018.
[26] *Id.*
[27] See https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/. Last accessed July 12, 2018.
[28] See video https://www.kaspersky.com/blog/attribution-not-easy/6348/, at min 3:45 for an explanation of their approach. Last accessed July 25, 2018.

We find that FireEye has publicly attributed approximately 47 APT groups,[29] 36 of which are nation-state actors, and 10 financially motivated (FIN) threat actors. [30] Of those nation-state groups, about 20 are suspected to be from China, with others suspected to be from Russia (i.e. APT28, APT29), Iran (i.e. APT33, APT34, APT35), Korea/DPRK (i.e. APT37), and other undisclosed or unknown countries or affiliations. A summary of these results are shown in Table 1.

Table 1: Named APTs[31]

Country	FireEye	CrowdStrike	Kaspersky[32]	Dell SecureWorks	Cisco Talos
China	20	40	N/A	5	9
Russia	3	3	N/A	6	3
Iran	3	7	N/A	1	3
North Korea	1	4	N/A	2	2
Criminal / Terrorist	10	29	N/A	3	1
Other	2	1	N/A	2	-
Unknown/Undisclosed	8	1	N/A	-	1
Total	47	85	36	19	19

CrowdStrike is much more prolific with regard to naming, citing at least 85 threat groups. For example, it has publicly attributed almost 40 Chinese-based APT groups alone, with at least an additional 3 from Russia, 7 from Iran, 4 from North Korea, and many more from other countries or criminal groups.[33]

Kaspersky has also publicly named almost 40 unique APT groups.[34] Note that while they maintain a webpage listing many more threats,[35] some of these relate to specific malware or attacks (e.g. Stuxnet, Blue Termite), while others do refer to APT groups (e.g. EQUATION GROUP).

Finally, Dell SecureWorks and Cisco Talos are less prolific in their attributions, with 19 each.

Again, these numbers are not meant to reflect relative capabilities of these companies, because there are many reasons why a firm may or may not track and/or name a given threat group either publicly or privately. Instead, these results are only meant to provide one perspective regarding the volume of APTs that are publicly named by private sector threat intelligence firms.

[29] Based on https://www.fireeye.com/current-threats/apt-groups.html, the company's blog posts, as well as http://apt.threattracking.com. Last accessed July 10, 2018. But again, we recognize that they track many more groups, campaigns, and activities not publicly disclosed.
[30] See https://www.sita.aero/globalassets/microsites/atis-apac-2018/the-dynamic-threat-landscape-in-the-aviation-sector-rob-van-der-ende.pdf, which claims that they track 10 financial threat groups. Last accessed July 18, 2018.
[31] Links to all sources are available from the authors upon request.
[32] See discussion above of why Kaspersky does not directly attribute to particular nation states or criminal groups.
[33] Based on company blog posts, http://www.crowdstrike.com/blog/, http://apt.threattracking.com, and the (admittedly dated) info graphic available at https://www.crowdstrike.com/blog/meet-the-adversaries/. Last accessed July 13, 2018.
[34] Based on searching all blog posts on https://securelist.com/ under the filter of "APT Reports" back to 2003.
[35] See https://apt.securelist.com/#!/threats. Last accessed July 19, 2018.

Naming Conventions

Attribution is also muddled because each company uses different naming conventions and often there are multiple names given to the same (suspected) threat groups. For example, FireEye takes a pragmatic approach to naming by appending an integer to the string, "APT" as shown in Figure 2.

Figure 2: FireEye APT naming[36]

On the other hand, CrowdStrike has adopted animal monikers for its APT naming convention as shown in Figure 3, where PANDA adversaries refer to Chinese threat actors, BEARS refer to Russia, KITTENS to Iran, TIGERS to India, CHOLLIMAs to North Korea, JACKALS to terrorist groups, and SPIDERS to criminal groups.

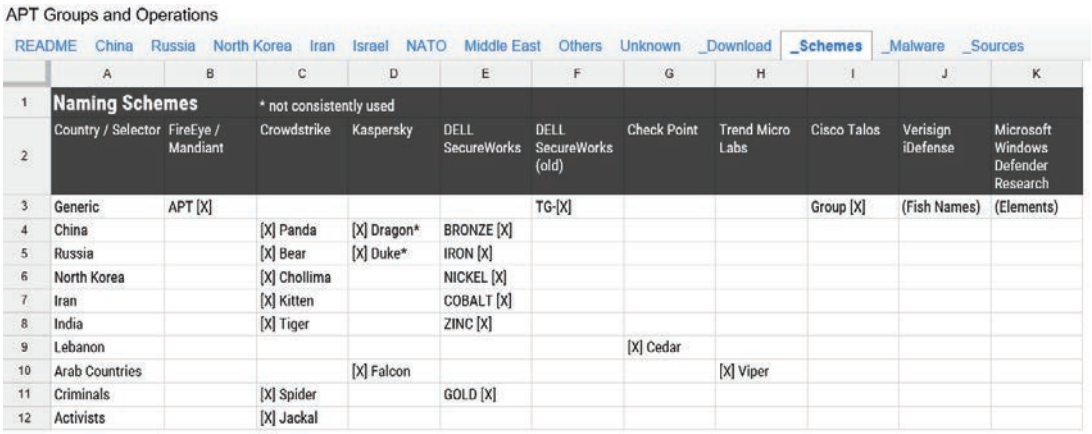
Figure 3: CrowdStrike APT naming[37]

Cisco Talos, on the other hand, uses "Group" followed by an integer number for their APT naming convention, and uses common nouns when naming criminal campaigns, as with COINHOARDER.[38] Dell SecureWorks uses metals (Gold, Bronze, Iron, Zinc, Nickel, Cobalt).[39] And finally, while reports are not

[36] Source, FireEye.
[37] Source https://www.crowdstrike.com/blog/meet-the-adversaries/. Last accessed July 12, 2018.
[38] See https://blog.talosintelligence.com/2018/02/coinhoarder.html#more. Last accessed July 13, 2018.
[39] Though, historically, they used the "TG" or Threat Group naming convention.

publicly available, Accenture iDefense uses fish-themed names such as, SNAKEMACKEREL, JACKMACKEREL, and SANDFISH (Accenture, 2017).

To our knowledge, there is no authoritative list of named APTs by all companies. However, the most comprehensive lists are available at MITRE's Advanced Tactics, Techniques and Common Knowledge (ATT&CK),[40] and the crowdsourced compilation curated by Florian Roth (@cyb3rops)[41] who provides the table as shown in Figure 4.[42]



APT Groups and Operations

README | China | Russia | North Korea | Iran | Israel | NATO | Middle East | Others | Unknown | _Download | _Schemes | _Malware | _Sources

	A	B	C	D	E	F	G	H	I	J	K
1	**Naming Schemes**		* not consistently used								
2	Country / Selector	FireEye / Mandiant	Crowdstrike	Kaspersky	DELL SecureWorks	DELL SecureWorks (old)	Check Point	Trend Micro Labs	Cisco Talos	Verisign iDefense	Microsoft Windows Defender Research
3	Generic	APT [X]				TG-[X]			Group [X]	(Fish Names)	(Elements)
4	China		[X] Panda	[X] Dragon*	BRONZE [X]						
5	Russia		[X] Bear	[X] Duke*	IRON [X]						
6	North Korea		[X] Chollima		NICKEL [X]						
7	Iran		[X] Kitten		COBALT [X]						
8	India		[X] Tiger		ZINC [X]						
9	Lebanon						[X] Cedar				
10	Arab Countries			[X] Falcon				[X] Viper			
11	Criminals		[X] Spider		GOLD [X]						
12	Activists		[X] Jackal								

Figure 4: APT naming conventions[43]

Another reason that attribution is messy is that the same threat actor can be known by multiple names across threat intelligence companies. For example, APT28 (FireEye) is also known as FANCY BEAR (CrowdStrike), TG-4127 (Dell SecureWorks), and Group 74 (Cisco Talos). CHARMING KITTEN (Crowstrike) is also known as APT33 (FireEye) and Group 83 (Cisco Talos). GOTHIC PANDA (CrowdStrike) is also known as TG-0110 (Dell SecureWorks), APT3 (FireEye), BUCKEYE (Symantec), and Group 6 (Cisco Talos), while other APTs may go by as many as 10 different names.

Threat Reports

Generally speaking, the threat reports by the private companies we examined include a number of important sections. First, they identify the named APT group, its motives, and details concerning known targets. For example, the APT37 article from FireEye mentions that this group is a "suspected North Korean cyber espionage group" whose "primary mission is covert intelligence gathering in support of North Korea's strategic military, political and economic interests," and that it has targeted "South Korean government, military, defense industrial base, and media sector." (FireEye, 2018). Similarly, FireEye describes APT28 (aka FANCY BEAR) as a "suspected Russian government-sponsored espionage actor" that has conducted operations "in support of Russian strategic interests" by targeting "entities in the U.S., Europe and countries in the former Soviet Union, including government and militaries, defense attaches[sic], media entities and dissidents and figures opposed to the current Russian Government." (FireEye, 2017)

[40] See https://attack.mitre.org/wiki/Groups. Last accessed July 18, 2018.
[41] See http://apt.threattracking.com. Last accessed July 18, 2018.
[42] Note that all information is compiled from public sources, and may omit proprietary information that may be more complete and/or accurate.
[43] Source, http://apt.threattracking.com. Last accessed July 17, 2018.

In addition, the reports provide information about known attack vectors, command and control structures, and specific vulnerabilities or custom malware used or developed during exploit. For example, reports may cite phishing (or spear-phishing) campaigns that leverage zero-day vulnerabilities launched from compromised servers, whose purpose is to infiltrate an organization and exfiltrate corporate documents (see APT28, APT37).

Timelines of observed activity are also often carefully documented in many reports. For example, Dell SecureWorks captured the time of day events of BRONZE UNION (aka TG-3390) infiltrating a victim, as shown in the top and bottom panels in Figure 5.

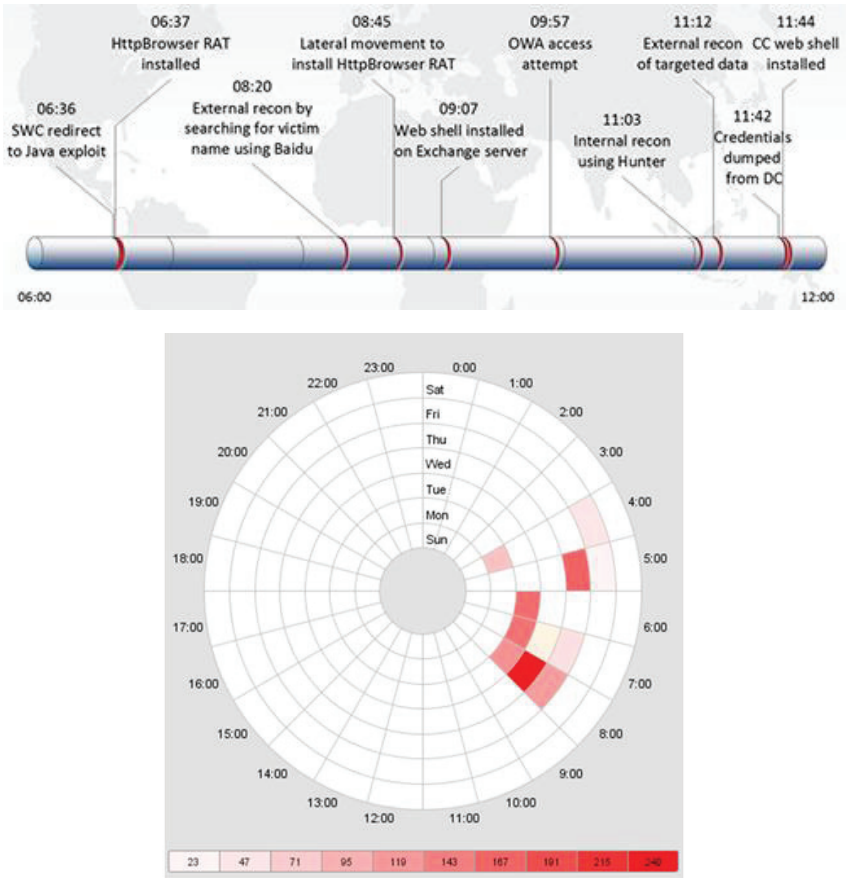


Figure 5: Timeline of BRONZE UNION activity[44]

Note: The top panel shows times stamps for a single infiltration, while the bottom panel depicts intensity of malicious activity according to time of day (as measured along a 24 hr clock), day of week (inner to outer circle), and intensity increasing in color depth.

Finally, some reports provide a level of confidence and justification for attributing particular incidents to a threat group. For example, FireEye asserts that "we assess with high confidence that APT37 acts in support of the North Korean government" which they base on "targeting profile," "malware development," and "probable links to a North Korean individual believed to be the developer" (FireEye,

[44] Source, https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage. Last accessed July 18, 2018.

2018). Similarly, CrowdStrike bases attribution, in part, on patterns of life, stating that, "[t]hese actors are rational and generally predictable…They tend to work normal business hours in their local time zone with few exceptions, and they don't typically work on weekends."[45] Kaspersky writes in one report, "Due to tools and tactics in use we attribute the campaign to LuckyMouse Chinese-speaking actor (also known as EmissaryPanda and APT27). The tools found in this campaign…are regularly used by a variety of Chinese-speaking actors. …Due to LuckyMouse's ongoing waterholing of government websites and the corresponding dates, we suspect that one of the aims of this campaign is to access web pages via the data center and inject JavaScripts into them."[46]

More information about threat reports for FireEye, CrowdStrike, Cisco Talos, Kaspersky, and Dell SecureWorks is provided in the Appendix.

Next we compare cyber attribution by the USG.

Attribution by the USG

In the U.S. context, the 2016 Presidential Policy Directive 41 "United States Cyber Incident Coordination" designates the FBI as the lead to conduct 'threat response' activities including providing attribution.[47] ODNI, through the Cyber Threat Intelligence Integration Center (CTIIC) and with analysis provided by the full intelligence community, is the lead on providing intelligence support. Other agencies, especially DHS, might also provide evidence or analysis that assists the USG in reaching attribution. In addition, the U.S. Treasury Department through the Office of Foreign Assets Control (OFAC) has authority to attribute and sanction an entity for malicious cyber activity as part of Executive Order 13694.[48] Attribution findings might be reached at various degrees of analytic confidence based on the type, extent, and significance of available evidence.[49] The United States' different bodies might not assess evidence the same way, and might disagree about attribution or confidence standards.

Once an attribution is reached, there is a secondary policy question of whether to publicly disclose the finding, and if so, in what form. In many cases, there have been leaks from USG officials, statements from Congress, or other press reports that an attribution finding has been internally reached, even though the USG has not offered an official public statement. In the relatively rare cases where the government makes a public attribution, these have come in a variety of forms: high level public statements, technical releases, intelligence assessments, and criminal indictments.

It should be noted that we do not assume that attribution by the USG (or any federal government, for that matter) is a perfectly calculated action with complete agreement by federal components and agencies. Indeed, conversations with former officials suggest that decisions to publicly attribute are fraught with political tensions and internal debates.

To date, there have been only a handful of official USG statements (16, by our count) identifying actors affiliated with nation-states for their cyber activity targeting U.S. persons or business, as shown in Figure 6. An accompanying table with citations is available in the Appendix.

---

[45] See https://www.crowdstrike.com/blog/peering-around-corner/. Last accessed July 12, 2018.
[46] See https://securelist.com/luckymouse-hits-national-data-center/86083/. Last accessed July 13, 2018.
[47] See https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. Last accessed July 24, 2018.
[48] See https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities. Last accessed July 28,2018.
[49] For more on analytic standards, see ODNI Intelligence Community Directive 203.

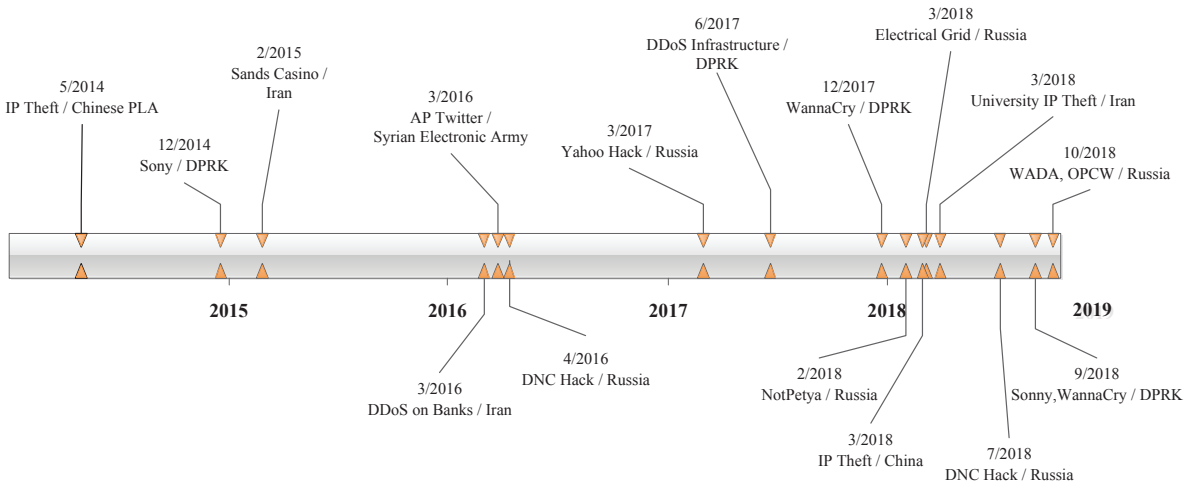


Figure 6: Timeline of USG attribution of cyber incidents

These data suggest that the frequency of public attribution by the USG is increasing in time. However, the USG has not taken a standardized approach to attribution—either in the timing of attribution, the mode, the type or extent of evidence supporting the attribution, the confidence level, or whether attribution is followed by other punitive measures. For example, the 2017 attribution of WannaCry and the 2018 attribution of NotPetya involved coordinated statements with international partners, however, those appear to be the sole cases of international collaboration.

Further, a number of the attribution statements explicitly reference the work of the private sector in supporting the attribution. For instance, the June 2017 DHS Technical Alert attributing DPRK's DDoS Botnet Infrastructure references the work of private sector companies IBM, Symantec, Novetta among others. In fact, for incidents involving private sector companies (for which the USG has no immediate visibility), it may likely *require* collaboration and information from the private sector in order to produce an attribution statement (we discuss collaboration in detail below).

Statements by the USG focus on the behaviors of the nation-states or offending individuals and incidents, rather than creating crafty naming schemes of APTs. For example, the documents from the Department of Justice (complaints and indictments) include extremely detailed information about the defendants and their affiliation (employment), a complete history of the defendants' TTPs, the outcome of their cyber activity, and the alleged criminal violations. For example, in the case of the indictment against 7 Iranians for committing DDoS attacks against companies in the U.S. from 2011-2013, the indictment includes two counts of conspiracy to commit computer hacking, and one count of unauthorized access to a protected computer.[50]

The attribution reports from US-CERT, on the other hand, refer to specific incidents, such as ransomware, or attacks against critical infrastructure (see Appendix), and therefore don't require attribution. The reports may include much of the same information as any private sector threat report, by including indicators of compromise (IOCs), TTPs, as well as any information US-CERT has regarding impact, and remediation measures. For example, recommendations from US-CERT for avoiding harm from the

[50] See https://www.justice.gov/usao-sdny/file/835061/download. Last accessed August 7, 2018.

WananCry ransomware attack include applying appropriate patches, ensuring anti-virus software is up to date and functioning properly, and testing one's backups.[51]

Now, to be clear, the variation in reporting style and content can largely be explained by the mission of the attributing agency. While the private sector may be thought of as a singular entity with similar interests, USG agency attribution is related to the purpose of the attributing agency.

Nation-State Attribution Data

While there are many reports describing individual attribution notices,[52] the most complete dataset of nation state incidents comes from the Council on Foreign Relations (CFR) which has collected a sample of over 220 observations of "publicly known state-sponsored incidents."[53] Note that the CFR dataset only contains observations, "in which the perpetrator…is suspected to be affiliated with a nation-state. The tracker focuses on state-sponsored actors because its purpose is to identify when states and their proxies conduct cyber operations in pursuit of their foreign policy interests."[54]

As shown in the left panel of Figure 7, the number of incidents has been increasing steadily since 2005. One explanation for the dramatic increase is the growing ubiquity, complexity and opportunities that have arisen because of adoption of electronic devices and opportunities to exploit them. Another possible explanation is that it has become easier to detect these events. We are unable to separately distinguish the two factors because while it is certainly the case that attacker capabilities have increased over the past decade, so too have defender capabilities.

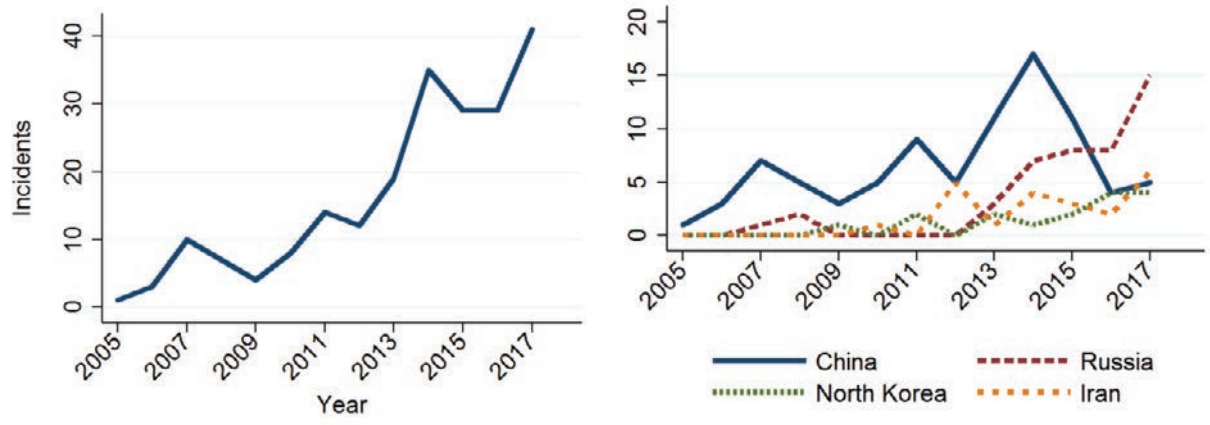


Figure 7: Cyber Incidents over Time (n=224), and Top Nation-States (n=177)

The right panel of Figure 7 shows the countries to which cyber incidents are most commonly attributed in the CFR dataset: China(86), Russia (50), North Korea (18) and Iran (23). These data show that while China has been most commonly attributed, Russia has seen the largest increase in incident attribution over the past 5 years. The sharp decline involving reported Chinese espionage activity is likely a result of the

[51] See https://www.us-cert.gov/ncas/alerts/TA17-132A. Last accessed August 7, 2018.
[52] For example, one report documents an impressive number of rapid efforts concerning attribution and sanctioning by the US government, https://www.endgame.com/blog/technical-blog/indictments-sanctions-and-broken-promises-two-active-weeks-us-cyber-policy. See also https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf for a summary of trends observed in 2017.
[53] See https://www.cfr.org/interactive/cyber-operations. Last accessed July 26, 2018.
[54] *Id.*

Obama-Xi agreement in which both countries agreed to stop conducting or supporting cyber-enabled theft of intellectual property."[55] On the other hand, the steady rise of Russian activity is consistent with reports of Russia's growing ability, and interest, to use cyber capabilities as a foreign policy tool.[56]

On the other hand, Figure 8 (left panel) shows the impact (outcome) of the events, and illustrates how the bulk of attribution has been against espionage activity, which is most often attributed to China and Russia (right panel).

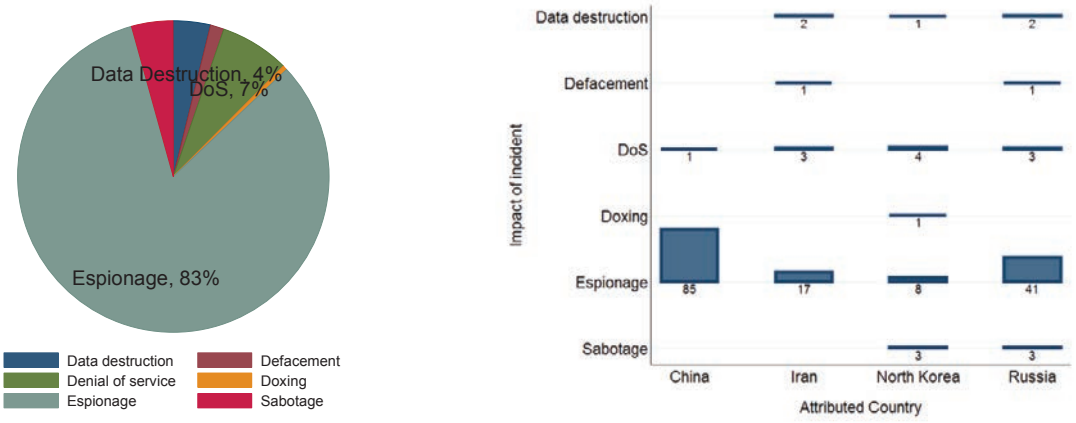


Figure 8: Impact of Incidents (n=208), by attributed country (n=177)

These results suggest that while China engages in predominantly espionage, North Korea and Russia engage in almost all forms of malicious cyber activity (of the forms recorded by this dataset). Note that this dataset also contains information about cyber incidents attributed to the U.S., which we discuss more in detail later in this Article.

Now that we have highlighted some of the complexities and tensions associated with attribution, and described the landscape of publicly available attribution reports, we next present results from interviewing cyber attribution experts.

Expert Interviews

In order to better understand the significance that the growing capability of private sector attribution may have for the USG, we performed qualitative research by interviewing 15 senior subject matter experts to explore 4 main topics:

1) **The purpose of attribution**. What are the motivations, reasons, and value of private sector, and government stakeholders attributing a cyber incident to a nation state or other threat actor?

2) **The risks and benefits** of private sector attribution of cyber incidents for the USG (including IC and LE), i.e. does attribution by the private sector pose any risks to the USG (such as forcing it to act prematurely), or does it present any benefits (such as helping provide an unclassified vehicle for discussions)?

[55] See https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later. Last accessed August 7, 2018.
[56] See https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111. Last accessed August 7, 2018.

3) **A comparison of capabilities** between private sector companies and USG government agencies, i.e. which group has better or different capabilities for information visibility, acquisition, and analysis, relative to the other?

4) **Opportunities for collaboration** between the USG and private sector. Given that these groups now exist in this ecosystem, what sort of collaboration makes sense going forward?

Formally, we performed thematic analysis based on semi-structured interviews in order to identify the strongest and most common themes that emerged from the interviews (Braun and Clarke, 2006; Glaser and Strauss, 1967). The purpose of thematic analysis is to achieve thematic saturation – the point at which collecting additional data reveal no new insights. In order to achieve saturation, we employed non-probabilistic, purposive sampling (Guest et al, 2006) using a convenience sample of individuals known to the Authors, as well as the chain sampling approach (Goodman, 1961) where we solicited additional candidates from the participants, as well as other colleagues. Our selection criteria for participants was based on domain expertise (e.g. cyber threat intelligence, cyber policy, or cyber law), and stakeholder organization (intelligence community, law enforcement, academic/think tank, or private sector threat intelligence company). In many cases, individuals had experience across multiple organizations, for example many private sector participants were former FBI, or IC employees. All participants were senior career technology, government, or policy professionals, as shown in Table 2.

Table 2: Participant expertise

Participant	Expertise		
	U.S. Govt[57]	Private sector[58]	Academic / Non profit
#1			x
#2	x		
#3	x		
#4	x		
#5	x		
#6	x	x	
#7	x	x	
#8	x		x
#9	x	x	
#10	x		
#11	x		x
#12	x		
#13			x
#14	x	x	
#15		x	

In total, we interviewed 15 participants from March through June 2018 and sent emails to 9 additional people, producing an overall response rate of 63% (15/24). Interviews were typically conducted on the phone by both authors of this Article, though two interviews were conducted by the principal investigator in a classified space.[59] Interviews were scheduled for 1 hour, but typically ran longer. Participants were

[57] This includes law enforcement, those working in the intelligence community, National Security Council staff, and other senior government policy roles.
[58] Includes either threat intelligence companies, or private security consulting companies.
[59] No classified notes were taken, nor does this Article contain any classified material.

not compensated financially for their participation, and no personally identifiable information was collected during the course of the interviews. Participation was voluntary, and the interviews were not recorded.

Research notes were taken by both authors during the interviews, and were compared between authors for interrater reliability (Nuenendorf, 2002). As a validation test, summary notes were then sent to the participants, and in only a few cases did participants revise their comments, though none in any material way. The summary notes were then tagged according to the relevant themes, and a codebook was created by the principal investigator after the completion of all interviews based on emerging topics within each theme. For intra-coder reliability, the principal investigator then re-evaluated the codebook, correcting any mistakes, and revising as appropriate. The final codebook consisted of 33 codes, across 5 themes (Purpose, Risks, Benefits, Capabilities, Collaboration). The *total* number of topics (light grey), and the number of *new* topics (black) identified from each subsequent interview are shown in Figure 9.

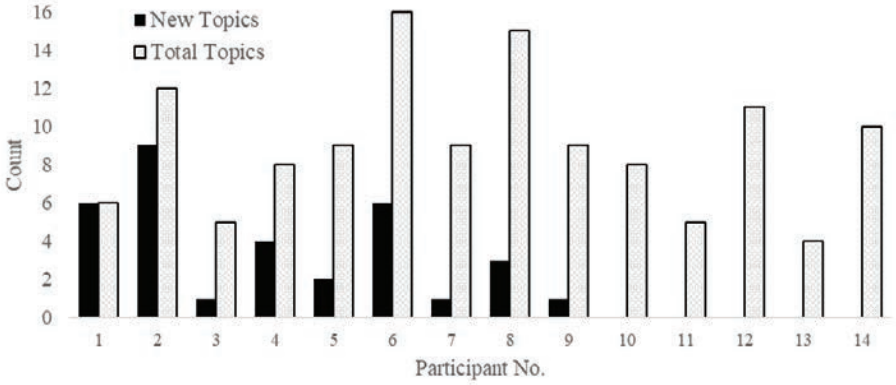


Figure 9: Topic Saturation

By the 5th interview we obtained 67% (22/33) saturation, 88% saturation by the 7th interview, and by the 9th interview, we achieved full saturation, suggesting we are reasonably assured to have identified all relevant themes from our interviews.

Next, we discuss the content of the interviews. Note that our intention of this section is to capture ideas and opinions of experts in the field of cyber attribution across disparate stakeholder groups. Therefore, the content below represents the thoughts and comments *of the participants only*, and do *not* reflect the opinions of the researchers of this Article or our affiliations.

Purpose of Attribution

We first asked participants about their views concerning the motivations by private sector and government agencies for attributing a cyber incident.

Unsurprisingly, there was the view that private firms publicly attribute in part to demonstrate the competence of the company, to raise its profile, and develop additional business opportunities. Participants offered examples of public attribution, such as Mandiant's APT1 report and CrowdStrike's attribution of the DNC attacks, that each, in their view, significantly increased the public prominence of those companies.

However, the most widespread view by participants was that private firms conduct public attribution to call attention to cybersecurity vulnerabilities and threats, and thereby help prepare and inform the broader

community of network defenders (for instance, CrowdStrike's stated purpose for publicly attribution of the DNC hack was to "help protect even those who do not happen to be our customers") (Alperovitch, 2016). One private sector participant even described a sense of moral responsibility that drove companies to call out bad actors in order to improve the cyberspace ecosystem. Public attribution of specific incidents, it was mentioned, can help the broader cybersecurity community better understand state-sponsored campaigns and actor-groups, which then assists network defenders in preventing future attacks.

In addition, participants noted that there are several companies with larger policy agendas that are served through public attribution. For instance, Microsoft has pursued a normative agenda to promote international stability by promoting governors on state-sponsored cyber operations, an objective furthered by public and regular disclosure of malicious actors.[60] Indeed, Microsoft has called for a formal attribution organization charged with "the verification of activities in cyberspace."[61] Relatedly, one interviewee also noted that Mozilla's stated mission to promote the Internet as a global public resource provides another motive for identifying actors that undercut that vision.

Participants disagreed about the importance of the private sector attributing an incident to state-sponsorship or direction. Although publicly assessing that an incident was under state-direction might help a company raise its profile, there were different views about whether the private sector has the capabilities to justify this type of claim (see below) and whether it actually is necessary to serve network defense goals. One private sector respondent noted that attribution to a nation-state (political attribution) may well be a distraction for network defenders and can consume scarce resources. Instead, this respondent noted, private sector attribution goals are best served by focusing on threat actor's TTPs rather than on the actor's relationship to a political entity. However, other respondents noted that political attribution helps ensure that victims truly appreciate their threat environment in order to adequately prepared for a state's highly resourced attacks.[62]

On the other hand, participants described how the USG has its own purposes for publicly attributing an attack, some of which align with private sector goals. The most commonly cited overarching motive for USG attribution was to promote deterrence in cyberspace. Participants noted that public attribution is an important component of deterrence for several reasons. First, public attribution helps 'deterrence by denial' by sharing information that can help build more effective cyber defenses. Participants noted that USG public attribution has sometimes come through technical indicator releases designed to be ingested by network defenders. Public attribution helps draw attention to these technical indicator releases and raises awareness of cybersecurity threat actors, vectors, and mitigation strategies. Second, participants described how public attribution is a prerequisite for economic sanctions or criminal indictments (e.g. the Chinese, Russian indictments to cyber activity). In these cases, public attribution is a preliminary and necessary piece of USG efforts to punish actors for their conduct. Although 'naming and shaming' is sometimes mentioned as a goal of public attribution, participants did not think that USG public attribution alone, in the absence of other punitive actions, imposed real costs.

In addition to deterrence, participants also noted that USG attribution may help build international consensus on what constitutes irresponsible or inappropriate behavior in cyberspace (e.g. norms-building). As more countries come to agreement on the 'red-lines' regarding state cyber conduct, they

[60] See for instance Microsoft's call for a Digital Geneva Convention: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. Last accessed July 26, 2018.
[61] For one articulartion, see https://blogs.microsoft.com/eupolicy/2016/07/08/the-role-of-cybernorms-in-preventing-digital-warfare/ Last accessed July 26, 2018
[62] For more on this debate, see https://pylos.co/2018/03/14/attribution-confusion/. Last accessed July 26, 2018.

will be better able to coordinate and impose collective punitive action. Interview participants currently in government drew attention to the coordinated Five Eyes (FVEY[63]) attribution of the WannaCry and NotPetya attacks and argued that these cases demonstrated coordinated action that can be used to further marshal international attention and collective responses.[64] So, unlike the private sector, participants discussed how the USG publicly attributes cyber incidents to further norm-building efforts and to rally the international community to take action.

A summary of these themes is presented in Table 3.

Table 3: Respondents' views on Purpose of Public Attribution by the Private Sector and the USG

Private Sector	USG
• Profile raising and business development • Informs network defenders • Promotes broader corporate policy and normative agenda	• Promotes deterrence • Informs network defenders • Prerequisite for other punitive actions (e.g. sanctions and indictments) • Support norms-building and rallies international partners for coordinated response

Benefits and risks of private sector attribution

We next asked participants about any benefits or risks of private sector attribution of cyber incidents that would be enjoyed, or borne by USG agencies, respectively.

Benefits

Overall, participants felt that private sector attribution was beneficial for the USG because it leveraged the private sector's technical capabilities (discussed below), thereby crowdsourcing the identification and association of malicious cyber activity with nefarious actors. One participant described this is a form of "self-policing" of bad behavior. This would help the USG by corroborating or validating their own public attribution, lending further credibility to any public statements. For example, FireEye was cited many times in a report by the Office of the United States Trade Representative describing Chinese theft of U.S. intellectual property.[65]

This kind of corroborating disclosure, it was suggested, could also help encourage the public to take a given attack more seriously, which may assist in support of a larger deterrence campaign. Participants also mentioned how private sector attribution may also help support internal governmental discussions, or inter-agency deliberations with government employees who may not have appropriate security clearances.

A number of participants also mentioned that private sector attribution would help the USG avoid having to give up sources and methods by disclosing IOCs, TTPs, or other details publicly. Further, when private sector companies invest their considerable resources providing technical attribution details, it was suggested that this could free up resources by the IC and LE, enabling them to focus on the harder problems of political attribution and understanding nation-state or criminal motives.

[63] See https://en.wikipedia.org/wiki/Five_Eyes. Last accessed August 10, 2018.
[64] See https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/. Last accessed July 26, 2018.
[65] See https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF. Last accessed July 26, 2018

Further, one participant mentioned how private attribution can bring together alliances (FVEY), and particularly, more than just attribution, it becomes the *process* of attribution that helps develop these relationships (as was likely the case with the FVEY reports of the WannaCry attack; BBC, 2017).[66]

On the other hand, one participant was much less optimistic about private sector (or any kind of strong technical) attribution. While not a risk, per se, the participant mentioned that even if USG or private sector could provide all the necessary information in a report, it would likely not matter because nations and their governments respond "politically, not factually." The thinking was that the USG needn't convince those who won't listen to the U.S. anyway, and so it becomes futile to disclose more information.

Risks

Participants cited numerous risks to the USG from private sector attribution. While public attribution can help corroborate the USG's message, it can similarly create confusion and uncertainty if the private sector contradicts it. For example, during the Sony data beach of 2014, some private individuals and companies cast doubt on the USG's announcement of North Korea involvement, suggesting that it was instead caused by and insider.[67] The disagreement within private sector over the *Olympic Destroyer* attack (in which North Korea was initially thought to have been responsible, but later was attributed to Russia) provides another example of how easily disputes can arise during attribution.[68] One participant even critically mentioned that if the government was "more effective" at attributing cyber incidents, there would be less opportunity for confusion or conflicting statements.

Overall, the risk of interfering with U.S. foreign policy was a major issue highlighted by a number of participants. One concern is that "attribution of malicious cyber activity to a state actor has foreign policy implications" and if US-based companies are viewed as having too close of a relationship with the USG, then any public attribution by these company might be interpreted as official U.S. policy. This could have many repercussions, it was mentioned, such as destabilizing sensitive negotiations the U.S. might be having with adversarial countries, or reducing the USG's ability to control its own message internationally when forming a coherent deterrence effort. Now, while the concern may be legitimate, none of the participants were able to point to a specific example of this occurring.

Similarly, participants mentioned that perception of too close a relationship between USG and private sector may cast doubt on the editorial independence of each party's conclusion – that rather than presenting corroborating evidence that is "independent, credible, and legitimate," attributions would be viewed as "two voices with the same conclusion."

Further, there were concerns from both USG and private sector participants about interfering -- either accidentally, or intentionally -- with an ongoing law enforcement, military or IC operation. One participant from a private sector company mentioned that they take precaution to avoid "tripping into" such situations and dutifully comply with government requests to stand down their investigation if it

[66] See https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/. Last accessed July 26, 2018.
[67] See http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-inside-job-not-north-korea-20141231-story.html. Last accessed July 26, 2018.
[68] https://medium.com/@theCTIGuy/attribution-versus-actor-centric-threat-intelligence-8ed722a7d4aa. Last accessed July 26, 2018.

would jeopardize a USG operation.[69] The same participant mentioned that while there is always a risk of interference, that the private sector doesn't (or shouldn't) have the responsibility to "guess what the government is doing." A USG participant added that private companies "can't assess the risk of stumbling on and undermining an ongoing government investigation" because the company wouldn't know *ex ante* what the government is pursuing.

A further concern related to how public attribution could affect adversary behavior. Participants mentioned that publication of technical attribution and IOCs had, at best, very short term utility, because a company's announcement would tip off an adversary, driving the adversary to change her tactics. However, as mentioned by two participants, there is no escaping this -- the same situation exists with vulnerability scanners or anti-virus software cause adversaries to update their tools based on new signatures.

Numerous participants were also concerned that private sector attribution could pressure the USG into taking action against the offending country.[70] On one hand, this was viewed as a useful catalyst if the USG was prepared and willing to take a public position or action against the nation-state. It could also be a positive outcome if it resulted in a social good, such as informing the public that the USG is aware of a particular threat, and is therefore doing something about it, or to prod the USG into taking action that it wouldn't have otherwise taken. On the other hand, the concern was that it may induce the USG into an action where it otherwise wouldn't be able or willing to act. For example, while some private organizations have associated the 2015 Office of Personnel and Management (OPM) breach with the Chinese government, the U.S. government has only gone so far as to say, through a public statement by former DNI James Clapper, that China is the leading suspect, with no formal attribution made subsequently.[71]

One very interesting consequence of private sector attribution that was raised was how it may lead to the creation of an international norm or law concerning an evidentiary standard for attributing a nation state with an act of war. In particular, public attribution may pose problems for the USG if such norms are driven by the private sector, and if the USG would be unable to keep up with the pace or technical sophistication of the reports. The USG has claimed there is no legal requirement to lay out evidence behind attribution (Egan, 2016). However, the 2015 report by the United Nations Group of Government Experts on Information Security (GGE) describes how countries must substantiate claims of international wrongdoing by states, though does not provide further detail.[72] According to our interviews, Russia and China have explicitly referenced this in response to USG attribution claims.

While not a risk to the USG, participants also described a particular risk to private sector companies, when publicly outing threat actors. Participants suggested that private sector attribution or even public disclosure of an investigation into cyber activities of an attack by a nation-state or criminal organization could produce unintended blowback for the company, either in terms of missed business opportunities, or risk to personal safety of the employees. For example, Costin Raiu, director of Global Research and Analysis Team at Kaspersky Labs, described in 2015 how, while analyzing a particular malware, someone allegedly broke into his home and left a message signaling him to "take a break" (Raiu, 2015).

---

[69] But not all firms are as considerate. In March 2018, the security firm Kaspersky released a report describing an alleged US-led counter ISIS operation (*Slingshot*), https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/. Last accessed July 26, 2018.

[70] Although another participant suggested that this was not a concern – the USG has every opportunity and freedom to act or not act at their choosing.

[71] See https://www.reuters.com/article/us-cybersecurity-usa-china-idUSKBN0P525G20150626. Last accessed July 24,2018.

[72] See http://undocs.org/A/70/174. Last accessed July 24,2018.

And so for at least one of our participants, the personal risk to their employees was considerable enough that they had become very cautious about international travel, and releasing any personal or identifiable information in their threat reports.

These benefits and risks are summarized in Table 4.

Table 4: Respondents' views on benefits and risks of private sector attribution

Benefits	Risks
• Private sector reinforcing/validating USG policy initiatives in order to lend credibility, without disclosing sources and methods • Private sector willing to make assertions where government will not (e.g. OPM) • Naming and shaming by private sector may help build norms, and deter bad behavior • Helps support or inform government analysis • Acts as informal outsourcing, and force multiplier by crowdsourcing efforts, thereby freeing the IC and LE to focus on harder problems of political agenda • Can help pressure USG into action, which may be good if it is prepared and willing to take action; or of there is a legitimate social good from this, such as signaling to the public that the U.S. is aware of a threat	• Can lead to confusion if USG is trying to coordinate a message and private sector makes erroneous or conflicting statements • Can interfere with an ongoing LE or IC investigation. e.g. *Slingshot* • Attackers may get tipped off and change their TTPs • May lead to norms in regard to a standard for quality of attribution – a standard that the USG would be unable or unwilling to meet • Attribution to nation-states is a foreign policy affair and should therefore only be conducted by USG • Speed of private sector makes USG look slow • As a risk to the private firms, attribution can put these companies, and in some cases, employees at personal risk; and perhaps lead to missed business opportunities

Comparing attribution capabilities between the private sector and USG

Next, we asked participants what they thought were the relative technical capabilities between private and public sector regarding attribution of cyber incidents.

Participants were unanimous in the belief that there was no single agency or company that had universally superior capabilities. Instead, most participants agreed that each stakeholder had unique strengths. For example, most thought that the private sector had greater visibility into domestic computing networks, as well as internationally because of the security software agents (sensors) installed on these networks. For example, FireEye claims to have information on "over half the Fortune 500…with devices in more than 67 countries worldwide,"[73] and Dell SecureWorks claims to have 4400 customers in 55 countries.[74] It is this visibility and access, it is argued, that enables them to examine IOCs, and track strains of malware, and APTs more quickly than USG. In fact, this was a capability that one law enforcement participant mentioned was an advantage for private sector, because law enforcement would be subject to legal process in order to acquire the same information.

[73] See https://lawfareblog.com/private-sector-cyber-intelligence-could-be-key-workable-cyber-arms-control-treaties. Last accessed July 26, 2018.
[74] See https://www.secureworks.com/. Last accessed July 18, 2018.

In addition, a senior manager at a threat intelligence company suggested that private sector companies also have the added advantages of speed and developing insights into identifying and tracking ongoing threats across multiple sectors simultaneously. This participant described how the business practices of private sector companies allow them to analyze broader trends more efficiently than the USG.

Another participant mentioned how an additional capability comes not from software or hardware, but the private sector's ability overall to attract and retain a more experienced workforce, often composed of former intelligence community and law enforcement career professionals.

However, despite this, participants noted that U.S. intelligence agencies and law enforcement have their own advantages over private companies. First, only they, it was argued, could achieve the highest confidence when attributing a cyber incident to a particular nation's command and control entity. That is, only through their intelligence apparatus would they be able to assess the context and the "greater [political] purpose, motives, and directives of the adversary." So while most participants agreed that this kind of political attribution would be difficult for private sector companies, one participant suggested quite strongly that because nation-state attribution is a foreign policy matter, it is not the role of the private sector to provide this level of resolution. Instead, it should be left to the government – that only it would have insights into the direction and intent of an adversary, especially in light of deterrence messaging, and the potential for false flag operations.

In addition, one participant suggested that law enforcement is in one of the best positions to acquire evidence and attribute an incident because of their authorities to compel evidence through warrants, subpoenas, and international cooperative agreements. Further, law enforcement organizations, it was suggested, have uniquely very strong cultures of policies and procedures regarding the documentation, preservation, defense, and presentation of evidence which aids in attribution, as well as public messaging.

Importantly, one participant mentioned that even despite the strong capabilities of the private sector, only the USG can impose significant consequences on an adversary through criminal indictments, convictions, formal sanctions, or other lawful effects.

In summary, therefore, the feeling was that while private sector companies may enjoy greater visibility and data collection domestically as well as internationally, and may have better business processes for analyzing these data and performing technical attribution, the U.S. intelligence community is the only entity that can (and perhaps *should*) reliably and credibly be attributing cyber incidents to nation states.

The key capabilities of each stakeholder are summarized in Table 5.

Table 5: Respondents' views on comparison of capabilities

Private Sector	USG (IC and LE)
• Have sensors on more computers and networks domestically, and internationally, allows them to perform better technical attribution more quickly • Advantage of better supply of workforce because of higher salaries and simpler hiring process • Companies have an efficiency that the USG doesn't, which comes from technical	• Federal government agencies have unique capabilities that better enable them to assess political motives (e.g. access to classified information) • Law enforcement has best culture for collection, documentation, preservation and publication of information, because of their necessity for judicial review

capabilities (visibility), and also business processes which leverage this visibility in order to gain insights into threat actors and the risk landscape across industries	• Law enforcement has unique authorities to subpoena/acquire and compel information • Law enforcement and IC have intelligence relationships with foreign governments which may provide advanced warning of impending or active cyber activity

Collaboration

All of the participants agreed that there was genuine value in collaboration between the USG and the private sector regarding public attribution. Participants noted that there is a lot the USG can learn from private firms, including information about the cyber threat environment, the TTPs used by malicious cyber actors, and investigatory details and techniques that can help it conduct its own attribution investigations. In addition, participants observed that if the USG decides to publicly attribute an incident, it can make the public case more persuasively by leveraging the work of private firms. Rather than releasing its own evidence and jeopardizing sources and methods, the USG can refer to the details released through private sector findings.[75] However, participants felt it is important for the USG to validate the private findings before leveraging those for its purposes.

Participants noted specific opportunities for collaboration, but also pointed to attendant risks. More formalized modes of collaboration could have a multiplicative effect where the full range of private sector capabilities could inform government investigations. However, participants noted that too close of a relationship poses risks to both the government and the private firm. One subject thought that the government, and especially law enforcement, would need to be careful that formalized collaboration did not violate laws regulating government dealings with the private sector. The private sector also might bear reputational or other risks if they are seen as an arm of the USG, rather than an independent entity. In particular, business opportunities abroad might be hampered if there is a perception that the firm shares client or other valuable information with the USG. Too close of a collaboration might also play in to a Chinese or Russian narrative that U.S. firms are really just extensions of USG policy. Participants did not offer actual cases of formalized collaboration that poses these risks, however one example might be the case of Kaspersky where the USG removed and banned Kaspersky products from Federal networks because of suspected ties with the Russian government.[76]

Informal collaboration between the USG and the private sector might provide benefits to each side without the risks associated with formalized modes. For instance, there are reports that Mandiant alerted the USG about the release of its APT1 report ahead of time, and FireEye has claimed that they regularly give government partners a notice before publication of a report.[77] Participants noted that this type of notification from a company might give the government an opportunity to prepare messaging and other responses once the attribution is public. It might also give the government the opportunity to assess the firm's findings and offer feedback that improves the firm's conclusions. Following the release of the Mandiant APT1 report, the USG incorporated some of the technical data released by Mandiant in their release designed to assist companies in combatting the Chinese IP threat.[78]

[75] E.g. see WannaCry statement at https://www.us-cert.gov/ncas/alerts/TA17-132A. Last accessed July 27, 2018.
[76] See https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4. Last accessed July 26, 2018.
[77] See http://fortune.com/2016/06/25/fireeye-mandia-china-hackers/. Last accessed July 24, 2018.
[78] See https://www.us-cert.gov/ncas/current-activity/2013/02/22/Ongoing-Malicious-Cyber-Activity-Against-US-Government-and-Private. Last accessed July 24, 2018.

Another informal type of collaboration, which has become quite common, was demonstrated with CrowdStrike's analysis of the DNC hack. In that case, CrowdStrike provided its forensics analysis to the FBI so that the FBI was able to conduct an investigation and reach its own findings. There might be other cases where cyber incident victims do not want the USG to conduct and direct investigation, but might be amenable to the USG indirectly reviewing a threat intelligence firm's analysis.

In all these cases of formal or informal collaboration, participants noted that there is a question as to the extent that the USG or the private firm should be transparent. More transparency might improve credibility, but also risks a perception that there is more that is not being shared.

It is also important to note that collaboration between the USG and private firms is currently facilitated by personal relationships. Many threat intelligence firms have been founded by or include senior representation from persons formally occupying senior government roles (e.g. CrowdStrike, Palo Alto Networks). The former government officials who occupy senior roles in private firms will have an understanding of how government functions and how the private firm might be well-positioned to assist.

Participants noted two other varieties of collaboration that present opportunities for the USG. First, is collaboration among private firms. Private firms involved in cybersecurity have collaborated on a range of issues including critical vulnerability scoring, information sharing, and other cybersecurity practices. These companies also collaborate on cyber attribution. One noteworthy example is Novetta's Operation Blockbuster report that attributed the Sony attack to the Lazarus group through collaboration among a private sector coalition that included Symantec and Kaspersky.[79]

Second, our interviews also suggested an important role for collaboration between governments. The WannaCry and NotPetya attributions featured coordination between the FVEY governments. This type of collaboration can potentially bolster the credibility of the attribution findings and rally others in the international community, even in the absence of publicly releasing the evidence that supported the findings. One risk however is that these types of coordinated roll-outs might further slow down an already lengthy public attribution process.

Lastly, participants drew attention to the various proposals for the creation of new formalized cyber attribution organizations. For instance, Microsoft has proposed the creation of a public-private organization[80] while others have argued that a new attribution organization would be most credible and transparent if it was composed entirely of private sector and non-government organizations. (Davis et al, 2017) Despite interest in further exploring these proposals, our interviewees noted that the extensive disagreement between governments and the divergence of approaches among private sector companies create doubts that any of the existing proposals would resolve the standardization, transparency, and credibility challenges with public attribution.

These disparate forms of collaboration are listed in Table 6.

Table 6: Respondents' views on modes of collaboration

Modes of Collaboration for Attribution
• Formal Public Private Collaboration

[79] See, http://www.novetta.com/2016/02/novetta-exposes-depth-of-sony-pictures-attack/. Last accessed August 10, 2018.

[80] See https://blogs.microsoft.com/eupolicy/2016/07/08/the-role-of-cybernorms-in-preventing-digital-warfare/. Last accessed July 26, 2018.

- Informal Public Private Collaboration (Mandiant and APT1, CrowdStrike and FBI)
- Collaboration Among Private Sector (Operation Blockbuster)
- Collaboration Among Governments (WannaCry, NotPetya)

Discussion

In this Article, we differentiated between technical vs political attribution and discussed how the practice of cyber attribution is a complicated, inexact art, with many stakeholders and equities. We described the attribution statements by the USG and the private sector, and examined a dataset of known attribution incidents. In particular, we observed that while the USG has attributed only a handful of cyber activity (14), the private sector is much more prolific in identifying, naming, and discussing in great detail the IOCs and TTPs of these threat groups. Now, some people may argue that this is normal and appropriate – that the USG has materially different interests and responsibilities compared with private companies, and that it is not the role of the USG (or any federal government) to publicly expose every nation or state-sponsored group for malicious cyber activity. However, the growing private marketplace and prolific attribution from the private sector creates a sharp contrast with the Federal government. This dynamic might mean that victims, media, and even foreign governments will increasingly look to private sector companies for assistance and information, and not see the USG as a valuable resource in incident response, thereby sidelining the USG's role and prominence in attribution of cyber incidents. It also may potentially create the appearance that the USG lacks the ability or resources to conduct its own attribution investigations, and thus is not able to effectively deter nation-state actors. The private sector may further come to the belief that they can operate without USG assistance, and undertake increasingly aggressive actions in external networks to investigate and attribute incidents (see also Defense Science Board, 2018 which advocates for increased authorities for private sector companies).

The increase in private and public organizations conducting cyber attribution, together with the ambiguity and difficulty in conducting proper cyber attribution, has led to a confusing state of affairs. These organizations do not operate with standardized (common) evidence collection and assessment practices. An attribution reached at high confidence by one company might not be assessed at the same confidence by another. This dynamic also applies to U.S. intelligence agencies which might have (healthy) disagreement about the strength and meaning of specific pieces of evidence. In addition, different organizations do not always distinguish whether they are attributing merely to machines, persons, or ultimate responsible parties. And if they attribute to a nation-state, they are not always clear about the extent to which the nation-state exercised direction and control over the operation. On the other hand, some private companies have been resistant to attribute to ultimate responsible parties, while others appear to leverage them for maximal marketing and sales opportunities. The use of a variety of naming conventions (e.g. FANCY BEAR, APT 28, SOFACY) further complicates the matter. It is likely because of this confusion that volunteer and non-profit efforts like Florian Roth's Google Doc, APTNotes, the Council on Foreign Relations' dataset have emerged to track and catalogue the full scope of attributions and named APTs. Yet, despite these attempts, further efforts to standardize naming, style, and content of attribution reports is greatly needed.

Expert Interviews

Regarding our interviews, it was interesting that the majority of experts from the private sector came from government – mostly either from law enforcement, or the intelligence community. This point was made a

number of times during conversations, and the consensus was that this was a positive development because it brought a culture of formal investigative tradecraft and legal responsibility to the job. Indeed, as was shown during a recent controversy concerning a private company and its alleged inappropriate collection of images from PLA laptops,[81] such actions may draw interest from federal prosecutors for violations of the Computer Fraud and Abuse Act (CFAA) or the Wiretap Act had the firm accessed a computer within the U.S. or internationally without authorization.[82]

Another observation we had during our conversations, was that all participants exhibited a deep and genuine commitment for what they were doing. Part of this is likely a function of the excitement for the job (e.g. catching bad guys in cyberspace is clearly a thrilling profession), but also there seemed to be a legitimate respect for national interests and security (e.g. catching bad guys who attack your country). Indeed, while interviews were only scheduled for 1 hour, they often lasted longer because participants were so passionate about the topic and eager to share their views.[83]

The conversations also revealed how there is much more collaboration both between private threat intelligence companies, and between private sector and the USG than most people would likely realize. However, the dynamics and frequency of the engagements are not fully clear. What does seem to be the case is that the USG relies heavily on the private sector for threat reports, and awareness, of malicious cyber incidents. While we cannot measure the extent to which each IOC or TTP is consumed by the USG, the reports, themselves, appear to provide them with valuable information that it can then reference, discuss publicly, and use to justify further actions.

What About Attribution of Cyber Incidents to the USG?

It is worth noting that no U.S. based threat intelligence company openly attributes cyber operations to the USG.[84] However, the cyber operations tracker at CFR states that "[n]ineteen countries are suspected of sponsoring cyber operations, including the United States," and that of the 204 state-sponsored incidents, 11 were recorded as being sponsored at least in part, by the USG.[85]

There are several possible explanations for the small number of U.S. observations. The simplest but least likely is that the U.S. does not conduct as many cyber operations as its rivals. This is unlikely given U.S. investments in cyber operation capabilities and reports about U.S. cyberspace activity. A more plausible explanation is that the U.S. has been more stealthy with its operations than other states, and that it dedicates significant care and resources to not be caught. A third and complementary explanation is that most cyber attribution capabilities in the private sector are possessed by U.S. companies who either don't have sensors and visibility in foreign (adversarial) networks, or simply do not track USG operations. It is reasonable to think that U.S. based firms do this out of respect for U.S. operations, patriotism, and in order to maintain a good working relationship with USG entities and agencies.

If these latter explanations (for the rarely attributed U.S. incidents) are true, then there is an important question about how long this will remain the case. We have described an environment of a growing set of capabilities in the private sector to attribute, and it is likely that these capabilities are not owned strictly by U.S. companies. Indeed, start-up threat intelligence companies around the world might find that their

---

[81] See. https://www.fireeye.com/blog/executive-perspective/2018/06/doing-our-part-without-hacking-back.html. Last accessed July 24, 2018.
[82] For CFAA, see 18 U.S.C. § 1030. For Wiretap Act, see 18 U.S.C. § 2511.
[83] Obviously there are many reasons why people enjoy talking. Here, we are highlighting those relevant to this discussion.
[84] While Kaspersky is clear not to attribute cyber operations to any nation state, they have disclosed activities suspected to be linked with the US. For example, see previous reference to the Slingshot operation.
[85] See https://www.cfr.org/interactive/cyber-operations. Last accessed July 27, 2018.

profile would be significantly raised if they can credibly attribute operations to the U.S.. And so, then perhaps the USG should prepare for this kind of exposure.

Attribution for Deterrence?

One of the major benefits of attribution is to serve as a deterrent against future malicious activity. But public attribution of a cyber incident to a nation-state does not necessarily imply any further punitive response. In some cases, public attribution might serve to denounce or name-and-shame a responsible party in a way that could be costly. For example, law enforcement hopes that indictments will restrict life opportunities for the accused (e.g. jobs, travel, etc.). However, in other cases public attribution will not itself be the primary response, and will precede other forms of cost-imposition, such as sanctions. Yet, the benefits of an indictment are not universally shared. One commentator argued that, "as a substitute for other responses to serious cyber intrusions, indictments on balance signal weakness" (Goldsmith, 2018).

Turning back to the CFR dataset, of the 48 cases for which a response by a nation-state was recorded, the action was predominantly a denouncement, as shown in Figure 10. Specifically, the left panel shows the responses (x axis) as a function of the top 4 offending countries (y axis), and highlights that China, Iran, and Russia each received criminal charges; that North Korea and Russia were the only countries to receive sanctions; and that all countries received multiple denouncements.

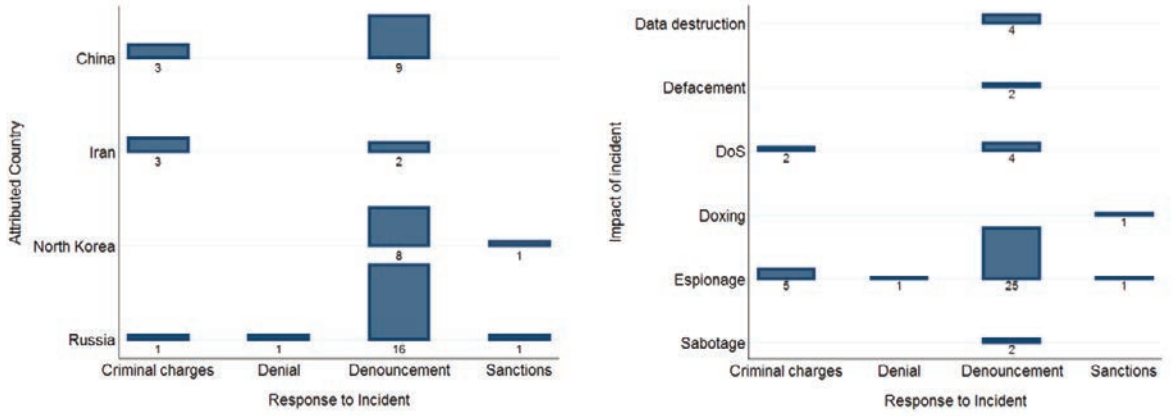


Figure 10: Nation-state response to cyber incident (n=48)

In addition, the crosstabulation in the right panel shows responses (x axis) as a function of type of incident (y axis), for the 48 incidents for which there was a response. For example, this shows that denouncements were by far the most common kind of response, and issued for every type of incident.

Together this suggests that while attribution (aka denouncement) is a relatively popular nation-state response, it is often not followed up with additional measures like sanctions.

Privacy and Safety Concerns

An emerging concern regarding attribution relates to individual privacy and safety. In this Article, we touched briefly on potential risks that employees of threat intelligence firms face when conducting their investigations into APT activities. And at least one of the managers we interviewed would frequently check with their employees about concerns over travelling abroad because of their work.

In addition, the more threat intelligence reports that are produced with more complete information about the individuals behind the operations, one wonders whether this creates a harmful norm for retaliation by other countries that could endanger U.S. persons. Indeed, one commenter wrote, "[h]ow will the United States respond when Russia and China and Iran start naming and indicting U.S. officials? …The Shadow Brokers revealed the identities of specific NSA operators, so even if the National Security Agency is great at concealment as a matter of tradecraft that is no protection against an insider threat" (Goldsmith, 2018). We are not aware of any specific instance where a private sector employee of a threat intelligence company was harmed as a result of their investigations or reporting, and we sincerely hope this does not become a reality.

Further there may be legitimate concerns regarding the privacy of U.S. persons and businesses if a U.S. or foreign government entity were to conduct enhanced surveillance in an effort to detect and attribute malicious cyber activity on privately owned networks. Certainly this is a complicated issue that will not be resolved by this Article. We merely wish to maintain awareness in order to promote transparency.

Intelligence Gain/Loss

Another concern raised during our interviews was the risks of tipping off an adversary with a threat report. This speaks to the familiar issue of intelligence gain/loss (IGL), and the practice of publicly calling out powerful adversaries for their malicious activity is not without careful consideration and deliberation. For example, Mandiant justified their 2013 APT1 report with:

> "It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased understanding and coordinated action in countering APT network breaches" (Mandiant, 2013).

Further, Cylance writes, "[w]e believe that if the operation is left to continue unabated, it is only a matter of time before the world's physical safety is impacted by it. While the disclosure of this information will be a detriment to our ability to track the activity of this group, it will allow the security industry as a whole to defend against this threat. As such, we are exposing this cyber campaign early in an attempt to minimize additional real-world impact and prevent further victimization" (Cylance, 2014).

In effect, these firms are recognizing that while public disclosure of adversary TTPs may cause them to abandon ongoing operations and change their practices, those risks are outweighed by the benefit of exposing the activities. Unfortunately, there does not appear to be sufficient information available that could be used to fully answer the question of whether the gains outweigh the losses. If there ever are formal efforts to standardize attribution indicators (IOCs) and reports, they should also include recommendations for assessing IGL.

Conclusion

After analysis and reflection, we believe that the private sector provides valuable capabilities that augment and support USG interests regarding investigation and attribution of malicious cyber activity. The capabilities and reach of the private sector is obviously strong and broad, and it offers additional information and insights that can bolster existing USG capabilities to detect and manage nation-state and criminal threats.

Specifically, there are opportunities for increased collaboration between public and private sector that can (and should) leverage personal relationships between former colleagues. And there may be more opportunities for more formal, structured, or frequent interactions. However, as was mentioned during our interviews, a collaboration that is too close or structured could well backfire. And so careful and thoughtful, but deliberate interactions will likely produce the best results for detecting and managing malicious cyber activity directed toward U.S. persons and businesses.

References

Accenture, (2017), Cyber Threat-Scape Report: Midyear cybersecurity risk review forecast and remediation.

Anderson, Collin (2018), When Indicators of Compromise Become Indicators of Counterterrorism, Blog, available at https://cda.io/notes/indicators-of-compromise-counterterrorism/. Last accessed April 20, 2018.

Andres Guerrero-Saade, Juan (2015) The ethics and perils of APT research: an unexpected transition into intelligence brokerage, Virus Bulletin Conference (VB2015). Available at https://www.red John S. hill.net.nz/files/r/Guerrero-Saade-VB2015.pdf. Last accessed April 20, 2018.

Alperovitch, Dmitri (2016), Bears in the Midst: Intrusion into the Democratic National Committee, CrowdStrike. Available at https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Last accessed August 8, 2018.

Bartholomew, Brian, & Andres Guerrero-Saade, Juan, (2016) Wave Your False Flags! Deception Tactics Muddying Attribution In Targeted Attacks, Virus Bulletin Conference (VB2016) October 2016. Available at https://cdn.securelist.com/files/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf. Last accessed April 20, 2018.

BBC, (2017), Cyber-attack: US and UK blame North Korea for WannaCry. Available at https://www.bbc.com/news/world-us-canada-42407488. Last accessed June 25, 2018.

Bishop, Matt, Gates, Carrie, & Hunker, Jeffrey (2009), Sisterhood of the Travelling Packets, NSPW'09, September 8-11, 2009, Oxford United Kingdom.

Caltagirone, Sergio, Pendergast, Andrew, Betz, Christopher (2013), The Diamond Model of Intrusion Analysis. Center For Cyber Intelligence Analysis And Threat Research. Available at http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf.

Cylance (2014), Operation Cleaver, Cylance.

Eichensehr, Kristen (2017) Public-Private Cybersecurity, Texas Law Review, 95:467-538.

Davis II, John S., Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase (2017), Stateless Attribution: Toward International Accountability in Cyberspace, RAND Corporation.

Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, Robert Axelrod (2017) Strategic Aspects of Cyberattack, Attribution, and Blame, PNAS vol. 114, no 11

Egan, Brian J., (2016) Remarks on international law and stability in cyberspace, Legal Adviser, Berkeley Law School, California, November 10, 2016. Available at https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf. Last accessed May 1, 2018.

FireEye (2017), Senate Intelligence Committee: Russia and 2016 Election, FireEye.

FireEye, (2018), APT 37 (REAPER), The Overlooked North Korean Actor, FireEye.

FireEye, (2018b) M-Trends2018, FireEye.

Glaser, B. G., & Strauss, A. L. (1967). The discovery of grounded theory: Strategies for qualitative research. Hawthorne, NY: Aldine.

Goldsmith, Jack (2018) Uncomfortable Questions in the Wake of Russia Indictment 2.0 and Trump's Press Conference With Putin, Lawfare Blog. Available at https://www.lawfareblog.com/uncomfortable-questions-wake-russia-indictment-20-and-trumps-press-conference-putin. Last accessed July 24, 2018.

Goodman, L.A. (1961). Snowball sampling. Annals of Mathematical Statistics. 32 (1): 148–170. doi:10.1214/aoms/1177705148.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field Methods, 18(1), 59-82. doi:10.1177/1525822X05279903.

iDefense, (2017) "Cyber-Espionage Threat Group Table, iDefense IntelGraph Reporting. Cyber-operations and Capabilities, iDefense.

Lin, Herbert, (2016) Attribution of Malicious Cyber Incidents: From Soup to Nuts, Working Paper, Stanford Institute for International Studies. Available at https://fsi.stanford.edu/publication/attribution-malicious-cyber-incidents-soup-nuts

Maurer, Tim (2018), Cyber Mercenaries, Cambridge University Press.

Healey, Jason (2011), Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council Issue Brief.

Mandiant, (2013), APT1: Exposing One of China's Cyber Espionage Units, Mandiant.

McHugh, M. L. (2012). Interrater reliability: the kappa statistic. Biochemia Medica, 22(3), 276–282.

Nuenendorf, Kimberly, A. (2002), Content Analysis Guidebook, Sage Publications,

Porter, Chris, (2016), Toward Practical Cyber Counter Deception, Journal of International Affairs, Winter, 2016.

Raiu, Costin (2015), Keynote address at Vulnerability Bulletin 2015 (VB2015), Video, available at https://www.youtube.com/watch?v=Pne5zQU0qpQ, approximately minute 2:30. Last accessed April 20, 2018.

Rid, Thomas & Buchanan, Ben, (2015) Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37. http://dx.doi.org/10.1080/01402390.2014.977382.

Simonite, Tom, (2015), Waiting for a Drop in Corporate Hacks after U.S.-China Deal, Technology Review, available at https://www.technologyreview.com/s/541706/waiting-for-a-drop-in-corporate-hacks-after-us-china-deal/.

Weinbaum, Cortney, Berner, Steven, McClintock, Bruce (2017), SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain, RAND Corporation.

Appendix

Threat Reports

FireEye

Threat reports are available at https://www.fireeye.com/current-threats/threat-intelligence-reports.html and https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-threat-research/threat-research/threat-intelligence. These references include blog posts and links to specialized documents dating back to 2013. The reports provide both summaries of newly identified trends in threats or tactics, short writeups of new APT groups, annual threat report summaries (M-Trends), industry-specific and detailed regional analyses. In addition, FireEye also manages a GitHub repository for IOC from select APTs.[86] The authors of the blog entries are generally, though not always, fully identified to a person.

CrowdStrike

Threat reports are mostly available from https://www.CrowdStrike.com/blog/category/threat-intel-research/, and include detailed analyzes of nation-state threat actors (i.e. through "Adversary of the Month") posts, as well as reports on malware, other cyber attacks, and best practices for protecting one's network – with most articles dutifully including marketing and sales information. The reports are quite colorful, often depicting custom APT graphic art, and are attributed to the human author.

Cisco Talos

Reports are available at available at https://blog.talosintelligence.com/, and attribute cyber campaigns, APT threat groups, and malware (typically RATs), and include both specific APT reports, as well as annual summaries. The products are clearly dated in blog posts and identify any contributing authors. They produce reports describing individual APT groups, weekly "Roundups" of IOCs and threat observed that week, all in considerable detail that includes registry keys, IP addresses, domains, and file hashes.[87]

In addition to the description Cisco Talos takes the following approach to attribution:

> "Everyone has certain characteristics that can be recognised. This may be a way of walking, an accent, a turn of phrase or a style of dressing. If you know what to look for you can easily spot a friend or acquaintance in a crowd by knowing what characteristics to look for. Exactly the same is true for threat actors. Each threat actor group may have certain characteristics that they display during their attack campaigns. These may be the types of malware that they use, a pattern in the naming conventions of their command and control servers, their choice of victims etc. Collecting attack data allows an observer to spot the characteristics that define each group and identify specific threat actors from the crowd of malicious activity on the internet."[88]

Kaspersky

Threat reports are available at https://securelist.com/all/?category=908, and attribute APTs, campaigns, and individual attacks. The reports can be quite long, and include a great amount of detail. Most authors of the APT threat reports are anonymized, identified only as GReaT (an acronym for Kaspersky's Global Research & Analysis Team), though in some occasions, human authors are identified.

---

[86] See https://github.com/fireeye/iocs. Last accessed July 17, 2018.
[87] See https://blog.talosintelligence.com/2018/06/threat-roundup-0616-0622.html#more. Last accessed July 13, 2018.
[88] See https://blog.talosintelligence.com/2014/10/threat-spotlight-group-72.html#more. Last accessed July 14, 2018.

As described in one blog post, Kaspersky likens their process for attribution to paleontology where investigators collect small bones (data) over the years, some of which may appear to be initially interesting, while most of it may be innocuous.[89] And over the years, as one acquires more evidence, more analysis is done and more connections are formed. That is, more parts of the skeleton are being put together until enough of it is assembled that it can be differentiated from other skeletons, and discussed holistically as a threat, and given a name.

Dell SecureWorks

These threat reports are available at https://www.secureworks.com/searchresults?contenttype=Threat%20Analysis&backresult=%2Fresearch, and include at least 100 entries dating back to at least 2008. As with other firms, the posts provide information on new threats, techniques, ransomware, as well as very detailed intelligence reports. The authors of the blog entries are sometimes attributed to specific individuals, as well as the generic "Counter Threat Unit Research Team."

And Dell SecureWorks bases their attribution decision on the following: "In most cases, [Counter Threat Unit (CTU)] researchers do not have intelligence to directly attribute a threat group, so attribution relies on circumstantial evidence and is an assessment rather than a fact. CTU researchers draw on three distinct intelligence bases for evidence of attribution:

> • Observed activity is gathered from CTU researchers' observation and investigation of a threat group's activity on a target network and across SecureWorks data, and analysis of TTPs the threat group employs.
>
> • Third-party intelligence is gained from trusted relationships within the security industry and with other private and public sector organizations, as well as analysis of open source intelligence.
>
> • Contextual analysis compares threat group targets against intelligence requirements of government agencies and other threat actors and compares tradecraft employed by a threat group to tradecraft of known threat actors."[90]

In addition, they justify their scoring criteria on that from the Office of the Director of National Intelligence (ODNI):

> "• High confidence generally indicates that judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.
>
> • Moderate confidence generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
>
> • Low confidence generally means that the information's credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that [there are] significant concerns or problems with the sources."[91]

---

[89] See https://securelist.com/the-art-of-finding-cyber-dinosaur-skeletons/67928/. Last accessed July 13, 2018.
[90] See https://www.secureworks.com/research/iron-twilight-supports-active-measures. Last accessed July 18, 2018.
[91] See https://www.secureworks.com/research/threat-group-4127-targets-google-accounts. Last accessed July 18, 2018.

Other Sources

The interested reader is also invited to browse the APTNotes, threat report repository at https://github.com/aptnotes/data, maintained by David Westcott and Kiran Bandla.[92]

Table of USG Attribution Statements

The list of USG attribution statements is shown in Table 7.

Table 7: USG attribution of cyber incidents

Date of First Incident	Date of Attribution	Incident	Attribution	Mode of Attribution
2006	5/2014	IP Theft	China	Indictment,[93] Statement
12/2014	12/2014	Sony Attack	DPRK	Statement,[94] Sanction
02/2014	02/2015	Sands Casino[95]	Iran	Statement
2011	03/2016	AP Twitter Feed, Others	Syrian Electronic Army	Indictment[96]
Late 2011-2012	03/2016	DDoS on Banks, Dam breach[97]	Iran	Statement, Indictment[98]
07/2015	04/2016	DNC hack[99]	Russia	Statement, Technical Alerts,[100] Sanction

[92] Though, we make no assessment as to the completeness or accuracy of this repository.
[93] See https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. Last accessed July 24, 2018.
[94] See https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation. Last accessed July 24, 2018.
[95] See http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html. Last accessed July 24, 2018.
[96] See https://www.justice.gov/opa/pr/computer-hacking-conspiracy-charges-unsealed-against-members-syrian-electronic-army. Last accessed July 24, 2018.
[97] See https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html?noredirect=on&utm_term=.660be7e66cf5. Last accessed July 24, 2018.
[98] See https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated. Last accessed July 24, 2018.
[99] See https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/. Last accessed July 24, 2018.
[100] See https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf. Last accessed July 24, 2018.

01/2014	03/2017	Yahoo Breach	Russia FSB	Indictment[101]
2009	06/2017	DDoS Infrastructure	DPRK	Technical Alert[102]
05/2017	12/2017	WannaCry	DPRK	Statement,[103] Technical Alert[104]
2010	03/2018	IP Theft	China	Statement[105]
06/2017	02/2018	NotPetya	Russia, or Russian actors[106]	Statement,[107] Technical Alert,[108] Sanction
03/2016	03/2018	Electrical Infrastructure Compromise	Russia	Technical Alert[109]
2013	03/2018	University IP Theft	Iran	Indictment[110]
2016	07/2018	DNC Election Hack	Russia	Indictment[111]
2014 - 2017	09/2018	Sony / WannaCry	North Korean	Indictment[112]
2014 - 2018	10/2018	World Anti-Doping Agency, Organization for the Prohibition of Chemical Weapons	Russia	Indictment[113]

[101] See https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions. Last accessed July 24, 2018.
[102] See https://www.us-cert.gov/ncas/alerts/TA17-164A. Last accessed July 24, 2018.
[103] See https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/. Last accessed July 24, 2018.
[104] See https://www.us-cert.gov/ncas/alerts/TA17-132A. Last accessed July 24, 2018.
[105] See https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF. Last accessed July 24, 2018.
[106] We include "Russian actors" per the Canadian statement, https://www.cse-cst.gc.ca/en/media/2018-02-15. Last accessed July 10, 2018.
[107] See https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/. Last accessed July 26, 2018.
[108] See https://www.us-cert.gov/ncas/alerts/TA17-181A. Last accessed July 26, 2018.
[109] See https://www.us-cert.gov/ncas/alerts/TA18-074A. Last accessed July 26, 2018.
[110] See https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary. Last accessed July 26, 2018.
[111] See https://www.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html. Last accessed July 17, 2018.
[112] See https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
[113] See https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.