Cyber attribution: technical and legal approaches and challenges

Nicholas Tsagourias
University of Sheffield
Sheffield, UK
nicholas.tsagourias@sheffield.ac.uk

Michael D Farrell
Georgia Institute of Technology
Atlanta, USA
michael.farrell@iisp.gatech.edu

Introduction

Attribution describes the process of assigning a particular act to its source not necessarily in the sense of its physical perpetrator but more importantly in the sense of its mastermind. Attribution is important because it forms the basis of appropriate and effective technical, political and legal determinations and underpins technical, political and legal action and responsibility. In the cyber context, attribution has often been presented as a challenge because of the anonymity cyberspace affords, the possibility of spoofing, the multi-stage nature of cyber attacks, and the indiscriminate nature of cyber tools. To this, one should add the required human and technical resources, the lengthy time scales, and the associated investigatory demands. State to state attribution is treated with even more trepidation since the aforementioned problems are magnified whereas attribution or misattribution can engender serious consequences. Things, however, are changing.

In the period 2007 to 2018, there have been more than twenty examples of high profile attribution claims of nation-state cyber attacks.[1] These include attributions made by governments, civil society, and industry.

One of the first public, high-profile instances of a large-scale cyberattack from a nation-state was the DDoS attack against the Estonian government, banks, and news agencies in 2007. The Prime Minister of Estonia, Andrus Ansip, attributed the attacks to Russia.[2] This attribution received public criticism from Finnish security company F-secure,[3] and was

[1] The term cyber attack is used here to describe malicious cyber operations in general
[2] Anderson, Nate. "Massive DDoS attacks target Estonia; Russia accused," *ArsTechnica*, May 14, 2007. https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/
[3] Ibid

contested within the government at the time. Later, Lauri Almann (the permanent undersecretary of Estonia's Ministry of Defense), called the experience of opening up about the attack "brutal" and "embarrassing" but also emphasized that the decision was "conscientious" and allowed Estonia to begin the process of information sharing with non-governmental institutions to deal with the crisis.[4]

The Sony hack of 2014 led to the first instance of the U.S. government publicly blaming a foreign government for a cyber attack against an American corporation.[5] The FBI officially attributed the attack to North Korea[6] and President Obama followed with a speech declaring that the U.S. would "respond proportionally ... at a time and place that we choose".[7] Shortly after, he imposed sanctions on ten North Korean individuals and three entities connected with the North Korean government.[8] Initially, the attribution was criticized by security researchers for its lack of clear information, and security firm Norse proposed an alternative theory in which the hack was the work of insiders unconnected with North Korea.[9] However, other private sector actors subsequently confirmed the FBI's attribution,[10] although there are some who still doubt its legitimacy.[11]

In 2017, the malware NotPetya spread around the world after an initial attack on Ukraine, infecting both companies and governments in Europe, Asia, and the Americas and causing billions of dollars of damage.[12] Within one week of each other, the U.K., U.S., Danish, Australian, Canadian, and New Zealand governments all made statements attributing

---

[4] Johnson, Derek B. "What governments can learn about the original Russian cyber attack," *FCW*, Nov. 6, 2017. https://fcw.com/articles/2017/11/06/estonia-cyber-johnson.aspx

[5] Nakashima, Ellen, "U.S. attributes cyberattack on Sony to North Korea, "The *Washington Post*, https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html?utm_term=.102230247125

[6] Kelly, Michael B, "Here's the Full FBI Statement Calling Out North Korea for the Sony Hack," Dec. 19, 2014. http://www.businessinsider.com/heres-the-full-fbi-statement-calling-out-north-korea-for-the-sony-hack-2014-12

[7] Nakashima, Ellen, "U.S. attributes cyberattack on Sony to North Korea, "The *Washington Post*, Dec. 19, 2014. https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html?utm_term=.102230247125

[8] Roman, Jeffrey, "FBI Defends Sony Hack Attribution," *Bank Info Security*, Jan. 7, 2015. https://www.bankinfosecurity.com/sony-a-7762; Morello, Carol & Greg Miller, "U.S. Imposes sanctions on N. Korea following attack on Sony," *The Washington Post*, Jan. 2, 2015.

[9] Makarechi, Kia, "Are Former Employees, Not North Korea, to Blame for the Sony Hack?" *Vanity Fair*, Dec. 30, 2014. https://www.vanityfair.com/hollywood/2014/12/former-employees-sony-hack-theories

[10] Guitton, *Inside the Enemy's Computer: Identifying Cyber Attackers*, Oxford University Press, 2017; Krebs, Brian, "The Case for N. Korea's Role in Sony Hack," *Krebs on Security*, https://krebsonsecurity.com/2014/12/the- case-for-n-koreas-role-in-sony-hack

[11] Schneier, Bruce, "We Still Don't Know Who Hacked Sony," *The Atlantic*, Jan. 5, 2015. https://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/

[12] Kovacs, Eduard, "U.S., Canada, Australia Attribute NotPetya Attack to Russia," *Security Week*, Feb. 16, 2018. https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia

NotPetya to the Kremlin, with the U.S. statement promising "international consequences." While several security companies and the media had previously attributed NotPetya to the Russian government, both academics and private security companies lauded the attribution as a step toward showing Russia that attacks of this kind would not go unrecognized, with leading cyber threat intelligence firm FireEye to state, "It appears the administration has drawn a line in the sand with an actor that's been extremely aggressive and enjoyed quite a bit of anonymity until now."[13] This example of government attribution was perceived by the public security community as significantly more credible than the attribution to North Korea three years earlier. It suggested greater sophistication and coordination among allied governments, and possibly also a change in public attitudes regarding the role of nation-states in these kinds of cyber attacks.

In 2012, Saudi Arabia's state-run oil company, Aramco, was hit with a major cyber attack. At the time, it was regarded as the most destructive act of computer sabotage on a company ever reported. Data on 75% of Aramco's corporate computers was erased by the virus — documents, spreadsheets, e-mails, files — replacing all of it with an image of a burning American flag. Immediately after the attack, Aramco was forced to shut down the company's internal corporate network, disabling employees' e-mail and Internet access, to stop the virus from spreading. Unnamed US government intelligence sources attributed this attack to Iran in interviews that were published by the NY Times newspaper[14] as part of a front page story, which was later supported by private security companies.[15]

The electric grid in Ukraine has also been a target of cyber attacks more than once since December 2015, with both the Ukrainian government[16] as well as companies and non-profit cyber security organizations[17] attributing the December 2015 attack to Russia. In February 2017 the Ukrainian government went further than a press release and held a public news conference in which Russian security services were identified as the perpetrator[18], along with private software firms and criminals, for new cyber attacks against industrial control systems after the December 2015 incident.

---

[13] Greenberg, Andy, "The White House Blames Russia for NotPetya, The 'Most Costly Cyberattck in History,'" *Wired*, Feb. 15, 2018. https://www.wired.com/story/white-house-russia-notpetya-attribution/
[14] https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html
[15] http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work
[16] http://mpe.kmu.gov.ua/minugol/control/uk/publish/printable_article?art_id=245086886
[17] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[18] https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN

What the above incidents also reveal is the actors involved in making determinations of attribution. These actors are governments, private security companies and civil society organisations. The most notable example of government-led attribution concerns the hacking into the Democratic National Committee emails. The Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) issued a joint statement claiming that the Russian government was responsible for the hack.[19] The FBI[20] report *Joint Analysis Report: GRIZZLY STEPPE—Russian Malicious Cyber Activity* reinforced the conclusion that Russia was behind the WikiLeaks releases. Furthermore, according to the report *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*, President Putin ordered the campaign to influence the US elections.[21]

With regard to government-led attribution it should be said that although it can be harder for governments to share their data sources or reveal methods, they typically have access to significantly more information. Both the U.S. and the U.K. have invested heavily on attribution technologies and attribution is viewed as part of the cyber security policies for deterrence and law enforcement purposes.[22] In 2012, Secretary of Defense Leon Panetta claimed the DoD had been investing in attribution and "potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America,"[23] and in 2015, the former UK Chancellor George Osborne stated, "To those who believe that a cyber attack can be done with impunity, I say

[19] Director of National Intelligence, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security" (7 October 2016), available at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, accessed on 24 August 2017.

[20] U.S. Department of Homeland Security & Federal Bureau of Investigation, "Joint Analysis Report: GRIZZLY STEPPE—Russian Malicious Cyber Activity" (29 December 2016), available at: https://www.uscert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZL Y%20STEPPE-2016-1229.pdf, accessed on 24 August 2017.

[21] ICA, "Assessing Russian Activities and Intentions in Recent US Elections" in Office of the Director of National Intelligence, "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution" (6 January 2017) ICA 2017-01D, p. 1, available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf accessed on 24 August 2017.

[22] "National Cyber Security Strategy 2016-2020," *HM Government*, 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strat egy_2016.pdf; "The Department of Defense Cyber Strategy," *U.S. Department of Defense*, April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[23] Panetta, Leon. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," *U.S. Department of Defense*, Oct. 11, 2012. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136

this: that impunity no longer exists."[24] Given the important interests underpinning a government's decision to attribute a cyber attack, there is an argument to be made that the government alone should be making that decision.[25] Some scholars have argued however that government attribution rarely occurs in isolation from the private sector and that the information sharing and cooperation between them has always informed official government attribution decisions.[26]

Private security companies are involved in attribution either independently or in conjunction with governments. The 2013 Mandiant APT1 report not only name a particular Chinese military unit involved in cyber attacks, the company also named individuals involved with the attacks. In this way, the report was detailed and raised the bar as to the quality of attribution claims a private cyber security firm could make.[27] Anecdotally, this seems to have spawned something of a "Mandiant-effect" for security firms whereby they believe they need a report of that nature under their belt to achieve widespread respect and credibility. When Crowdstrike published a report on the 'Putter Panda' threat actor group the following year, the company wanted to highlight a different People's Liberation Army (PLA) cyber unit in China to show that the cyber espionage problem was more widespread than described in the APT1 report.[28] Moreover, Crowdstrike was motivated to provide even more findings and make a case that left little room for doubt. In the introduction to the report, it is acknowledged that even after the APT1 report, and the indictment of five Chinese nationals, that Chinese officials continued to deny all actions, stating, "The Chinese government, the Chinese military and their relevant personnel have never engaged or participated in cyber theft of trade secrets." In response, the Crowdstrike report states, "Through widespread espionage campaigns, Chinese threat actors are targeting companies and governments in every part of the globe... We believe that organizations, be they governments or corporations, global or domestic, must keep up the pressure and hold China accountable until lasting change is achieved."

---

[24] Osborne, George, "Chancellor's speech to GCHQ on cyber security," Nov. 17 2015. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

[25] Romanosky, Sasha, "Private-Sector Attribution of Cyber Attacks: A Growing Concern over the U.S. Government?" *Lawfare*, Dec. 21, 2017. https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government

[26] Eichensehr, Kristen E. "Public-Private Cybersecurity," *Texas Law Review*, 95 (2017). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847173

[27] APT 1 report

[28] "Putter Panda," CrowdStrike Intelligence Report, June 2014. https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

With regard to the involvement of the private sector in attribution it should be noted that the private sector experienced an increasing amount of cyber espionage from foreign state actors in the period 2005 to 2010, and there was a growing sense of frustration among some of them that the government was not doing enough to prevent these malicious activities.[29] It is possible that private actors began taking action and publicly attributing attacks around 2010 to help fill this void and make it harder for the government to ignore such activities. Commercial firms also believed that they could help expose criminal behavior and support their customers by potentially reducing the threat. The increased number of government-led cyber attributions might indicate that the private sector's disclosures helped turned that tide, that a threshold of acceptable behavior was surpassed, or some combination of the two. However, the private sector has not stopped making attribution claims now that governments are making them, too. There are apparent benefits to private sector attribution. Companies can be more transparent without the need to protect classified information, although companies can also have sensitive or proprietary data sources.[30] They may also be able to act more freely and with less bias towards political objectives.[31] These features can lend transparency, accountability, and legitimacy to private reports. However, private actors may be more likely to take greater risks, including the possibility of being wrong. They are also more removed from the broader social, economic, and political impacts of their work. And, of course, commercial companies have motivations that ultimately relate back to creating value for their shareholders.

A notable civil society actor that has been involved with attribution for many years is The Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto. The group has focused on researching digital espionage against civil society, including practices that impact freedom of expression and human rights. In general, these issues have not received the same prioritization from governments and industry in terms of justifying cyber attribution. But The Citizen Lab has been uncovering espionage networks for longer than most actors. In 2009, the group published a report called "Tracking GhostNet:

---

[29] Smith, Brad, "The need for a Digital Geneva Convention," Microsoft, February 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[30] Carr, Jeffrey, "Responsible Attribution: A Prerequisite for Accountability," Tallinn Paper no. 6 (2014) http://www.ccdcoe.eu/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%206%20Carr.pdf

[31] Guitton, *Inside the Enemy's Computer*; Gerstein, Josh. "Iran cyber indictment came days after U.S.-Iran deal," *Politico*, March 24, 2016. https://www.politico.com/blogs/under-the-radar/2016/03/iran-cyber-indictment-came- days-after-us-iran-deal-221202

Investigating a Cyber Espionage Network,"[32] which was the result of a 10-month investigation into alleged Chinese cyber spying against Tibetan institutions. The report documented 1,295 infected hosts in 103 countries. The determination about who was in control of the GhostNet system was not the primary motivation of the report. Although it states that the analysis points to China, the report focused on documenting the extent of the infiltration to "serve as a wake-up call."[33] Other universities such as Georgia Tech have also received sponsored research funding to develop enhanced attribution frameworks[34] and counter the use of botnets which are essential to early stages of most malicious cyber campaigns.[35] While still in relatively early stages, this research demonstrates a commitment on behalf of government sponsors (US, in this case), to seek new and/or evolved approaches to cyber attribution that are releasable to the public and based on unclassified data that can be more easily disseminated as part of attribution claims.

Although the preceding discussion and the data provided in Table 1 does not include every nation-state attribution that was made in this time period, it does provide a snapshot that highlights several phenomena, including a number of changes in the process and intensity of attribution over the years. These changes relate to the scale, origin, transparency, and coordination of cyber attribution.

Year	Description	Attributed by?	Attributed to?	How delivered?	Verified by others?
2007	Estonian DDoS	Estonia	Russia	Statement	No
2009	Ghost Net	Citizen Lab	China	Report	No
2010	Google, other US companies	Google	China	Statement	Yes
2010	Stuxnet	VirusBlokAda	US, Israel	Blog	No
2011	Gmail hacking	Google	China	Statement	No

[32] "Tracking GhostNet: Investigating a Cyber Espionage Network," Citizen Lab, March 28, 2009. https://issuu.com/citizenlab/docs/iwm-ghostnet
[33] "TRACKING GHOSTNET Investigating a Cyber Espionage Network," Citizen Lab, March 28, 2009. https://citizenlab.ca/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/
[34] http://www.news.gatech.edu/2016/11/29/17-million-contract-will-help-establish-science-cyber-attribution
[35] https://www.gtri.gatech.edu/newsroom/faster-detection-cleanup-network-infections-are-goals-128-million-project

2012	Saudi Aramco (Shamoon)	Symantec, Kaspersky, Seculert	Iran	News media	Yes
2013	APT 1	Mandiant	China	Report	Yes
2014	Sony	US	North Korea	Statement	Yes
2014	White House, State Dept	Powerline	Russia	Blog	No
2014	Operation SMN	Novetta	China	Report	No
2014	Putter Panda	CrowdStrike	China	Report	No
2015	GitHub DDoS	Citizen Lab, International Computer Science Institute	China	Blog	No
2015	TV5 Monde outage	FireEye	Russia	Report	Yes
2016	DDoS on US banks	US	Iran	Indictment	Yes
2016	DNC	US	Russia	Statement	Yes
2016	Ukraine power grid (2)	Ukraine	Russia	Statement	Yes
2016	Bangladesh Central Bank	Symantec	North Korea	Report	Yes
2016	NATO troops phone hack	NATO	Russia	News media	No
2017	Belgacom	Belgium	UK	Criminal investigation	Yes
2017	WannaCry	US, UK, Australia	North Korea	Statement	Yes

2018	NotPetya	US, UK, Australia, Denmark, New Zealand, Canada	Russia	Statement	Yes
2018	Hacks on US institutions	US	Iran	Statement	Yes

Table 1. Timeline of key nation state cyber attacks. Selected examples as notable from public literature. Privately-sourced attributions are shaded in yellow. Publicly-sourced attributions shaded in blue.

- *Scale.* The number of attribution claims has increased over time. Between 2007 and 2013 (seven years) there are just seven examples. However, between 2014 and 2018 (just five years) there are 15 examples. This increase has been documented in numerous sources.[36] This could be a function of a higher volume of cyberattacks in the first place, or perhaps, a tipping point that encouraged more actors to "out" foreign state actors publicly.
- *Origin.* There is greater willingness from governments to publicly attribute cyberattacks. For example, the first listed attribution claim that was originally made by the U.S. government (rather than the government confirming a private sector report) was in 2014. But in the years since, the U.S. has led the public attribution of at least five nation-state cyberattacks. Other countries, including Ukraine, Belgium, U.K., Australia, New Zealand, and Canada, have also publicly attributed cyberattacks that affected their countries in recent years.
- *Transparency.* There is pressure to release the analysis behind an attribution claim. As was said, the 2013 Mandiant APT1 report was notable for the depth of analysis it provided, and there have since been other attribution reports that have included a similar level of detail and description. In general, private sector attribution claims tend to include more detailed technical analysis than do public sector claims – often

[36] "Cyber Warfare: From Attribution to Deterrence," Infosec Institute, October 3, 2016. https://resources.infosecinstitute.com/cyber-warfare-from-attribution-to-deterrence/

assumed as the need for the latter to protect classified information or protect the sources and methods used to collect such information.

- *Coordination*. Although competition and adversarial relationships between companies and governments remain an important element of attribution, there have been more examples of coordinated action and information sharing. This includes examples from the private sector such as Operation SMN, which was coordinated by numerous industry partners in 2014,[37] and from governments such as the 2017 NotPetya attribution. The NotPetya assertion originally from the U.S. but was quickly verified by other countries including the U.K., Australia, Denmark, New Zealand, and Canada.[38]

What also transpires from the preceding discussion is that attribution is not a monolithic process; it is a multifaceted and interactive process involving various actors, domains (technical, political, legal), determinants and techniques. In a previous article one of the authors described the three-fold dimension of attribution as technical, political and legal.[39] Technically, attribution is about the forensic investigation of a malicious incident to origins of an attack platform and its associated tooling and infrastructure. Political attribution is about the political determination of 'who did it' in the form of an individual or a state and is based on political analysis, assessment and judgment. As the report *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution* put it '[a]n assessment of attribution usually is not a simple statement of who conducted an operation, but rather a series of judgments that describe whether it was an isolated incident, who was the likely perpetrator, that perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation.[40] Political attribution is performed by the executive branch of the government or by political institutions in general and underwrites political decisions and action. Legal attribution is about the legal

[37] "Operation SMN: Axiom Threat Actor Group Report," Novetta, 2014. http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

[38] Kovacs, Eduard. "U.S., Canada, Australia Attribute NotPetya Attack to Russia," *Security Week*, February 16, 2018. https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia

[39] Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution', *Journal of Conflict & Security Law* 17, 2 (2013); Herbert Lin. "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Columbia Journal of International Affairs* 70(1) (2016): 75-137,11.; David Clark and Susan Landau. "Untangling Attribution." Massachusetts Institute of Technology, 2011. http://static.cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf; J

[40] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION 1 (2017), 2

determination of 'who did it' on the basis of legal criteria in order to ascribe legal consequences. Legal attribution is usually performed by legal professionals such as courts.

This does not mean that these processes are mutually exclusive; instead they support, infuse and shape each other although their determinants and techniques may differ. To explain, technical attribution feeds into the political and legal attribution processes because they both rely on forensic evidence in order to make political or legal determinations but it is also the case that technical attribution cannot always identify the individual or the state behind the attack which is the function of the political process of attribution whereas political determinations of attribution need to comply with the legal standards of attribution if a state wishes to use the remedies offered by international law.

This article will study the technical and international law approaches to attribution, identify challenges associated with cyber attribution and consider proposals to improve cyber attribution. For this reason, section 2 will discuss the techniques and determinants of technical attribution whereas section 3 will examine the legal determinants of attribution according to the law of state responsibility. The law of state responsibility has been chosen because attribution is one of its constitutive elements and because the function of the law of state responsibility is to maintain international legality.

Because legal determinations of attribution require assessment and interpretation of technical evidence, the article will go on to consider in section 4 what evidence is required to establish attribution, what is the required standard of proof and who has the burden of proof. These issues will be examined in the context of the ICJ as the primary judicial mechanism to adjudicate matters of state responsibility. In section 5 the article will discuss proposals for improving the legal process of cyber attribution and more specifically proposals envisioning the revision of the legal determinants of attribution and proposals envisioning the creation of an international attribution agency.

2. Technical cyber attribution

In order to discuss technical cyber attribution in a concise way that supports the goals of this paper, we use the botnet as our fundamental component for analysis since it is not only central to the threat landscape but generic enough to explain concepts that apply across a wide spectrum of malicious cyber activities. This treatment is not intended to be

comprehensive or detailed as the technical elements alone of attribution could fill several volumes and the purpose of this paper is to examine legal aspects in more detail.

A botnet has been the fundamental building block for malicious cyber campaigns of various flavors for nearly two decades. Simply put, a botnet is a collection of compromised host computers that can be herded for any of several different uses by its owner – the botmaster. As depicted in Figure 1, there are three fundamental actions that take place in a botnet, which can be separated into phases of the botnet lifecycle: infect, command & control (referred to in shorthand as C2) and monetize.

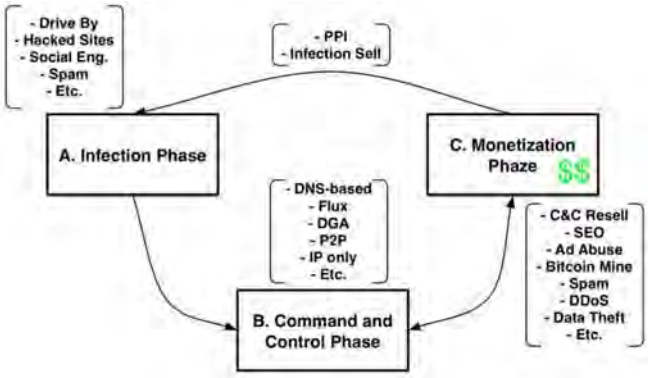

Figure 1. The three phases of the botnet lifecycle.

Botmasters set up their C2 infrastructure in such a way so they can ensure high levels of agility and resiliency. To date, malware analysis has dominated much of the attribution analysis efforts. Using static and dynamic analysis of malware samples, security researchers are trying to keep up with modern botnet threats (i.e., identifying new C2 domain names and IP addresses). This often leads the security community to even "attribute" a threat based on the malware family behind the illicit operation, rather than the orchestrated deployment of cyber operations infrastructure.

When used in isolation, this "binary-focused" approach has decidability limits. It is, among other problems, very difficult to simulate user behavior and to execute all different versions of the malware family that "enable" the botnet. Furthermore, not all infections (or bots) will be utilized (or monetized) in the same way by the botmaster. Therefore, binary-focused efforts face "scalability" and "visibility" challenges. As malicious actors recognize these limits, and exploit analysis constraints in novel malware techniques, e.g., challenging researchers in terms of how long one should execute the malware, how many binaries must

one run in order to have sufficient coverage of the botnet due to polymorphism,[41] which binaries must one run, etc.

Binary-focused analysis systems are (i) unlikely to build a "honeypot" that seamlessly resembles the actual Internet, and (ii) they may never know a priori the adversarial tactics that a botmaster would employ in order to stay under the radar from existing defenses or to evade malware analysis. Changing the status quo in the fight against Internet threats would require new methods to passively track (in raw network traffic) the evolution of malicious activities and threats over time.

Cyber threat actors achieve their malicious ends by relying on a complex series of actions, as seen in Figure 1, to infect (A) and persist (B) on an infected machine, remotely communicate with the criminals (B), and monetize the infected machine (C). Each component of this chain introduces *entities*, such as malware samples used for infection or domain names used for command and control (C2) communication, that have explicit *relationships*, such as malware sample m *queries* the C2 domain d. These relationships can be unified to identify threats in unknown traffic and potentially even the cyber criminals themselves. Furthermore, malware often removes its tracks on the victim machine, which makes efficient and reliable passive network data collection paramount to successful detection.

In order to examine and track the evolution of a given malicious operation, which is part of the traceback task in an attribution, we need to be able to answer some basic questions: 1) how do infections get created? 2) how do botnets remain under the control of the adversary? and 3) how are infections monetized by the adversary? Clearly it is up to the discretion of the illicit *operator* to decide upon these three questions. However, we can assume three things: first, there must be an infection phase, whereby the adversary infects vulnerable hosts. Second, there must be a command and control (C&C) infrastructure in-place, so the adversary can control the infected hosts. Third, there must be a way that the adversary can profit from the illicit operation.

Network-centric attribution hierarchy

Technical attribution of a malicious threat can take place at multiple levels from as specific as identifying the individual(s) responsible for orchestrating it to as general as discovering the tools used to support it. It is a useful concept to consider a hierarchy for technical attribution

[41] A. Dinaburg, R. Royal, M. Sharif, and W. Lee. Ether: malware analysis via hardware virtualization extensions. In ACM CCS, 2008.

discussions. Each level of the hierarchy explains increasingly more about a given threat and its actor as it is traversed from bottom to top.

At the bottom of the technical attribution hierarchy are the *infrastructure and tools* used to support malicious activity. For example, the malware used, the URL structure of command and control (C2) protocols, and the host infrastructure all reflect tool choices made by the threat operators. This information is regularly used in industry and academia alike to classify,[42] cluster,[43] and perform coarse technical attribution[44] of related threats. With respect to attribution, grouping infrastructure and tools can help identify patterns used in a specific campaign or by specific criminal operators, intuitively suggesting that this grouping will help with higher levels in the attribution hierarchy.

The next level up on the technical attribution hierarchy corresponds to a *campaign* carried out by the underlying tools and infrastructure and initiated by the threat actor(s). We define a malicious campaign to be a group of infrastructure and tools used for a single purpose. For example, it is documented that threat actors often register swaths of domain names at a time for a particular malicious campaign.[45]

Next in the technical attribution hierarchy is the *virtual actor*, which corresponds to the cyber presence of one or more threat actors. One of the very few technical representations of a virtual persona are registrant information contained in WHOIS records, which may correspond to real-world representations of the physical person(s) behind a threat. Table 2 shows an example of how the attribution hierarchy can be correlated with network level features. In this project, our intention is to research and qualify the merit of such network signal with the respect of their ability to attribute historic and current attacks.

---

[42] Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. Building a dynamic reputation system for DNS. In the Proceedings of 19th USENIX Security Symposium (USENIX Security '10), 2010. Leyla Bilge, Engin Kirda, Christopher Kruegel, and Marco Balduzzi. EXPOSURE: Finding malicious domains using passive dns analysis. In Proceedings of NDSS, 2011.

[43] Ulrich Bayer, Paolo Milani Comparetti, Clemens Hlauschek, Christopher Kruegel, and Engin Kirda. Scalable, behavior-based malware clustering. In NDSS, volume 9, pages 8–11. Citeseer, 2009. Georg Wicherski. pehash: A novel approach to fast malware clustering. In LEET, 2009. R. Perdisci, W. Lee, and N. Feamster. Behavioral clustering of HTTP-based malware and signature generation using malicious network traces. In USENIX NSDI, 2010.

[44] Mandiant. APT1. Technical report, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[45] DomainTools. Bulk Domain Registration Agents. Technical report, 2015. http://informationsecurity.report/Resources/Whitepapers/49ae492c-7d2b-4c46-83ea-bb8e8543a0d4_The%20DomainTools%20Report%20Bulk%20Domain%20Registration%20Agents%20as%20Cyber%20Threats.pdf. Shuang Hao, Nick Feamster, and Ramakant Pandrangi. Monitoring the initial dns behavior of malicious domains. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pages 269–278. ACM, 2011.

Level	*Source*	*Data*
Physical person	Real world	Name, aliases, address, phone number
	WHOIS	Registrant: name, phone number, address
Virtual persona	WHOIS	Registrant: email, name, phone number, address
Campaign	WHOIS	**Registration date, name servers, registrar**
Infrastructure and tools	Malware	**Host infrastructure, MD5 hashes**
	Blacklists	**Host infrastructure, URLs**

Table 2. Incomplete list of potential data points for different levels of the attribution hierarchy. Note that bold items either cannot be faked or hidden in WHOIS or doing so would cause a botnet to operate improperly if altered.

The various components of the threat lifecycle form a *technical attribution hierarchy*; a hypothetical example is shown in Figure 2. As we go up the y-axis, we identify information more specific to the actual threat actor and as we move along the x-axis we find less reliable, easier to spoof information. For example, it is trivial to lie about the organization used to register a domain name, but for malicious infrastructure to resolve, it *must* use a proper IP address or Name Server. Note the hierarchical nature between the threat actors (grey), virtual personas (blue), WHOIS information (yellow), and infrastructure (pink and orange).

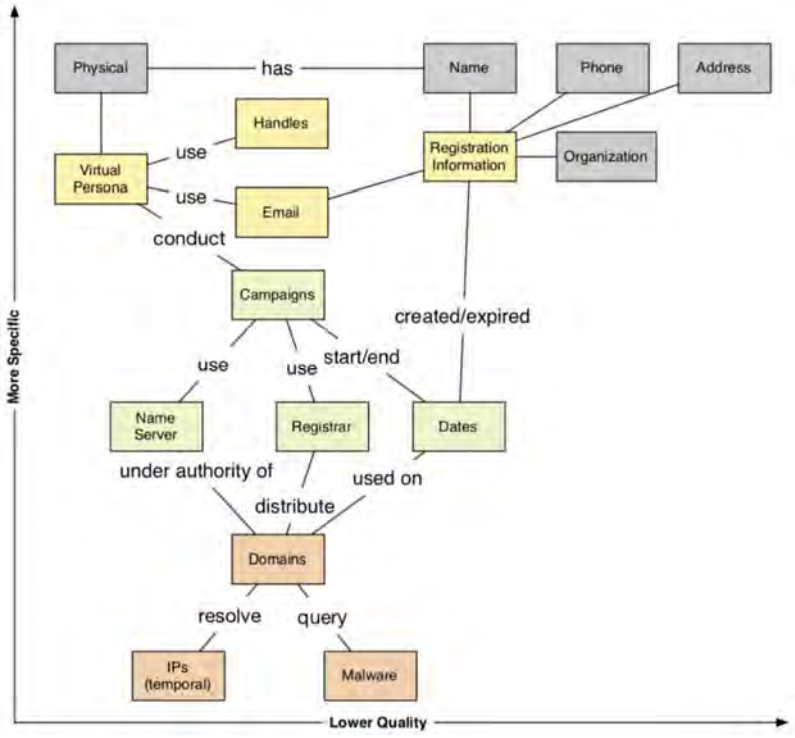

Figure 2. Relational data processing is needed to understand unknown traffic and attribute malicious threats.

In conclusion, the current state of technical attribution using network data utilizes very large data sets and analysis processes, and focuses on data that are very difficult or impossible to fake. For example, if the command-and-control (C2) function of a malicious cyber operation requires use of the Internet services such as DNS, data elements that support accurate and timely domain name resolution are very useful. The end goal of precise and consistent technical attribution to an individual remains challenging and it is even more challenging attribution to a state. This is supplemented by the political process of attribution. The combination of technical and political attribution would then feed into the legal process of attribution if a state decides to utilize the available international law remedies. This issue will be discussed in the next section.

3 Attribution in international law

It is perhaps restating a truism to say that international law as a governance tool is ontologically and functionally dependent on states. As the founding subjects of international law states are the main bearers of obligations and responsibility. States are however

inanimate entities which act through physical persons. As the Permanent Court of International Justice (PCIJ) noted in its Advisory Opinion on German Settlers in Poland, 'States can act only by and through their agents and representatives'.[46] Attribution in international law 'subjectivises' an act in that it transforms a private act into a state act that is, an act of a subject of international law.[47] In doing so attribution triggers the application of international law and underpins international responsibility and it is for this reason that attribution is a constitutive element of the law of state responsibility.[48] Attribution is also a 'normative' process whose scope and content is moulded by international law's normative reach as far as subjects are concerned as well as by its approach to what is a state. Because the definition of state for the law of state responsibility is reduced to the substantive structures, entities and functions through which its lego-political order is maintained and because the law of state responsibility is premised on a sharp distinction between the public (state) and the private domain[49] the bases of attribution are inevitably quite narrow. Consequently, attribution in the law of state responsibility requires an identifiable, direct and close link between a state and an individual or between a state and an act; a link that overrides the latters' independent existence.

This occurs when an institutional, functional and agency link between a state and a person or an act is established. The institutional link covers the relation between a state and its *de jure* or *de facto* organs.[50] *De jure* state organs are those that are defined as such by the state's law. The army for example is a *de jure* state organ; consequently, malicious cyber operations executed by army officers will be automatically attributed to the state. Similarly, a hacker group incorporated into the state apparatus, for example into the army, becomes a *de jure* organ whose acts will be attributed to that state.[51] This will cover for example the Estonian Defence League[52] or Unit 6138. According to the 2013 Mandiant report 'ATP1 Exposing

[46] German Settlers in Poland, Advisory Opinion [1923] PCIJ Rep Series B No 6 at 22
[47] Olivier de Frouville, 'Attribution of Conduct to the State: private individuals' in James Crawford, Alain Pellet and Simon Olleson (eds), *The Law of International responsibility* (OUP 2010) 257 270; Luigi Condorelli and Claus Kress, 'The Rules on Attribution: General Considerations', ibid, 221.
[48] Art 2 International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts (2001) (ARSIWA) and James Crawford, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries (CUP 2002) 84; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), [2007] ICJ Rep 43 (Bosnia Genocide), paras 179, 379 385
[49] Bosnia Genocide para 406, Crawford, 91
[50] Art 4 ASRIWA; ICJ, *Bosnia Genocide,* para 385.
[51] *Bosnia Genocide,* , para 389.
[52]

One of China's Cyber Espionage Units', Unit 61398[53] is a unit within the PLA believed to operate under the 2nd Bureau of the 3rd Department of the People's Liberation Army General Staff Department (GSD).[54] Similarly, with regard to the hacking into the DNC, twelve Russians were indicted in July 13, 2018.[55] According to the indictment, they were GRU, a Russian military intelligence agency, officers.[56] D*e facto* organs are state instrumentalities. In the *Nicaragua* case the ICJ spoke of complete dependence and control[57] whereas in the *Bosnia Genocide* case the ICJ spoke of "strict control" or a "great degree of control."[58] Consequently, a group of hackers created by a state to perform state functions and operating under the control of that state but not incorporated within the state apparatus is a *de facto* organ unless there is some margin of independence in decision-making.[59]

A functional link between a state and an entity exists when an entity is empowered by a state to exercise governmental authority.[60] The delegation of authority in this case should be specific and should involve functions whose performance requires special state powers. For instance, if a company takes offensive cyber defence action in order to protect its property, this act will not be attributed to a state even if the company acts on the basis of enabling legislation such as the one contemplated in the US[61] because the delegation of authority under said legislation is not specific and does not involve governmental functions.

---

[53] Mandiant, APT1 Exposing One of China's Cyber Espionage Units (2013), https://www.fireye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf Executive summary

[54] Mandiant, APT1, 3, 8-9; FireEye SPECIAL REPORT / RED LINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE June 2016 https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf; Mikk Raud, China and Cyber: Attitudes, Strategies, Organisation (2016) https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf

[55] https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf ; https://www.theguardian.com/us-news/2018/jul/13/russia-indictments-latest-news-hacking-dnc-charges-trump-department-justice-rod-rosenstein

[56] Ibid, para 2

[57] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States of America*), para 109; *Bosnia Genocide*, paras 390-391, 307.

[58] *Bosnia Genocide*, paras 391, 393.

[59] *Bosnia Genocide*, para 394.

[60] Articles 5 and 6, ASRIWA.

[61] For a discussion of US proposals see *Robert Chesney*, Legislative Hackback: Notes on the Active Cyber Defense Certainty Act Discussion Draft, Lawfare (7 March 2017) available at: https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft.

An agency link is established when a state instructs or directs a person or when a state exercises control over the malicious act.[62] With regard to the criterion of control, two standards have emerged in international jurisprudence. One is that of effective control over the act which requires indispensable state input in the commission of the malicious act[63] and the other is that of 'overall control' over an organised group which is established "not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity" and "it is not necessary that, in addition, the State should also issue, either to the head or to members of the group, instructions for the commission of specific acts contrary to international law."[64] According to the ICJ, the 'effective control' standard applies for purposes of state responsibility although the Court recognised that different standards of control may apply in different areas of international law.[65]

Applying now Article 8 ASR to the DNC hacking, according to the report *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*[66] Russia's President Vladimir Putin ordered the campaign to influence the US elections.[67] This invokes the attribution standard of instructions. In order for instructions to lead to attribution, they need to be given in relation to each specific act that constitutes a violation of international law[68] and the instructions need to be carried out as such by those instructed. A general call for action or a general policy does not amount to instructions even if there is political alignment between the perpetrators of malicious acts and the policy. In the case at hand, ordering a campaign to influence the US elections does not amount to specific instructions addressed to particular persons and, moreover, does not in itself amount to instructions to commit unlawful acts. Consequently, related activities cannot be attributed to Russia on the basis of Article 8 ASR in a similar way that the DDOS attacks on Estonia by patriotic hackers cannot be attributed to Russia. If, hypothetically, specific and lawful instructions to influence the US elections were issued, unlawful acts incidental to the otherwise lawful acts of influencing the elections would be attributed to Russia but not those

---

[62] Article 8, ASRIWA; *James Crawford*, The International Law Commission's Articles on State Responsibility (2002), 110-113
[63] *Nicaragua*, paras 116-117; *Bosnia Genocide*, paras 398, 402-406, 413-414
[64] *Prosecutor v Duško Tadić a/k/a "DULE"* (Appeal) ICTY-94-1-A (15 July 1999), paras 131-137; Tallinn Manual 2.0, Rule 82 paras 3-8.
[65] *Bosnia Genocide*, para 406 but also see 404-5
[66] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION 1 (2017)
[67] Ibid, P1
[68] *Bosnian Genocide* para 400.

acts that went beyond what has been ordered. The latter will remain private acts, not attributed to Russia.[69]

Applying Article 8 ASR to China's acts of cyber theft, according to the 2013 Mandiant report 'Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support.'[70] In a different section, the report says that Unit 61398 acted with the 'full knowledge and cooperation of the Chinese government'.[71] The language used to describe the relation between Unit 61398 and China varies but state sponsoring perhaps alludes to 'overall control' which was rejected as a basis of attribution whereas direct governmental support perhaps alludes to 'effective control' and consequently attribution to China according to Art 8 ASR.

A related question is under what circumstances malicious acts by private Chinese corporations can be attributed to China in view of China's economic model which does not separate clearly between private and public enterprises or between state and commercial activities. Instead, a network of formal or informal links between enterprises and the state exists.[72] To this, one should also add China's broad concept of national security which also encompasses the economy.[73] It can be said that to the extent that privately-owned companies are dependent on the state and their decision-making process is controlled by the state, they are *de facto* organs according to Art 4 ASR and their malicious cyber activities will be attributed to China. In order to establish attribution on that basis, one needs to take into account the thick network of interactions between the state and the companies, the amount of funds received by the state, the number of management seats controlled by the state as well as

[69] ASR with Commentaries, p. 48

[70] Mediant, APT1 Exposing One of China's Cyber Espionage Units (2013), https://www.fireye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf Executive summary

[71] Mandiant ATP1, 59

[72] Li-Wen Lin and Curtis J. Milhaupt, "We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China," Stanford Law Review 65 (2013): 697; Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership: State Capitalism and the Chinese Firm," Georgetown Law Journal 103 (2015): 665, 668; The 'China, Inc.+' Challenge to Cyberspace Norms, Robert D. Williams Aegis Series Paper No. 1803, 69 https://www.hoover.org/sites/default/files/research/docs/williams_webreadypdf1.pdf

[73] National Security Law of the People's Republic of China, art. 2, adopted July 1, 2015, http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm

the number of shares controlled by the state.[74] If, instead, the private company is delegated to exercise governmental functions, its acts will be attributed to China according to Art 5 ASR.[75] If the company's functions only align with or just support China's policies, this is not a sufficient link to establish attribution according to the existing criteria neither is if China exercises 'overall control' over the company.

Another method of attributing conduct to a state is when a state acknowledges and adopts the particular conduct as its own.[76] Attribution in this case is not based on a contemporaneous and concomitant link between a state and a person or an act but on the subsequent endorsement by the state of the act committed by third parties.[77] Again, attribution requires a close link between the state and the act which is established through its approval which transforms the initially unattributable act into a state act. The approval needs to come from the highest level of government and should be clear and unequivocal.[78] For example, if a state acknowledges and adopts a cyber terrorist attack committed by ISIS, Article 11 will apply.

Would voluntary assumption of responsibility satisfy the attribution standard of Article 11? For instance, can the Stuxnet attack be attributed to Israel or to US since US and Israeli authorship of the attack was insinuated by undisclosed senior officials. [79] The answer is in the negative. In the first place, it was not a case of acknowledging and adopting an act committed by a third party which is the gist of Article 11 but of acknowledging an act committed by organs or agents of the acknowledging state. Secondly, the acknowledgement was not followed by adoption and thirdly it was not explicit. Had the Stuxnet attack been committed by third parties, Article 11 would apply only if the assumption of responsibility by the US or Israel was done by high level officials, was explicit and indicated adoption of the act and intent to accept legal responsibility.

In the preceding lines we reviewed the attribution criteria set out in the law of state responsibility and explained their application to cyber attacks. As indicated, the criteria cannot be fulfilled easily, and this leads to a legal void and to responsibility gaps. This state of affairs is not peculiar cyberspace. As international jurisprudence demonstrates, holding

[74] *Salini Case—Salini Costruttori SpA and Italstrade SPA v Kingdom of Morocco* ICSID Case No. ARB/00/4, Decision on Jurisdiction dated 16 July 2001, 42 ILM 609 (2003)
[75] Iran-United States Claims Tribunal, [Phillips Petroleum Co. Iran] v. Islamic Republic of Iran, Award No. 326–10913–2, 3 November 1987, Iran-United States Claims Tribunal Reports, vol. 21 (1989), p. 79, § 89
[76] Art 11 ASR
[77] ICJ, *Reports*, 1980, p. 35, para 74
[78] ASR 293
[79] David E Sanger, 'Obama Order Sped Up Wave of Cyberatacks against Iran', *New York Times*, 1 June 2012

states responsible for wrongful conduct is the exception than the rule because of difficulties in fulfilling the attribution criteria. The difficulties surrounding the normative standards of attribution are compounded by evidentiary difficulties. As the Russian presidential spokesman, Dmitry Peskov said the United States "should either stop talking about [Russia being responsible for the DNC hack] or produce some proof at last."[80] The next section discusses evidentiary issues associated with cyber attribution.

4 Type of evidence, standard of proof and burden of proof

In this section we will consider the question of what type of evidence is required to establish cyber attribution; what the appropriate standard of proof is and, finally, who has the burden of proof. Evidence is crucial because it can explain and justify determinations of attribution and also underwrite legal responsibility. Since questions of evidence are critical in court proceedings, we will examine these issues in the context of the ICJ. The ICJ as the primary judicial mechanism adjudicating on matters of state responsibility has deal with the issue of evidence for attribution purposes in the *Georgia v Russia* case[81] and the *Nicaragua* case where the Court recognised the difficulties in establishing attribution through evidence. As it said, 'the problem is not … the legal process of imputing the act to a particular State … but the prior process of tracing material proof of the identity of the perpetrator'.[82]

Type of evidence

In the absence of strict rules on evidence and on admissibility, the ICJ is open to any type of evidence furnished by the parties. In relation to cyber attribution, parties can thus submit documentary evidence such as cyber strategies, legislation, official reports or reports by independent bodies such as think-tanks, NGOs, as well as intelligence reports even if in redacted form.[83] They can also submit forensic, visual and digital evidence. The latter can include, but is not limited to:

- Malware samples
    - Compiler language

[80] Laura Smith-Spark, *Russia Challenges US to Prove Campaign Hacking Claims or Shut Up*, CNN (Dec. 16, 2016, 4:49PM), http://edition.cnn.com/2016/12/16/europe/russia-us-hacking-claims-peskov/index.html
[81] Case Concerning Application of the International Convention on the Elimination of all Forms of Racial Discrimination (Georgia v. Russian Federation) (Preliminary Objections) 2011, paras 51–3, 57–61, 81
[82] *Nicaragua Case* para 57.
[83] Roscini, M. 2015. Evidentiary issues in international disputes related to state responsibility for cyber operations. Texas International Law Journal. 50 (2), pp. 233-273

  - Programming language
  - Compile time
  - Libraries used
  - Patterns/ordering of execution events
  - Keyboard layout for malware creation
- Scripts and programs used on victim network or host (e.g. non-malware)
- IP addresses for C2
- Domain names for C2
- Registration info for infrastructure
- Payment info for infrastructure

Notwithstanding such lax approach to the type of evidence accepted by the Court, it is for the Court to assess the relevance and probative value of the submitted evidence.[84] According to an academic study, the factors it takes into consideration in its assessment are:

1. Source: whether the source of the evidence is independent from the parties and whether it has been corroborated;
2. Interest: whether the fact-finding in question has been carried out by a disinterested party;
3. Relation to events: whether the fact-finding is a direct observation of the events by someone who was present at the time or whether it is secondary information (or hearsay);
4. Method: whether the fact-finding was carried out in a methodologically sound manner;
5. Verification: whether the evidence has been previously cross examined or corroborated;
6. Contemporaneity: less weight will be given to evidence not prepared at the time when the facts occurred due to the Court's wariness of documents provided specifically for the case before the Court;
7. Procedure: whether the evidence has come before the Court in accordance with its Rules of Procedure.[85]

[84] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, [2005] I.C.J. 168, para 59; Pulp Mills Case para 168

Digital or technical evidence poses particular challenges to these criteria. Digital evidence is resource intensive and its probative value depends on its reliability which itself depends on verification and authentication. The reliability of cyber evidence may however be compromised by security or other restrictions imposed on the evidence or by the fact that the party that supplies the evidence does not want to reveal the underlying attribution technology. Yet, even if the technology is revealed, it may not be broadly accessible, something that can impact negatively on the external verification of the evidence. Under such circumstances cyber evidence will most probably be dismissed in view also of the Court's decision in the *DRC v. Uganda* case where it dismissed the relevance of certain internal military intelligence documents because they were unsigned, unauthenticated, or lacked explanation of how the information was obtained.[86] By way of contrast, in the *Tolimir* case the ICTY did not dismiss evidence in the form of satellite images provided by the US. The US provided the evidence on condition that no discussion is to be had 'relating to the technical or analytical sources, methods, or capabilities of the systems, organizations, or personnel used to collect, analyse, or produce these imagery-derived products'. [87] As was expected, the accused challenged the reliability of such evidence because 'no evidence was presented on their origin, the method of their creation, the manner of their editing, how to interpret them or whether they were delivered to the Prosecution in their original form or previously modified'. The reason the Trial Chamber did not dismiss that evidence[88] perhaps resides on the fact that it was able to establish the facts through other corroborating evidence. The ICJ also seems to accept or at least to not challenge unverified evidence which is corroborated by other evidence. However, corroborating evidence needs to be of a high value and the Court seems to be biased in favour of reports by International Organisations or independent bodies. It thus seems that reports by cyber security companies such as Symantec, McAfee, Mandiant (now FireEye) may be of a lower probative value in particular if the sources of their evidence are not revealed.[89] Moreover, their neutrality and the process according to which their reports are produced may be questioned. The fact that their reports are 'second-hand' accounts may also impact on their

---

[85] A Riddell and B Plant, *Evidence before the International Court of Justice* (British Institute of International and Comparative Law 2009, 192

[86] Armed Activities Case, paras. 125, 127–28, 133–34, 137

[87] ICTY, *Prosecutor v Zdravko Tolimir*, Case No IT-05-88/2-T, Trial Judgment, 12 December 2012 (Tolimir Trial Judgment') 67

[88]Tolimir Trial Judgment 68- 69

[89] Oil Platforms (Iran v. U.S.),Judgment, 2003 I.C.J. 161, para. 60

probative value. Regarding press reports of cyber incidents, they can be used illustratively as corroborating the existence of a fact but their probative value remains peripheral.[90] Also, press reports cannot in themselves establish public knowledge of an event but they can contribute to public knowledge depending on corroboration of facts through other evidence and on the diversification of the sources of information.[91] Regarding the Stuxnet attack for example, the incident was first reported by the New York Times with the rest of the press replicating the story. These press reports do not provide direct evidence of the incident or establish public knowledge of the incident since they derive from one source without any primary and direct evidence.[92]

This leads us to the next issue which concerns the probative value of single sourced evidence. This will be the case for instance when sensitive security matters are at stake which are not subject to public knowledge or when the technology supporting the evidence is not widely available. The Court treats with caution single sourced evidence[93] unless it is corroborated by other evidence but how the Court will deal with this issue in the cyber domain remains to be seen.[94]

A critical question in judicial determinations concerns the ability of judges to comprehend and assess complex technical evidence. The Court can appoint external experts, seek external expert advice,[95] request further information from the parties,[96] or request information from International Organisations[97] but the question remains as to whether judges have the technical expertise or specialised knowledge to scrutinise and probe expert opinion and evidence on their own merits, lest expert opinion substitutes judicial fact finding.[98] Related to this is the volume of evidence that can potentially be submitted to the Court. Technological developments such as social media can contribute to enormous increase in evidence overwhelming the Court if it is unable to distinguish relevant and reliable evidence which assists it to understand the fact and determine attribution from irrelevant one.

---

[90] Nicaragua case, para. 62; Armed Activities Case, para. 68; Bosnia Genocide Case, para. 357.

[91] Nicaragua case, para 63
[92] Nicaragua Case para 63
[93] Armed Activities Case para 61; Nicaragua case para 64
[94] Riddell and Plant, Evidence before the International Court of Justice 217
[95] Art 50 ICJ St
[96] Art 49 ICJ St
[97] Art 34(2) ICJ St
[98] See *Pulp Mills on River Uruguay (Arg. v. Uru.)*, 2010 I.C.J. 14, (dissenting opinion of Judge *ad hoc* Vinuesa) para 71 and ibid, Joint dissenting opinion of Judges Al-Khasawneh and Simma, para 4

Another problem is that cyber evidence is difficult to collect because it requires cross border investigations. For example, items such as malware and scripts are collected from victim systems residing in different jurisdictions, whereas items such as registration information for infrastructure used in a cyber campaign exist in databases of third parties that operate the Internet. In relation to this it should be noted that the Court has not dismissed illegally obtained evidence and it has taken 'a more liberal recourse to inferences of fact and circumstantial evidence' when evidence is under the control of the other party.[99] It seems that the Court's more relaxed approach to circumstantial evidence is an attempt to alleviate the burden on states to furnish evidence but, at the same time, it can also be viewed as an attempt to discourage violations of international law in the collection of evidence.

Circumstantial evidence includes surrounding political, economic or technical facts and circumstances which can reasonably establish the fact that needs to be proved. As the 2010 GGE report said 'The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence'.[100] What can count as circumstantial evidence is the geopolitical context within which the attack took place,[101] the political character of the victim, the beneficiaries of the attack, the apparent origin of the attack, the sophistication of an attack, the timing of the attack, the scale of the attack. For example, attacks on governmental services or on military infrastructure will most probably be deemed to be authored by adversary states as do large scale attacks or sophisticated attacks. As Kaspersky Lab opined with regard to Stuxnet, its 'sophistication, purpose and the intelligence behind it suggest the involvement of a state'.[102] If the geopolitical context is also taken into consideration, one can point the finger to certain states. That said, inferences from circumstantial evidence should be reasonable in light of some primary evidence.[103] In the *Nicaragua* case for example, circumstantial evidence indicated the level of US support to the Contras, but such evidence was not sufficient to prove US direction in the absence of hard

[99] *Corfu Channel Case* (*United Kingdom of Great Britain and Northern Ireland v Albania*) (Merits) [1949] ICJ Rep 4, 18; A Riddell and B Plant, *Evidence before the International Court of Justice* 112-113.
[100] 2010 GGE
[101] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington, DC: CCSA; The Atlantic Council, 2013), p. 21
[102] Clement Guitton and Elaine Korzak, 'The Sophistication Criterion for Attribution', *The RUSI Journal* 158, 4 (2013)
[103] *Corfu Channel*, Dissenting Opinion of Judge Badawi Pasha, para 59. See also *Case Concerning Application of the Convention on the Prevention and Punishment of Genocide* , Dissenting Opinion of Vice-President Al-Khasawhen, para 51.

evidence.[104] In light of this, neither Stuxnet nor the DDOS attacks on Estonia can be attributed to a state, just on the basis of circumstantial evidence.

Related to this is the question of whether adverse inferences can be drawn from the non-production of evidence or from a party's refusal to cooperate. According to Richard Clarke the United States should 'judge a lack of serious cooperation in investigations of attacks as the equivalent of participation in the attack'.[105] Drawing adverse inferences from non-cooperation or from non-disclosure of information is quite standard in political processes. One can recall here the 2003 Iraqi saga where the US and UK drew adverse inferences from Iraq's failure to provide them with the requested evidence as well as from its failure to co-operate with the UN inspectors. Such an approach can be contrasted to the Court's cautious approach on this issue.[106] In the *Bosnia Genocide* case for example the ICJ denied Bosnia's request to order Serbia to produce unredacted documents from the meetings of the Supreme Defence Council of Serbia, a decision that drew criticism even from within the Court. According to the critics, these documents might have provided evidence of the relation between FRY and Republika Srpska leading to attribution of the genocidal acts to Serbia. [107]

Finally, the fact that a state controls its cyberspace or is aware of previous cyber incidents emanating from its territory can also be relied upon as circumstantial evidence. For example, in the Teheran Hostages case knowledge of the attack was inferred from the fact that Iran was monitoring the situation around the embassy for security purposes.[108]

Standard of proof

In international jurisprudence, there is no uniform standard of proof[109] with the ICJ applying, depending on the circumstances, a variety of standards such as 'sufficient' evidence,[110]

[104] Nicaragua Case, para 111
[105] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), p. 178; Healey, 'Beyond Attribution'
[106] Bosnia Case paras 44, 204-6 *Corfu Channel Case* 32.

[107] Bosnia Genocide Case Dissenting Opinion of Vice-President Al-Khasawhen, para 35.
[108] Teheran Hostages Case, paras 64-5; See also *Corfu Channel* 19-20
[109] *Oil Platforms* case, para 189; Separate Opinion of Judge Higgins, paras 30-33; and Separate Opinion of Judge Buergenthal, para 41.

'conclusive' evidence[111] or 'beyond a reasonable doubt'.[112] That said, the Court requires a higher standard of proof for charges of exceptional gravity.[113] Against this background, what standard of proof would shroud judicial determinations of attribution with sufficient degree of confidence?

In order to answer this question, one needs to consider the rationale behind the standard of proof. In a narrow sense, the standard of proof underwrites correct decisions and protects parties against erroneous decisions. In a broader sense, the standard of proof and its different gradations serves societal policies. For example, the criminal law standard of 'beyond a reasonable doubt' is high because its aim is to protect individuals from erroneous convictions by recognising that in criminal law cases the parties are not equal and the consequences of convictions are serious.

Such a high standard is not however necessary in international law because responsibility is not criminal in nature and the parties to the dispute are legally equal. Furthermore, state responsibility is undifferentiated as far as its consequences are concerned with the possible exception of responsibility for violations of *jus cogens* norms which in principle engenders serious consequences and reputational costs.

In light of the above, it is submitted that the 'preponderance of the evidence' is the most suitable standard for attribution purposes. According to this standard, if the evidence presented by one party compared to the evidence presented by the other party demonstrates that attribution to the particular state is more likely to be true, the former will be deemed to have proven the case. This standard also recognises the equal footing of the parties and leads to equal distribution of the risk of erroneous decisions.

Regarding violations of *jus cogens* norms, the standard of "clear and convincing proof" should apply. That said, the application of this standard encounters the difficulty of identifying the *jus cogens* norms since jurisprudence on the matter is not settled. For example, whether the prohibition of the use of force is a *jus cogens* norm is debated.

---

[110] *Case Concerning Armed Activities on the Territory of the Congo* para 172; *Case Concerning Military and Paramilitary Activities in and against Nicaragua* para 110; *Oil Platforms* para 57.

[111] *Case Concerning Armed Activities on the Territory of the Congo* para 91; *Oil Platforms* para 71; *Case Concerning Application of the Convention for the Prevention and Punishment of Genocide* para 209.

[112] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* para 422.

[113] *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* paras 209-210.

With regard to the DNC hacking, Admiral Stavridis[114] wrote that if the United States were to use its own offensive cyber-tools to punish Russian hackers by knocking them off-line or even damaging their hardware, the burden of proof for attribution would be higher in that it would need definitive information on the command and control center that launched the hacking activity. What standard of proof is required in this case depends on whether damaging hardware amounts to a use of force. If it does not amount to a use of force or if the prohibition of the use of force is not a *jus cogens* norm as the authors claim, the standard of preponderance of evidence is the appropriate evidentiary standard but if the prohibition of the use of force is a *jus cogen*s norm, then 'clear and convincing evidence' will be needed. In both cases the applicable standard will be lower than the standard of definite evidence.

Burden of proof

The burden of proof refers to the question of whether it is the acting state that needs to provide evidence to substantiate its claim or whether it is the accused state that needs to disprove the claim. For example, is it for the US to prove Russian interference or for Russia to disprove the claim? International jurisprudence traditionally holds that the burden of proof falls on the party that makes a particular assertion.[115] The critical question here is whether the burden of proof should shift to the other party because of difficulties in collecting cyber evidence. It can be argued that the state that controls cyber infrastructure may be in a better position to furnish such evidence, but this is perhaps true with regard to certain states only. Moreover, if the burden of proof is to shift to the accused party, the opportunities for making spurious claims increase. The ICJ has not accepted the reversal of the burden of proof in such situations[116] but as was said it has relaxed the criteria concerning the type of admitted evidence.[117] The ICJ's position can be contrasted with political processes where the reversal

---

[114] James Stavridis, *How to Win the Cyberwar Against Russia*, FOREIGN POLICY (Oct. 12,2016), http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/

[115] *Case concerning Pulp Mills on the River Uruguay* (*Argentina v Uruguay*) (Request for the Indication of Provisional Measures) [2006] ICJ Rep 113, para 162; *Application of the Convention on the Prevention and Punishment of the Crime of Geno*cide , para 204; *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States of America*) (Jurisdiction of the Court and Admissibility of the Application) [1984] ICJ Rep 392, para 101; *Ahmadou Sadio Diallo (Republic of Guinea v Democratic Republic of the Congo), Merits, Judgment, I.C.J. Reports 2010*, p 639 at 660, para 54; *Application of the Interim Accord of 13 September 1995 (the former Yugoslav Republic of Macedonia v Greece),*
Judgment of 5 December 2011, I.C.J. Reports 2011, p 644 at 668, para 7

[116] *Case concerning Pulp Mills on the River Uruguay* , paras 162-164.

[117] *Fisheries Case* (*United Kingdom v Norway*) [1951] ICJ Rep 116, 138-139; *Nuclear Tests* (*New Zealand v France*) [1974] ICJ Rep 457, para 17

of the burden of proof is quite frequent and came to its heyday with regard to Iraq and the question of its WMD. [118]

What the preceding discussion has demonstrated is that international law is quite flexible as far as evidence is concerned. Parties can furnish any type of evidence and in the absence of a set standard of proof, the standard of preponderance of evidence emerges as the most appropriate for cyber attribution. The main evidentiary challenge facing cyber attribution is that of assessing the reliability of the furnished evidence.

5. Recommendations for improving the attribution process: establishing an international attribution agency and revising the attribution standards

In the preceding sections we have identified certain challenges associated with the attribution process associated to ts standards and the required evidence. In this section we will consider proposals for addressing these challenges. The first proposal envisages the establishment of an international attribution agency to centralise the investigation and communication of attribution and the second proposal envisages the revision of the attribution standards.[119]

The aim behind the establishment of an attribution agency is to depoliticise, streamline and regularise the attribution process and thus restore trust in attribution determinations. Blueprints range from an agency with purely private-sector membership, an agency with private-public membership or an international (inter-state) agency. [120] All proposals seem to stress the importance of independence, transparency, and equal geographic representation. These proposals also raise a number of important questions about membership, competence, decision-making, and accountability but it is not our aim to engage in a detailed assessment of such proposals. Our aim instead is to assess the contribution of the proposed agency to attribution determinations performed by the ICJ. As was said previously, the ICJ can appoint proprio moto an independent body to conduct enquiries or to provide expert opinion[121] in relation to cases under litigation and the proposed agency could in principle assist the ICJ with the investigation and interpretation of cyber evidence and with understanding complex

[118] CL Powell, Secretary of State, 'Remarks to the United Nations Security Council' (New York, 5 February 2003) <http://2001-2009.state.gov/secretary/former/powell/remarks/2003/17300.htm.

[119] Stateless Attribution (Rand 2017); Microsoft, From Articulation to Implementation: Enabling Progress on Cyber Norms https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8 Atlantic Council, Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf

[120] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI

[121] Art 50 ICJ St

technical evidence in view of the Court's lack of expertise and competence.[122] That said, the Court has utilised such external agencies very infrequently and the systematic use of such an attribution agency would require a change in the Court's culture. Yet, even if a cultural shift is to occur, the Court still needs to maintain its independence as the final arbiter of the facts and as the final arbiter of the law. If the proposed attribution agency acquires the authority envisaged by its promoters, the Court's function as the final arbiter of facts may be challenged particularly since the agency's findings will concern attribution which is one of the two constitutive elements of the law of state responsibility. Of course, it is for the Court to determine whether the legal criteria of attribution have been met or whether a state is responsible, but facts determine the outcome and in the absence of particular expertise by the Court, questioning the agency's findings will be quite difficult. Second, the time frame within which such an agency can produce its reports is critical for purposes of adjudication but equally if the agency is to play the role envisaged by its promoters. For example, the ATP1 report which attributed incidents of cyber theft to China took six years to be completed. Even if Court proceedings are quite slow, the Court would require a quicker report. On a more general level, long time-frames for producing reports will frustrate prospective political or legal action and for this reason states may bypass the agency or its reports. This brings us to the next critical point. The usefulness of such an agency ultimately depends on the willingness of states to cooperate, not only the litigant states but also third states since questions of cyber attribution may involve multiple jurisdictions. This is one of the most serious challenges facing proposals for the creation of an attribution agency. States want to retain their sovereign right to make independent decisions on attribution, to protect whatever information they deem necessary and to protect their cyber infrastructure from peering eyes. As the UK Advocate-General put it 'There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based, or to publicly attribute hostile cyber activity that it has suffered in all circumstances'[123] and, similarly, Brian Egan the former Legal Advisor to the State Department stated that 'there is *no* international legal obligation to reveal evidence on which attribution is based prior to

[122] Pulp Mills Case, Joint Dissenting Opinion of Judges Al-Kasawneh and Simma at para 8.

[123] Cyber and International Law in the 21st Century https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

taking appropriate action.'[124] Even within a more integrated organisation such as the EU it was made clear that **'**attribution to a State or a non-State actor remains a sovereign political decision.'**[125]** If state opposition is not overcome, the possibility of creating such an agency is rather remote whereas, even if such an agency is created, its effectiveness and authority will be considerably diminished.

The second proposal envisages the revision of the attribution standards for purposes of cyber attribution. As was noted, the attribution criteria are quite strict, and this inevitably produces a legal void either because the standards cannot be fulfilled or because they can be easily evaded. If attaching responsibility to non-state actors as independent legal persons or attaching responsibility to states without attribution[126] is not currently on the international law's agenda, and if law is to maintain its relevance as a governance tool, it is important to adjust the attribution[127] criteria to the more subtle modes of interaction between states and non-state actors in cyberspace. It should be recalled in this respect that the existing criteria were developed in an era where non-state actors were created by states to pursue their proxy wars abroad and they were dependent on states for material resources and direction. The existing criteria thus reflect such unequal and vertical relations between states and non-state actors but, currently, many non-state actors are self-sufficient and have more independent standing and agendas. Their relationship with states can also cover a wide spectrum ranging from shades of attachment to shades of detachment; from vertical to more horizontal relations; from continuous to more ad hoc relations. That said, non-state actors and states can still operate in tandem to pursue common goals. Against this background, it is not unreasonable to require a lower degree of state control over a non-state actor to establish. In contrast to the effective control standard which requires direct state input into the act committed by the non-state actor, the overall control test proposed by the ICTY lowers somewhat the required degree of control by looking holistically and cumulatively into state relations with non-stare actors. Such relations can be financial, organisational, material and political. Although, as was said the ICJ rejected the overall control criterion, there is no compelling reason to permanently exclude it from the alw of state responsibility. As a matter

[124] BJ Egan, International Law and Stability in Cyberspace, 35 Berkeley JIL (2017), 169, 177

[125] DRAFT COUNCIL CONCLUSIONS ON A FRAMEWORK FOR A JOINT EU DIPLOMATIC RESPONSE TO MALICIOUS CYBER ACTIVITIES ("CYBER DIPLOMACY TOOLBOX") Council of the European Union, 7 June 2017, para 4

[126] Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council Issue Brief (2011); Jason Healey, The Spectrum of National Responsibility for Cyberattacks, 18 Brown J. World Aff. 57 (2011)

[127] See also UK AG Cyber and International Law in the 21st Century https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

of fact the effective control criterion is a judicial invention and the Court acknowledged that different attribution criteria can apply in different areas of the law. Furthermore, Article 8 ASR does not qualify in any way the requisite standard of control and, as the commentary notes, this standard should apply with a degree of flexibility.[128] Moreover, official statements on attribution in cyberspace do not mention effective control. For example, Harold Koh the former Legal Advisor of the US Department of State spoke of sufficient degree of control. As he said, 'if a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act'.[129]

Even if the 'overall control' standard would somewhat relax the required degree of control, it is still a demanding criterion because of the scope of required state input into the activities of non-state actors. Yet, as was said, a non-state actor in cyberspace may not need financial support, training or material resources but may act in pursuance of a state's policy out of allegiance. In such a situation a *de facto* but *ad hoc* relationship of alliance between a state and a non-state actor can be established if the non-state actor manifestly acts in pursuance of state policies and the state implicitly or explicitly accepts this state of affairs. For example, if a group of patriotic hackers is engaged in operations to support a state's political causes and the state explicitly or implicitly accepts such actions, the acts of the group should be attributed to the state. As President Putin said recently "If they [hackers] are feeling patriotic, they will start contributing, as they believe, to the justified fight against those speaking ill of Russia."[130] With regard to patriotic hackers, the state may provide encouragement, communicate with them, influence them or guide them through signalling but it does not organise the attacks, there is no dependency and control and the state's overall input is below the overall control standard.[131] That notwithstanding, patriotic hackers align with and support state policies. The immediate question is on what basis such allegiance can be formed. The

[128] James Crawford, *The International Law Commission's Articles on State Responsibility* (CUP 2002) 112
[129] H Koh, 'International Law in Cyberspace' (United States Cyber Command InterAgency Legal Conference, Fort Meade, MD, 18 September 2012)5www.state.gov/s/l/ releases/remarks/197924.htm. Egan 177 and UKAG

[130] Putin concedes 'patriotic' hackers might target foreign elections
FT, June 1, 2017 https://www.ft.com/content/f607ac6c-46e6-11e7-8519-9f94ee97d996

[131] R. Hang, 'Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism' 5 Yale Review of International Studies (2014), 47

word 'patriotic' alludes to nationality or ethnicity but in our opinion religion can also be added as a basis of allegiance. This attribution standard based on the non-state actor's allegiance to the state and the state's acceptance of its activities to some extent expands the attribution rationale of Article 11ASR. It can however apply in relation to groups than individuals and indeed to groups that exhibit a degree of coordinated action.

We also propose a standard of constructive attribution. Constructive attribution would cover situations where a state does not have control over persons or conduct but has control over the circumstances that allow a wrongful act to be committed. For example, if a state is aware of the activities of non-state actors, fails to suppress their activities, refuses external support in this respect and such conduct is critical for the commission of a wrongful act, the wrongful act will be attributed to the state. Similar arguments were used by the US in relation to the 9/11 attacks to establish the responsibility of Afghanistan.[132] In relation to the Russian hacking of the DNC, Admiral Stavridis[133] wrote that under prevailing international law, if a nation has information of a nexus of offensive activity, has requested it to stop, and the offending nation declines to do so, that offensive center is liable for attack.'

6 Conclusion

What are the broader take-aways from the preceding discussion? First, the purpose and standards of attribution vary depending on context, domain and set of actors. Attribution can serve legal accountability by holding individuals or states accountable; it can serve power projection by highlight technical and political capability, as part of a broader strategic contest between states; it can serve policy prescription by formulating and enforcing norms and can serve protection by gaining insight into threat actors and improve protection against them.

Second, attribution is characterised by different degrees of certainty; it is not absolute or deterministic.

---

[132] UNSC 'Letter from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council' (7 October 2001) UN Doc S/2001/946; UNSC 'Letter from the Charge d'affaires ai of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council' (7 October 2001) UN Doc S/2001/947. See also Resolutions 1368 (2001) and 1373 (2001)

[133] James Stavridis, *How to Win the Cyberwar Against Russia*, FOREIGN POLICY (Oct. 12, 2016), http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/

Third, attribution is not an inevitability. States as indeed companies may or may not pronounce on attribution. Deciding whether to publicly attribute a cyber attack is complicated, non-standardized, and often the most challenging decision that a government has to make. There are thus key threshold questions of whether, why, when, and how to make an assertion and any decision is embedded in a larger strategic calculus.

Fourth, there are many benefits of shared public-private engagement on attribution either on an ad hoc basis or through an international agency. They include increased transparency and knowledge, allowing governments to better utilize sparse resources, and having a force multiplier for attribution. However, there are also limits to how extensively global companies are willing to be seen to work with (or against) particular governments but above all to what extent states are willing to abdicate themselves from sovereign decisions.

Fifth, the existing legal standards of attribution reflect more traditional forms of collaboration between states and non-state actors and cannot capture the more subtle ways of collaboration between states and non-state actors in cyberspace and the fact that non-state actors are prominent in cyberspace. Therefore, the attribution standards need to be revisited in order for law to maintain its relevance as a governance tool.

Sixth, evidentiary rules need to be revisited in order to support than to frustrate reasonable determinations on attribution.

Seventh, it should be accepted that when we move away from technology to governance neither the law nor the technology nor the politics can single-handily solve the problem of attribution but attribution should be treated as a synthetic and synergetic process; each process (technical, political, legal) deals with aspects of attribution which feed into the other but establishes attribution according to its own techniques and rationale.

Therefore, a single holistic regime of attribution is unlikely to emerge in the near future. What is needed is to understand the rationale, techniques, artifacts that each process is employing and also understand the aims and the context behind the attribution process. Technical attribution must be based on data that can be shared and processes that can be peer-reviewed. As for the law, it should not withdraw from cyberspace but face and shape cyber reality.