TALLINN PAPERS

Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva,
Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe

Opportunities for Public and Private Attribution of Cyber Operations

TALLINN PAPERS YOUNG SCHOLAR EDITION

This issue is the outcome of Indiana University Cybersecurity Risk Management Programme Capstone Project 2020. CCDCOE seeks to help empower upcoming voices in the cooperative cyber defence community by providing a supportive forum for young cyber defence specialists and relevant educational endeavours to share their ideas and build networks.

Tallinn Paper No. 12
2021

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Previously in This Series

No. 1 Kenneth Geers “Pandemonium: Nation States, National Security, and the Internet” (2014)

No. 2 Liis Vihul “The Liability of Software Manufacturers for Defective Products” (2014)

No. 3 Hannes Krause “NATO on Its Way Towards a Comfort Zone in Cyber Defence” (2014)

No. 4 Liina Areng “Lilliputian States in Digital Affairs and Cyber Security” (2014)

No. 5 Michael N. Schmitt and Liis Vihul “The Nature of International Law Cyber Norms” (2014)

No. 6 Jeffrey Carr “Responsible Attribution: A Prerequisite for Accountability” (2014)

No. 7 Michael N. Schmitt “The Law of Cyber Targeting” (2015)

No. 8 James A. Lewis “The Role of Offensive Cyber Operations in NATO’s Collective Defence” (2015)

No. 9 Wolff Heintschel von Heinegg “International Law and International Information Security: A Response to Krutskikh and Streltsov” (2015)

No. 10 Katrin Nyman Metcalf “A Legal View On Outer Space and Cyberspace: Similariteis and Differences” (2018)

No. 11 Elaine Korzak “Russia’s Cyber Policy Efforts in the United Nations” (2021)

Disclaimer

The Tallinn Papers

The NATO CCDCOE's Tallinn Papers are designed to inform strategic dialogue regarding cyber security within the Alliance and beyond. They address cyber security from a multidisciplinary perspective by examining a wide range of issues, including cyber threat assessment, domestic and international legal dilemmas, governance matters, assignment of roles and responsibilities for the cyber domain, the militarization of cyberspace, and technical. Focusing on the most pressing cyber security debates, the Tallinn Papers aim to support the creation of a legal and policy architecture that is responsive to the peculiar challenges of cyberspace. With their future-looking approach, they seek to raise awareness and to provoke the critical thinking that is required for well-informed decision-making on the political and strategic levels.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by invitation, proposals dealing with issues of strategic importance and acuteness will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org

Opportunities for Public and Private Attribution of Cyber Operations

Garrett Derian-Toth,[1] Ryan Walsh,[2] Alexandra Sergueeva,[3] Edward Kim,[4] Alivia Coon,[5] Hilda Hadan[6] and Jared Stancombe[7]

Abstract

State-sponsored cyber-attacks have altered the playing field of international conflict and espionage because these operations often fall below the established threshold of response and regularly target private infrastructure. This has created difficulties for victim nations and their private sector entities regarding how to attribute a state-sponsored offensive cyber operation and what role each party should play in the attribution process. More broadly, the attribution of state-sponsored offensive cyber operations affects more than just cybersecurity. Rather, there is a relationship between attribution of offensive cyber operations and international relations where attribution is used for purposes such as reinforcing rules in cyberspace and imposing costs on malicious actors. Offensive cyber operations and attributions are used to shape a state's global policy and posture and can reflect generations of conflicts, allegiances and intelligence-sharing networks. This paper gives an overview of the motivations, tools, techniques, procedures and alliances of attribution of state-sponsored offensive cyber operations. For the purposes of this article, attribution is defined as creating a body of evidence or a claim publicly linking a state to an offensive cyber operation. Along the way, the limitations of attribution, the general legal framework, norms regarding attribution and alternatives to attribution are examined. Our research reveals a fragmentation among actors regarding attitudes towards attribution and information sharing. We have also identified factors that reflect positive outcomes for attribution, including developing cyber norms, increasing the role of private sector actors and evolving laws that actively prevent cyber interference. Our findings are supported by a dataset that tracks state-sponsored offensive cyber operation attribution.

Introduction

International conflict and competition have increasingly taken place in cyberspace, joining kinetic operations. The United States Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent network of

[1] J.D., Cybersecurity Law & Policy Certificate, class of 2021, Maurer School of Law, Indiana University, Garrett.m.dt@gmail.com.

[2] Cybersecurity Risk Management class of 2021, Indiana University, ryandwalsh44@gmail.com.

[3] Cybersecurity Risk Management class of 2020, Indiana University, asergueeva@hotmail.com.

[4] J.D., Cybersecurity Risk Management class of 2021, Indiana University, ekim180@gmail.com.

[5] Cybersecurity Risk Management class of 2020, Indiana University, alicoon@iu.edu.

[6] M.S. of Informatics, Indiana University, Cybersecurity Risk Management class of 2020, hhadan@iu.edu.

[7] Cybersecurity Risk Management class of 2020, Indiana University, jared.stancombe@gmail.com.

information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers."[8]

Within this domain, offensive cyber operations have evolved to include cyber espionage and interference with critical infrastructure or democratic processes through cyberspace. As such, this paper defines an offensive cyber operation as, "[t]he employment of [harmful] cyber capabilities [against an external target] to achieve objectives in or through cyberspace."[9]

State-sponsored offensive cyber operations have become widely recognised following several recent events beginning with the 2007 attacks on Estonia, the 2014 Sony Entertainment breach and in the wake of Russia's election interference in the 2016 US election. Offensive cyber operations have an asymmetric cost structure, meaning that threat actors can often execute the same offensive cyber operation on thousands of targets at once, while the targets must defend against every type of attack themselves.[10] The mix of asymmetry of costs and the relatively low operational cost of offensive cyber operations enables countries that were historically unable to compete in kinetic warfare to be highly competitive in cyberspace. These factors also enable countries such as North Korea or Iran to use offensive cyber operations to thrust themselves onto the world stage through highly sophisticated targeted operations.[11]

As offensive cyber operations have grown in scale and frequency, perpetrators have increasingly been unmasked by both public and private actors through public attribution. For the purposes of this paper public attribution is defined as the public release of strategic, technical and operational information to support an assertion that a state or state-sponsored organisation has engaged in an offensive cyber operation. This should not be confused with attribution as a general term for ascribing responsibility or blame, but rather as a specific term for ascribing responsibility and blame to a state for their role in a cyber operation. This information is then used by states to pursue political, economic or legal paths to impose a cost on the culpable adversary. These could be economic sanctions, criminal indictments, diplomatic actions, or military or intelligence actions. Exploring the nuances of publicly attributing state-sponsored offensive cyber operations is the focus of this discussion.

This discussion begins by examining international norms in cyberspace. Attribution is inherently political and the lack of norms and standards surrounding attribution ultimately adds to the politicisation and hinders an attribution's credibility. Attribution trends between NATO countries and countries outside NATO are examined, showing that an increased density of traditional alliances, intelligence sharing agreements and aligned incentives correlate with coordinated attributions. Further, countries having strong private sectors, and strong partnerships between public and private sector actors, correlated with more successful attributions in both qualitative

---

[8] 'Department of Defense Dictionary of Military and Associated Terms' (DoD, June 2020) <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> accessed 11 Nov 2020.

[9] Michael N. Schmitt, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (Cambridge University Press, 2 Feb 2017) <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 17 May 2021 (Tallinn Manual 2.0). The definition is an amended citation of the Tallinn Manual 2.0 Glossary Definition of the term Cyber Operation.

[10] Gregory Conti, 'Why Haven't we 'Solved' Cybersecurity?' (Federal News Network, 12 Aug 2020) <https://federalnewsnetwork.com/commentary/2020/08/why-havent-we-solved-cybersecurity/>, accessed 11 Nov 2020.

[11] Jenny Jun, Scott LaFoy and Ethan Sohn, 'North Korea's Cyber Operations' (Center for Strategic and International Studies, Dec. 2015) <https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf> accessed 11 Nov 2020.

and quantitative terms.[12] Next, we discuss what leads to successful attributions, the limitations of attribution and alternatives to it such as active defence and the offensive elements of cyber deterrence. Ultimately, one option is through the development of evidentiary standards and a Transnational Attribution Institution. Through these two developments, attribution's political pitfalls can be mitigated and stability in cyberspace improved, increasing international security and stability more broadly.

As much as possible, our findings are reflected by our attribution dataset. This dataset was created using attribution data from the CFR Cyber Operations Tracker dataset which identifies state-sponsored offensive cyber operations from January 2015 to March 2020.[13] The CFR dataset is in English, so some publicly attributed state-sponsored offensive cyber operations may not be reflected. However, this dataset is the most comprehensive collection of state-sponsored offensive cyber operations publicly available. Our analysis focuses on the state of attribution based solely on data that is publicly available, thus this was the best available resource.

Attribution, Stakeholders and Strategy

Public attribution of state-sponsored offensive cyber operations is complex and has political, technical and legal aspects. States can use attribution as a vehicle to advance their political goals, but there is often a risk involved in making a public attribution.[14] Any response from the attacked party, such as attribution or a hack-back, must be carefully considered before being undertaken due to the political implications that such a response would cause. Another consideration that attributors must address is what evidence to present when making the claim. This evidence includes technical, operational and strategic information known as indicators,[15] and the amount of evidence presented varies with each attribution. Attributing with limited evidence can leave others to question whether the attributor has identified the real perpetrator. Publishing too much evidence can convince the international community that the attributor has identified the correct actor, but it can also reveal classified sources and methods. Finally, national and international laws and norms must be negotiated. International law provides the basic rules of attribution, such as which acts are attributable to a nation-state, codified into the Draft Articles on the Responsibility of States for Internationally Wrongful Acts.[16] However, state-sponsored offensive cyber operations usually fall under the use of force and thus into a grey area where international law is still developing.

---

[12] Our Dataset. Authored by Alexandra Sergueeva and Hilda Hadan, reflects public attributions of Nation State-Sponsored Offensive Cyber Operations from January 2016 through March 2020. Available at <https://github.com/hilda93hadan/Cyber-Attack-Attribution-Data>.

[13] Council on Foreign Relations, 'Tracking State-Sponsored Cyber attacks Around the World' (Council on Foreign Relations, Aug 2020) <https://microsites-live-backend.cfr.org/cyber-operations> accessed 11 Nov 2020.

[14] Clingendael Netherlands Institute of International Relations, 'Foreign Policy Responses to International Cyber-attacks' (September 2015) <https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf> accessed 11 Nov 2020.

[15] Brian Bartholomew and Juan Andres Guerrero-Saade, 'Wave your False Flags' (Virus Bulletin Conference, October 2016) <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf> accessed Nov 11 2020.

[16] International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' (November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1) <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf> accessed 25 May 2021 (Draft Articles on State Responsibility). Analysis of the applicability to cyberspace is documented also in Tallinn Manual 2.0.

Attributing a state-sponsored offensive cyber operation is thus a political act that depends on the victim state's strategic goals, cyber-related norms and international and national laws. Adding to the complexity, states are not the only actors in the attribution space; industry maintains a continually growing presence in the attribution of state-sponsored offensive cyber operations and brings with it a different set of standards, goals and potential for collaboration.

2.1 Cyber-related Norms and Attributing Trends

Since the establishment of the United Nations Group of Governmental Experts (UN GGE) in 2004, the general outlines of internationally acceptable cyber norms have been laid. In 2013, the GGE agreed that international law and the UN charter applied to state activity in cyberspace.[17] In 2015, it agreed to eleven non-binding norms,[18] including that: (1) states should not interfere with the critical infrastructure of other states; (2) they should not target Computer Security Incident Response (CSIR) teams; (3) they should assist other nations to investigate offensive cyber operations; and (4) they should not knowingly allow their territory to be used for internationally wrongful acts using [Information and Communication Technologies] ICTs.[19]

Unfortunately, the process of establishing broad, internationally accepted cyber norms has recently fragmented.[20] After a failure to achieve consensus at the 2017 GGE session, Russia established an alternative norms-creating forum known as the Open-Ended Working Group (OEWG) which began holding meetings in 2019.[21]

The failure of the 2017 session centred around states' rights.[22] The representative from Cuba argued that the proposed adoption of these concepts would 'legitimise unilateral punitive force actions, […] by States claiming to be victims of illicit uses of ICTs.ICTs',[23] while the US representative countered that states 'who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace

[17] Council on Foreign Relations, 'The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?' (Council on Foreign Relations, 20 Jun 2017) <https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what> accessed 11 Nov 2020.

[18] Council on Foreign Relations, 'The First Even Glocal Meeting on Byber Norms Hold Promise, But Broader Challenges Remain' (Council of Foreign Relations, 30 Sep 2019) <https://www.cfr.org/blog/first-global-meeting-cyber-norms> accessed 11 Nov 2020; see also UN, 'Efforts to Implement Norms of Responsible State Behavior in Cyberspace , as Agreed in UN Group of Governmental Expert Reports of 2010, 2013 and 2015' <https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf> accessed 22 Nov 2020.

[19] Ibid.

[20] Shannon Vavra, 'World Powers are Pushing to Build their own brand of cyber norms' (Cyberscoop, 23 Sep 2019) <https://www.cyberscoop.com/un-cyber-norms-general-assembly-2019/> accessed 11 Nov 2019.

[21] Ibid.

[22] Declaration by Miguel Rodriguez, representative of Cuba, at the final session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York, June 23, 2017 <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf> accessed 27 July 2021.

[23] Ibid.

[…] with no limits or constraints on their actions'.[24] Most international scholars and commentators saw that political motivations on both sides had made consensus unachievable.[25]

Despite this divergence of perspective, the substantive session of the GGE in December 2019 remained optimistic about the potential for cooperation[26] and highlighted the 'opportunity for countries that have been less engaged on the issue of ICT-security in the context of international security to join the conversation'.[27]

Applying these trends to attribution, the vast majority of attacks and subsequent attributions have followed similar ideological trends. For example, in the data surveyed,[28] China, Russia, Iran and North Korea have been identified as the responsible actors for 75% of all state-sponsored offensive cyber operations.

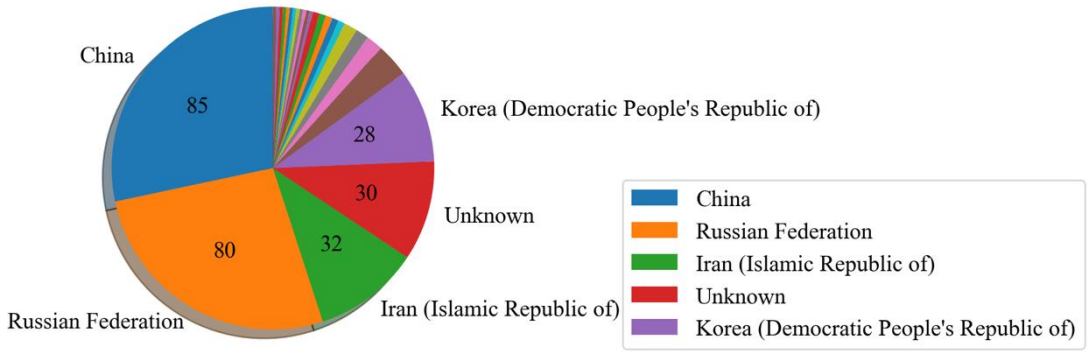

Figure 1. Public Attributions of State-Sponsored Offensive Cyber Operations, by Nation-State Sponsor 2015-2020

Our research has found that offensive cyber operation attributions are made primarily by small groups of nations. The US government and US private sector are the number one attributors of state-sponsored offensive cyber operations. While the US stands out as the most prolific attributor, its traditional allies often align when making attributions. For example, the Five Eyes community, an intelligence-sharing alliance consisting of the US, UK, Australia, Canada and New

[24] Michele G. Markoff, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, New York City, June 23, 2017 <https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/> accessed 22 Nov. 2020.

[25] Henriksen (n 22); See also Eneken Tikk 7 Mika Kerttunen, The Alleged Demise of the UN GGE: An Autopsy and Eulogy (2017), <https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf>.

[26] United Nations, 'Collated summaries of the regional consultations of the GGE' (United Nations, Dec. 2019), <https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf> accessed 22 Nov. 2020. By the time of publishing this paper, the GGE has successfully submitted a consensus report. Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security. Advance copy, <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf> accessed 03 June 2021.

[27] Ibid.

[28] Our Dataset (n 12).

Zealand, has made the most public attributions to date, most notably coming together to denounce Russia for several offensive cyber operations in 2016 and 2017.[29]

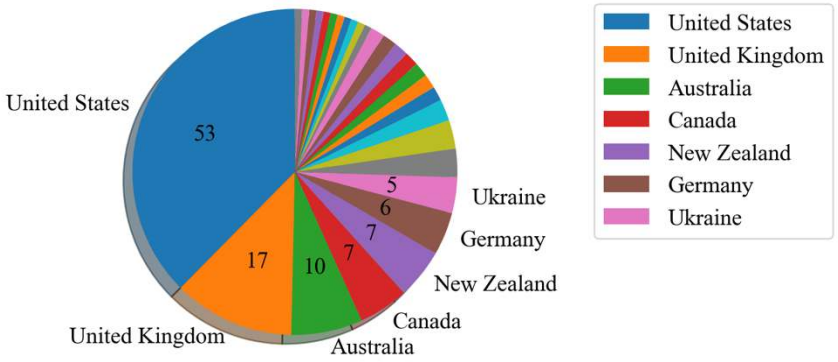

Figure 2. Public Attributions of State-Sponsored Offensive Cyber Operations, by Attributing Country 2015-2020

2.2 Parties in the Attribution Process

Parties to the attribution process can be national or transnational. However, the most energetic dynamic to date has been between public and private entities. The public sector has traditionally been at the forefront of attribution, but the private sector has repeatedly demonstrated its ability to independently attribute state-sponsored offensive cyber operations.[30] Our data indicates that 25% of attributions are sponsored by only public attributors, 65% by private actors and 10% by both. While public entities are typically executive agencies charged with intelligence, law-enforcement or defence, private sector entities include private companies that were subject to attack, private-cybersecurity firms and news outlets which choose to publish particular attributions.

A government's decision to attribute a state-sponsored offensive cyber operation may come from policy shifts. For example, in 2018, the Trump administration sought to enhance the cyber capabilities of the US and to take a harder line with North Korea, leading to the WannaCry ransomware attribution.[31] Germany and the US took a similar initiative when China began its campaign of intellectual property theft from western industrial countries.[32] Aside from policy shifts, the public sector has attributed offensive cyber operations to ensure the security of elections,

[29] National Cyber Security Centre, 'Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed' (3 Oct 2018) <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> accessed 11 Nov 2020.

[30] Sasha Romanosky and Benjamin Boudreaux, 'Private-sector Attribution of Cyber Incidents' (Feb 2019) International Journal of Intelligence and Counterintelligence <https://www.rand.org/pubs/external_publications/EP68257.html> accessed on 11 Nov 2020.

[31] Thomas P. Bossert, 'It's Official: North Korea Is Behind WannaCry' (Wall Street Journal, 17 Dec 2017), <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537> accessed 11 Nov 2020; Office of the Inspector General, 'Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation', (Dec 2019) <https://www.justice.gov/storage/120919-examination.pdf> accessed 11 Nov 2020.

[32] The White House, 'Annual Intellectual Property Report to Congress' (March 2020) <https://www.whitehouse.gov/wp-content/uploads/2020/04/IPEC-2019-Annual-Intellectual-Property-Report.pdf> accessed 16 Nov 2020.

such as in the 2016 DNC hack.[33] Additionally, when a large number of countries, private companies and people are victims of an attack, such as was the case in NotPetya, governments attribute an attack to deter future attacks by imposing sanctions or by holding those who perpetrated the attack criminally liable.[34]

Where public actors primarily attribute to promote national security and political goals, private actors have a more diverse array of incentives, including but not limited to profit-motives, self-marketing, and moral reasons.[35] For example, private cybersecurity firms are often hired by attacked entities to perform cyber investigations into compromised systems. Private firms use attribution reports generated by these investigations to showcase their products, generate buzz and help market services such as 'threat intelligence'.[36]

Given the complexity and political nature of attributing state-sponsored offensive cyber operations, some have voiced concerns over the private sector's involvement in the attribution space[37] and conflicting attributions and misattribution from poorly sourced or analysed information can confuse and the situation.[38] These effects could pressure a government to attribute publicly when it would rather take a more nuanced approach or strain international relations when tensions are already high. However, unlike public actors who must weigh the costs of unwanted escalation, strained diplomacy and deal with information sharing barriers like classification, private actors are unconstrained and can quickly combine information from various sources into a publication much more quickly.[39]

Public-sector attribution also carries specific benefits over private sector attribution. Only a sovereign government can formally charge entities with crimes, levy sanctions, expel diplomats and respond with proportionate actions up to the use of armed force, if justified. Domestic criminal charges and international extradition treaties allow government attributions to carry more weight, such as in the case of North Korea's WannaCry or China's OPM hack.[40] This is an extension of domestic criminal law to encompass and punish transnational crime. A recent example of this was the 2018 extradition of Yanjun Xu, a Chinese intelligence official, from Belgium to the US for prosecution.[41] However, due to the lack of extradition treaties with Russia or China and the principle of sovereign immunity, this policy has had mixed results.[42] A second benefit the public

---

[33] Report of The Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf>.

[34] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyber attack in History' (WIRED, 22 Aug 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 11 Nov 2020; Lauren Cerulus, EU Sanctions Russian Hackers for 2015 Bundestag Breach (Politico, 2020) <https://www.politico.eu/article/eu-sanctions-russias-fancy-bear-hackers-for-2015-bundestag-breach/>.

[35] Romanosky and Boudreaux (n 29)

[36] Sasha Romanosky, Private Sector Attributions of Cyber Attacks: A growing concern for the US government? (2017) https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government accessed 11 Nov 2020.

[37] Ibid.

[38] Ibid.

[39] Ibid.

[40] Office of the Director of National Intelligence, 'A Guide to Cyber Attribution' (14 Sep 2018) <https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf> accessed 11 Nov 2020.

[41] Katie Benner, 'Chinese Officer Extradited to United States to Face Charges of Economic Espionage' (New York Times, 10 Oct 2018), <https://www.nytimes.com/2018/10/10/us/politics/china-spy-espionage-arrest.html> accessed 11 Nov 2020.

[42] The sheer number of major attacks shows little to no deterrence from the application of domestic laws internationally. *See* Center for Strategic & International Studies, 'Significant Cyber Incidents' (Aug 2020) <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents> accessed 11 Nov 2020

sector enjoys is evidentiary. The public sector is in the best position to acquire evidence through international agreements, intelligence agencies and subpoenas. Finally, nation-states may choose to attribute an attack in bulk by harnessing existing relationships and alliances to give their attribution more weight, such as the Five Eyes or NATO states.

Several benefits have been observed through a strong private sector and a strong partnership between the public and private sectors. For example, allowing the private sector to work with the public sector can help leverage the private sector's technical capabilities. A private-public partnership has been seen in nearly every state-sponsored offensive cyber operation attribution.[43] A public-private relationship can also help add validation to the public sector's attribution, which can add political strength to that attribution. Private sector attribution can sway governmental discussions or agency deliberations, help the public sector avoid giving up intelligence sources and methods, free up resources for the public sector and help build relationships between the public and private sectors.[44]

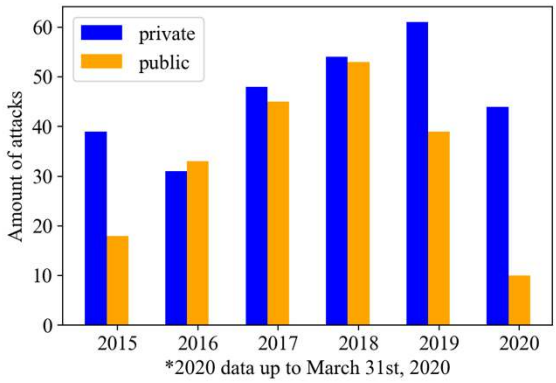

Figure 3. Public Attributions of Nation-State Sponsored Offensive Cyber Operations, by Public and Private Actors 2015-2020

2.3 Factors Leading to Successful and Risks of Attributions

The goal of attribution is to deter future offensive cyber operations by 'naming and shaming' the aggressor on the international stage. Aside from a decrease in the frequency or intensity of offensive cyber operations targeted at the victim state, measuring which outcomes make an attribution successful can be difficult.

Unsurprisingly, private sector attributors measure successful attributions by traditional business metrics. These include the extent to which it leads to the accomplishment and continuation of business objectives, increased profits, or enhanced reputation, 'informing the broader community

[43] Bossert (n 30).

[44] Romanosky and Boudreaux (n 29).

of network defenders' of threats and vulnerabilities and the promotion of 'broader corporate policy and normative agenda'.[45]

For the public sector, a successful attribution is measured by whether or not the political goal of the attribution was achieved. That could be the promotion of deterrence, informing network defenders, promotion of norm-building, or as a 'prerequisite for other punitive actions'.[46] For example, if a state attributes a cyberattack to justify a military response, then the opinion of the international community, the evidentiary standards and the opinion of the state's own citizenry of that justification will be the measure of the success of the attribution.

Information sharing networks between attributing stakeholders can help to reduce information asymmetries. For example, information sharing between entities can help develop understanding of commonly known APT strains such as Cloud Hopper from China[47] or the Lazarus Group from North Korea.[48] However, attribution carries risks. Threat actors can use this shared intelligence to adapt their own tactics, techniques and procedures (TTPs).[49] An example of this is the Olympic Destroyer malware, where it is still unclear whether the attack was launched from North Korea or Russia, because it contains malware used by both Fancy Bear and the Lazarus Group.[50] Threat actors can also use information such as the technical indicators of compromise and attack tactics to prepare new attacks. For example, there is evidence that China and other actors learned from and adapted Russia's election interference techniques and used these techniques to interfere in the 2020 US election.[51] Some of the techniques used by Russia could be found in the US Department of Justice indictments,[52] and it is likely that actors like China and others have studied these techniques and adopted them into their own toolset, which improved their capabilities.

Information sharing of incomplete research can lead to misattribution or the media sensationalising false information. An example of these pitfalls occurred during the CyberCaliphate false flag hack.[53] During that operation, the hack was first misattributed to Iran. However, further enquiries by FireEye found that the attack was a clever false flag operation from Sofacy, a Russian state-sponsored cyber group that masqueraded as a group from Iran to shift

---

[45] Sasha Romansky and Benjamin Boudreaux, 'Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government' (Feb 2019) RAND National Security Research Division <https://www.rand.org/pubs/external_publications/EP68257.html> accessed 23 Nov 2020; Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks' (2015) The Journal of Strategic Studies <https://ridt.co/attributing-cyber-attacks/> accessed 23 Nov 2020.

[46] Ibid.

[47] PwC, 'Operation Cloud Hopper' (PwC, Apr 2017) <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf> accessed 11 Nov 2020.

[48] GReAT, 'Lazarus Under The Hood' (SecureList, 3 Apr 2017) <https://securelist.com/lazarus-under-the-hood/77908/> accessed 11 Nov 2020.

[49] Bartholomew and Guerrero-Saade (n 15).

[50] Kaspersky Team, 'Olympic Destroyer: who hacked the Olympics? (Kaspersky Daily, 9 Mar 2018) <https://www.kaspersky.com/blog/olympic-destroyer/21494/> accessed 11 Nov 2020.

[51] 'Interference 2020: Foreign Interference Attribution Tracker (Beta). A Project of the Digital Forensic Research Lab (DFRLab) of the Atlantic Council' accessed Nov 2020.

[52] Department of Justice, 'Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election' (DOJ, 13 July 2018) <https://www.justice.gov/archives/opa/gallery/grand-jury-indicts-12-russian-officers-hacking-offenses-related-2016-election#:~:text=Deputy%20Attorney%20General%20Rosenstein%20announced,the%202016%20U.S.%20presidential%20election.> accessed 30 Nov 2020.

[53] FireEye Threat Intelligence, 'Hacking the News: Global News Media Firms and Small Market Outlets In' (FireEye, 2 Jun 2015) <https://www.fireeye.com/blog/threat-research/2015/05/hacking_the_newsgl.html> accessed 11 Nov 2020.

suspicion.[54] Sensationalist media reporting can also spread incomplete information. For example, an unattributed cyberattack in Austria was blamed on Russia by media pundits; however, this attribution was later recanted.[55] Russia's response and the pushing of incomplete information highlight the inherent nature of false flag operations and the risks these pose to attribution. It is hard to know how many of these operations have been identified and how many achieved their goal of misidentification or no identification. Nonetheless, these incidents seem to be rare and nation-states typically have the same response to attribution, no matter who the attributor is, calling them 'baseless accusations'.

Attributors should consider current political tensions and trends when attributing. When Canada's Citizens' Lab released an article attributing a spyware attack to Saudi Arabia,[56] the Saudi government retaliated by threatening retaliation and launching a social media campaign telling Canada to stay out of other countries' affairs.[57] One image posted on social media during this time was a plane flying into Toronto's CN Tower,[58] likely meant to be taken as a threat. The situation did not escalate beyond online threats, but these did end up putting a strain on Canada's relationship with Saudi Arabia and, by extension, their Middle Eastern allies.

Lastly, the limitations of using domestic law against APT-level actors, the lack of broad international treaties, the lack of consensus on how international laws apply and opaque definitions and standards have led to several unwelcome outcomes: (1) a *de facto* acceptance of offensive cyber operations that fall below the threshold use of force;[59] (2) the responsibility mechanism for states often being the prosecution of individuals rather than nation-states; and (3) a trend of loose coalitions of international actors based around existing intelligence, military or political alliances which trace, attribute and respond to offensive cyber operations. A legal attribution framework could resolve many of the issues discussed in this section and mitigate most risks.

In light of these risks, and despite differences between attributors and their interests, several factors have been identified which can strengthen an attribution. First, accuracy is important; attributions must accurately attribute the specific offensive cyber operation to the correct actor.[60] Misattributing an offensive cyber operation can lead nation-states to rely on false information when retaliating against the misattributed party, creating international turmoil. For example, if the act was attributed wrongfully and countermeasures were taken against a wrong state, the victim

---

[54] FireEye Threat Intelligence, Hacking the News: Global News Media Firms and Small Market Outlets In the Crosshairs of Cyber Threat Groups (FireEye, 2 Jun 2015) <https://www.fireeye.com/blog/threat-research/2015/05/hacking_the_newsgl.html> accessed 30 Nov 2020.

[55] Gareth Corfield, Austrian foreign ministry, 'State actor' hack on government IT systems is over (The Register, 14 Feb 2020) <https://www.theregister.com/2020/02/14/austria_foreign_ministry_hack_turla_group_allegs/> accessed 30 Nov 2020.

[56] Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak and Ron Deibert, 'The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil '(CitizenLab, 1 Oct 2018) <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/> accessed 11 Nov 2020.

[57] Ashifa Kassam and Kareem Shaheen, 'Saudi critics jab Canada on Twitter and TV as diplomatic feud deepens' (The Guardian, 9 Aug 2018) <https://www.theguardian.com/world/2018/aug/09/saudi-linked-twitter-accounts-troll-canada-over-human-rights-amid-row>.

[58] Ashifa Kassam, 'Saudi group posts photo of plane about to hit Toronto's CN tower amid Canada spat'' (The Guardian, 8 Aug 2018) <https://www.theguardian.com/world/2018/aug/07/saudi-arabia-canada-toronto-cn-tower-9-11-photo-apology> accessed 11 Nov 2020.

[59] Public-Private Analytic Exchange Program, 'Commodification of Cyber Capabilities' (Department of Homeland Security, 2019) <https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf> accessed 11 Nov 2020.

[60] Kristen Eichensehr, 'The Law and Politics of Cyber attack Attribution' (15 Sep 2019) 67 UCLA L. Rev. 520.

state itself will have committed an internationally wrongful act.[61] Therefore, for the long-term reputation of the attributor and the attribution process in general, the attribution must be accurate. To ensure that it is, attributors should find support for their conclusions in verifiable evidence.

To ensure public acceptance and legitimacy, the attribution itself must be efficiently disseminated to the public through trusted sources. These include private sector threat reports, high-level public sector statements, public sector technical releases, public sector intelligence assessments, criminal indictments and even sometimes government leaks reported by the media or other trusted sources.[62]

Additional factors have been identified to aid in improving successful attributions for both public and private entities. These include: strong public and private partnerships; strong information-sharing networks between nation-states; potential for repercussions such as sanctions or hack backs to prevent attacks; having a well-cultivated private sector; attributing an attack in concert with other countries to create more impact; relatively little time elapsing between attack and attribution; the attributor having a strong reputation; and existing public sector and private sector information-sharing networks.[63]

These factors alone cannot 'fix' attribution because cyberspace lacks standards and norms, making an attribution inherently political and subjective. With this in mind, developing specific cyber-related norms would lead to increased outcomes of attributions.

2.4 Law and Transnational Institutions

Although issues remain, technical attribution has evolved to a sufficient degree to meet the challenge of tracking and tracing attackers[64] and the parallel development of legal standards would create certainty and clarity.[65] Public attribution remains a political decision, but it still must follow applicable International or domestic regulations and legal standards. Attributions resulting from a legal process have greater legitimacy, leading to a study of tactics and methodologies, pose a threat of retaliation, allow implementation of countermeasures and produce norms for appropriate behaviour.[66] To that end, the two approaches put forward are an agreed burden of proof standard and stateless attribution.

---

[61] United Nations, 'Responsibility of States for Internationally Wrongful Acts' (2001) <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf> accessed Feb 2021.

[62] Romansky and Boudreaux (n 44)

[63] Eichensehr (n 59); Rid and Buchanan (n 44); Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (Sept 2016) Hoover Institution <https://www.hoover.org/research/attribution-malicious-cyber-incidents-soup-nuts-0> accessed 23 Nov 2020.

[64] Delbert Tran, 'The Law of Attribution: Rules for attributing the source of a cyber-attack' (Yale Journal of Law & Technology, 2018), < https://yjolt.org/law-attribution-rules-attributing-source-cyber-attack > accessed 11 Nov 2020.

[65] Ibid. '*The real question . . . is how to create a legal system with sufficient rules of evidence and procedure to legitimize its legal judgments identifying a party as the cause of a cyber-attack*'.

[66] Ibid.

Regarding evidentiary standards, attribution does not require absolute certainty.[67] Only a sufficient evidentiary burden needs to be met, as in all legal determinations.[68] Examples of types of evidence include the narrowness of the target, the resources required by the attacker, the context and technical indicators.[69] What is missing are the evidentiary procedures that allow for the formation of legal judgments.

There is no explicit international law on the standard of proof in attribution[70] and the amount of evidence required varies significantly in each case.[71] For example, in 2018, the US Central Intelligence Agency (CIA) reported with 'high confidence', that Russian military intelligence (GRU) created Notpetya,[72] and the UK claimed that the Russian military was 'almost certainly' responsible.[73,74] Further development of the evidentiary standard may arise from future cyber sanctions, especially since the European Union (EU) recently established a sanctions regime for cyberattacks.[75] The EU utilised this facility for the first time in July 2020,[76] although it was careful not to conflate sanctions with official state attribution.

Scholars have suggested tuning evidentiary burdens to the severity of the response, whether political, economic or military.[77] For example, an economic sanction might only require a preponderance of the evidence (51%), while the justified use of military force might require proof beyond reasonable doubt (99.9%). This sliding scale approach has been hinted at by the International Court of Justice (ICJ),[78] endorsed by the Tallinn Manual 2.0 and described by

---

[67] Office of the Director of National Intelligence, 'A Guide to Cyber Attribution' (14 Sep 2018) <https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf> accessed 11 Nov 2020

[68] Tran (n 63), *'..[Q]uestions of responsibility are rarely decided solely through a single technological tool or form of evidence and judgments of responsibility often do not turn on smoking-gun declarations of guilt'.*

[69] Office of the Director of National Intelligence, 'A Guide to Cyber Attribution' (14 Sep 2018) <https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf> accessed 11 Nov 2020.

[70] Ibid, *'The United States has taken the position that in the absence of explicit international law on the standard of proof, 'international law generally requires that States act reasonably under the circumstances*'.

[71] Ibid.

[72] Shannon Vavra, 'Russia behind NotPetya cyberattack in Ukraine, CIA concludes' (Axios, 15 Jan 2018) <https://www.axios.com/russia-behind-notpetya-cyberattack-in-ukraine-cia-concludes-report-1515853877-d7677367-9e2a-49a9-ba74-ec2c0a46299f.html> accessed 11 Nov 2020.

[73] United States Department of The Treasury, 'Treasury Sanctions Russian Cyber Actors for Interference with the 2016 United States Elections and Malicious Cyber-Attacks' (Mar 2018) <https://home.treasury.gov/news/press-releases/sm0312> accessed 11 Nov 2020.

[74] National Cyber Security Centre, 'Russian military 'almost certainly' responsible for destructive 2017 cyber attack' (14 Feb 2018) <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> accessed 11 Nov 2020.

[75] Adam Botek, 'European Union establishes a sanction regime for cyber-attacks' (CCDCOE, May 2019) <https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks> accessed 11 Nov 2020.

[76] Samuele De Tomas Colatin, Si vis pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action, CCDCOE <https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/> accessed 24 Nov. 2020; See Press Release, EU imposes the first ever sanctions against cyber-attacks, Counsil of the EU (30 July 2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/#> accessed 24 Nov 2020.

[77] See Tran (n 63) '*One can easily imagine, for instance, that laws for attribution could change their standards of strictness or flexibility based on the severity of the sanction imposed on the state against whom an attack is attributed. . . . Generally, a preponderance of the evidence standard fits the goals of attribution . . . [but] [i]n cases where a military strike is proposed or threatened as a countermeasure, the law of attribution should ratchet its burden of proof to the reasonable-doubt standard.'*; See also Eichensehr (n 59).

[78] See Case Concerning Application of the Convention on the Prevention & Punishment of the Crime of Genocide (Bosnia & Herzegovina v. Serbia & Montenegro), 2007 I.C.J. 47, 130 (Feb. 26, 2007) para. 210 (noting that when a state is accused of genocide 'the Court requires proof at a high level of certainty appropriate to the seriousness of the allegation'); see also Netherlands Letter, supra note 111, at 7 ('Under international law there is no fixed standard concerning the burden of proof a state must meet for (legal) attribution and thus far the International Court of Justice has accepted different standards of proof'.).

academics from Yale, UCLA and the University of Westminster.[79] Further development and acceptance of this sliding scale approach by an international tribunal like the ICJ or group of aligned states may be the logical first step.

Some worry that requiring a specific level of proof for an attribution might increase the costs for developing nations and have the effect of decreasing the total number of attributions.[80] However, these concerns are met with the promise of higher quality attributions, increased clarity of international norms, fostering transparency into states actions and decreasing the number of 'trust me' attributions.

The absence of standard methodology to investigate evidence has led to confusion, suspicion and a request for greater transparency. To mitigate these concerns, one solution would be institutionalising transnational attribution or stateless attribution. Stateless attribution aims to legitimise the attribution process by increasing uniformity and decreasing the politicisation of attributions by having a third-party attribute offensive cyber operation. Stateless attribution in the form of a Transnational Attribution Institution (TAI), as suggested by several scholars,[81] could serve as a neutral global platform in which to perform authoritative public cyber-attributions.[82] In taking the attribution out of the hands of states, the 'TAI would be an independent entity or set of processes whose attribution decisions would aspire to be widely perceived as *unbiased, legitimate and valid,* even among parties who might be antagonistic (such as rival nation-states)'.[83] Microsoft, the Atlantic Council, the Rand Corporation and the Council on Foreign Relations have all produced research on this issue.[84] There are significant challenges to the creation and legitimate functioning of a TAI, including how to staff it with credible experts.

However, the TAI should not be the sole body conducting attribution on the international stage. A TAI could be created most closely in the image of the International Atomic Energy Agency (IAEA). This certifying authority would have two foundational functions. First, a TAI could provide a certification decision on whether an attribution met the evidentiary standard based on a sliding scale burden of proof. Second, a TAI could provide a certification decision on whether, based on the evidence presented, the correct conclusion was reached in the attribution. A TAI constituted this way would bring with it a host of positives. It could create and solidify an evidentiary standard

---

[79] Tallinn Manual 2.0; Eichensehr (n 59); Tran (n 63); Marco Roscini, Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations (June 30, 2014). Texas International Law Journal, Vol. 50, p. 233, 2015.

[80] Eichensehr (n 59).

[81] See Kristen E. Eichensehr, The Law & Politics of Cyberattack Attribution; Karl Grindal, Brenden Kuerbis, Farzaneh Badii and Milton Mueller, 'Is it Time to Institutionalise Cyber-Attribution?' (Georgia Tech Internet Governence Project, 21 August 2018) <https://www.internetgovernance.org/research/is-it-time-to-institutionalise-cyber-attribution> accessed 11 Nov 2020.

[82] Karl Grindal, Brenden Kuerbis, Farzaneh Badii and Milton Mueller, 'Is it Time to Institutionalise Cyber-Attribution?' (Georgia Tech Internet Governence Project, 21 August 2018) <https://www.internetgovernance.org/research/is-it-time-to-institutionalise-cyber-attribution> accessed 11 Nov 2020.

[83] Ibid.

[84] Scott Charney, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze and Paul Nicholas, 'From Articulation to Implementation: Enabling Progress on Cybersecurity Norms'. (Mircrosoft, Jun 2016) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8> accessed 11 Nov 2020; Jason Healey, Klara Tothova Jordan, Nathaniel V. Youd and John C. Mallery, 'Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security'. (Atlantic Council. November 2014) <https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf> accessed 11 Nov 2020; John S. Davis II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern and Michael S. Chase, 'Stateless Attribution: Toward International Accountability in Cyberspace'. (RAND Corporation, 2017) <https://www.rand.org/pubs/research_reports/RR2081.html> accessed 11 Nov 2020; Elena Chernenko, Oleg Demidov and Fyodor Lukyanov, 'Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms'(Council on Foreign Relations, 23 Feb 2018) <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms> accessed 11 Nov 2020.

for attribution. It would improve the legitimacy of attributions and the ability for attributions to lead to successful redress for victims. It would improve consensus around the perpetrator of an attack and reduce the perpetrator's ability to deny. It would democratise attributions and be open to all willing states, regardless of their political system. Additionally, a TAI would bring clarity and enforceability to insurance coverage disputes, data breach cases and liability protection proposals and justify responses. Beyond these foundational principles, if it were also constituted in a way that would allow it to expand on these principles as needs around norms developed, it would have staying power as an international organisation.

Even a TAI constituted this way would encounter roadblocks. States would still be hesitant to share sensitive data and to outsource key international relations functions. Most likely leading to any TAI becoming at best a supplemental option to the existing mechanisms of public attribution. Ultimately, the addition of a TAI could lead to a general improvement in international cybersecurity norms and standards leading to a more ordered and safer world.

2.5 Alternatives to Public Attribution

When a nation-state learns that they are subject to an offensive cyber operation, public attribution may not follow. For various reasons, a nation-state can choose to internally attribute, bilaterally attribute, or not to conduct an attribution investigation at all. For example, when the cost to investigate and publicly attribute a cyberattack exceeds the perceived benefit, the state may pursue alternatives to public attribution. The costs associate with investigating are not trivial and can be divided into three types: economic costs, opportunity costs and political costs. The economic costs involve the financial costs of the required technology and human capital required to perform an attribution. A country seeking to perform an attribution may not have the technical expertise within its government to perform the forensic analysis of a cyber operation. Also, they may not have the budget or the technical tools to support an attribution effort.

The opportunity costs of attribution relate to how time and resources could have been used, or what is given up by conducting an attribution. For example, 'fixating on the threat group behind the attack takes time, energy and resources away from performing the practical measures that are necessary to keep the organisation's network secure'.[85] It is a resource-limited world and, in a world where cyber operations happen constantly, using resources to defend against the next or current cyber operation may be more important than finding out who was responsible for the previous one.

The political costs may involve revealing sophisticated attribution capabilities, such as publicising information that could allow adversaries to gain insight into both the attributor's technical and espionage capabilities. Public attribution of cyber operations could also place states at risk of retaliatory action. States could wrongfully attribute an attack to an innocent third party, which could lead to consequences that could complicate diplomatic relations or increase tensions.

[85] Brandon Levene, 'The Attribution Trap: A Waste of Precious Time & Money' (Dark Reading 31 July 2019) <https://www.darkreading.com/threat-intelligence/the-attribution-trap-a-waste-of-precious-time-and-money/a/d-id/1335353> accessed 28 February 2021.

These constraints may inhibit the ability of a state to publicly attribute a malicious cyber operation, and prevent it from accomplishing its foreign policy or national security goals.

a) Internal Attribution

While some states may have sophisticated forensic tools, mature intelligence capabilities and strong relationships with allies that allow for the sharing of intelligence, they may choose not to publicly attribute a cyber operation to an adversary. Instead, they may choose to exploit their cyber capabilities to gain an advantage over their adversary through acts of espionage or by conducting covert cyber operations against them while maintaining plausible deniability. For example, US strategies like 'persistent engagement' and 'defending forward' use sophisticated intelligence and military capabilities to gain insights into an adversary's capabilities and seek to gain a competitive edge, which are then exploited for strategic advantage.[86]

States may choose internal attribution when the benefits of a public attribution are low and traditional means of deterrence by punishment are ineffective. Economic sanctions, criminal indictments and other forms of political retaliation may not deter the adversary. Publicly attributing an attack could result in retaliatory action such as further cyber operations or damaged foreign relations with that country, particularly if a third party is wrongfully attributed.[87] For example, in 2013 the DoD clearly stated that the Chinese were directly responsible for attacks spanning the globe as the US Department of Homeland Security published Internet Protocol (IP) addresses linked to the Chinese military and the national security adviser made a public statement about China's cyber efforts in stealing US intellectual property. All this was done before the summit between President Obama and Prime Minister Xi intended to decrease tensions between the two countries.[88] Finally, states may choose not to divulge the evidence used to justify the attribution, as it could potentially compromise their own intelligence and cyber sources, methods and capabilities.[89]

b) Bilateral Attribution

While public attribution seeks to 'name and shame' as a means of deterring adversaries, others seek to use bilateral attribution to deter cyber operations using diplomatic leverage.[90] Bilateral attribution involves a victim state using diplomatic channels to attribute a cyber operation against the alleged perpetrator state.[91] This has been a popular alternative to public attribution used by France, which has taken the position that it does not need to publicly disclose the information used to attribute a cyber operation to an adversary.[92] The Netherlands has taken a similar stance.

---

[86] Michael P. Fischerkeller, Richard J. Harknett, 'A Response on Persistent Engagement and Agreed Competition' (Lawfare, 27 June 2019) <https://www.lawfareblog.com/response-persistent-engagement-and-agreed-competition> accessed 1 December 2020.

[87] Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age (PublicAffairs 2015) [pp. 158-159].

[88] Ibid.

[89] Tran (n 63).

[90] Arthur P. B. Laudrain, 'France's New Offensive Cyber Doctrine' (Lawfare, 26 February 2019) <https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine> accessed 1 December 2020.

[91] François Delerue, Alix Desforges and Aude Géry, 'A Close Look At France's New Military Cyber Strategy' (War On The Rocks, 23 April 2019) <https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/> accessed 1 December 2020.

[92] Laudrain (n 89).

France, however, is increasingly moving towards public attribution as it builds its cyber capabilities, engages with allies and shifts its strategy towards enforcing cyber norms.[93] A state may pursue bilateral attribution if it traditionally conducts foreign policy through formal diplomatic channels or if it lacks the capabilities to pursue deterrence by punishment through criminal indictments, economic sanctions, or offensive cyber capabilities.

c) No Attribution

Another alternative to attribution is to choose not to pursue an investigation of a cyber operation, but rather to use the forensic artefacts collected to pursue active defence strategies instead of attribution. These could include hacking back or using data such as the IP addresses of command-and-control servers, URLs found in the static analysis of malware code or other indicators that could allow a victim to retaliate against an unknown adversary's infrastructure to either recover stolen data or disrupt or destroy their capabilities. Another alternative could be to use these artefacts and indicators to increase the costs of future attacks by sharing threat intelligence, investing in cybersecurity infrastructure and sharing information with allies through deterrence by denial strategy.

Hacking back carries political, economic, and legal risks. For this reason, many countries prohibit private companies from hacking back. In the United States, for example, there are no legal protections for unauthorized hacking back; rather the US Computer Fraud and Abuse Act (CFAA) prohibits any 'unauthorised access' to a computer, 'unauthorised transmission' of things like malware, or actions that damage protected computers or networks.[94] Thus, accessing the aggressor's computer or network without authorisation will cause potential criminal penalties. Domestic law may provide entities, such as law enforcement or intelligence agencies, a legal basis to conduct hack backs. Under international law, states are free to engage in whatever activities, provided they do not violate any international wrongful act.[95] Therefore, the fact that international law does not provide a norm permitting hack back activities has little relevance. Rather, it has to be asked, whether there is a norm that forbids it.

Second, hacking back could significantly increase the risks of retaliation by the aggressor, potentially causing collateral damage which could include civilian systems.[96] Third, enabling hacking back has the risk of unintended collateral damage when states pursue revenge attacks in cyberspace.[97] Lastly, the possibility of mistaken attribution leads to the risks of harming an innocent third party, given that attackers can leave fake clues such as spoofed IP addresses to mask their origins.[98]

---

[93] Kristen Eichensehr, 'Cyberattack Attribution and International Law' (JustSecurity, 24 July 2020) <https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/> accessed 1 December 2020.

[94] Office of Legal Education, Prosecuting Computer Crimes (OLE Litigation Series, 14 January 2015). <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf> accessed 1 December 2020.

[95] Draft Articles on State Responsibility (n 15).

[96] Robert Chesney, 'Hackback Is Back: Assessing the Active Cyber Defense Certainty Act' (Lawfare, 14 June 2019) <https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act> accessed 1 December 2020.

[97] Ibid.

[98] Robert Anderson, Brian Lum and Bhavjit Walha, 'Offense vs. Defense' (University of Washington, 11 December 2005) <https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/OffenseVsDefense.pdf> accessed 1 December 2020.

Conclusion

Attribution is the necessary first step in the justification of any kind of response to a cyber operation. The success of attribution is grounded in the goal of the attribution, which changes depending on the attributing actor. In comparing private and public sector attribution, a strong private sector and a strong public and private-sector partnership lead to better outcomes. Attribution trends between NATO and non-NATO countries show that an increased density of traditional alliances, intelligence sharing agreements and aligned incentives correlates with a greater likelihood of coordinated attribution. Lastly, the application of international law to cyberspace is a work in progress and creating evidentiary standards around attribution should be the next step. The creation of a Transnational Attribution Certification Institution is a worthy longer-term goal.

Limitations to attribution do exist. Attackers can plant false flags, misattribution can occur and attribution can lead to a rise in tension or even to conflict. Active defence is the main alternative to attribution. While alternatives exist, attribution is currently the best first response and can be a successful response to state-sponsored offensive cyber operations and deter future ones. By harnessing public-private partnerships, collective attributions drawing on existing alliances, developing evidentiary standards for attribution now, producing a TAI in the future, correctly attributing the state responsible and ensuring the goals for attribution are just and achieved, attribution can be effective now and improved in the future.