

---

# Cyber Attribution: Technical and Legal Approaches and Challenges

Nicholas Tsagourias\* and Michael Farrell\*\*

## Abstract

*Considering the role of attribution in the law of state responsibility, this article examines the technical and international law methodologies and determinants used when attributing malicious cyber activities falling below the use-of-force threshold to a state, and identifies the challenges that arise which lead to responsibility gaps. The article goes on to discuss a number of proposals that aim to improve the effectiveness of the attribution process and also close some of the existing responsibility gaps. They include institutional proposals envisaging the creation of an international attribution agency; normative proposals advocating the revision of the legal determinants of attribution; and proposals concerning the standard of proof. The aim of the article is to reconstruct the theory and practice of cyber attribution in order to enhance the regulatory potential of international law in this area.*

## 1. Introduction

Modern societies are increasingly dependent on digital technology and infrastructures; for this reason, malicious cyber operations can cause serious harm to individuals, industry and states. Such harm can be physical, digital, economic, societal, political, psychological, reputational, it can affect security, or be a combination of all of these factors. For example, the cost of cybercrime is reported to be between US\$799 billion and US\$22.5 trillion globally,<sup>1</sup> whereas the US government estimated the cost of malicious cyber activities to its economy to be between US\$57 billion and US\$109

\* Professor of International Law at the University of Sheffield and Director of the Sheffield Centre for International and European Law, UK. Email: [nicholas.tsagourias@sheffield.ac.uk](mailto:nicholas.tsagourias@sheffield.ac.uk).

\*\* Co-Executive Director of the Institute for Information Security & Privacy, Georgia Institute of Technology, USA. Email: [michael.farrell@iisp.gatech.edu](mailto:michael.farrell@iisp.gatech.edu).

This article was prepared as part of a project on Protecting Civilian Institutions and Infrastructure from Cyber Operations: Designing International Law and Organizations, carried out by the Center for International Law and Governance at the Fletcher School of Law and Diplomacy, with financial support from Microsoft Corporation and the Hitachi Center for Technology and International Affairs.

<sup>1</sup> Dreyer et al., 'Estimating the Global Cost of Cyber Risk: Methodology and Examples', RAND (2018), available at [www.rand.org/pubs/research\\_reports/RR2299.html](http://www.rand.org/pubs/research_reports/RR2299.html).

billion in 2016.<sup>2</sup> These are dazzling figures, but even small-scale malicious cyber operations can cause serious and long-term harm. For example, tampering with even one voting machine can delegitimize the entire electoral process.

Individuals, industry and states thus have an interest in preventing and suppressing malicious cyber operations,<sup>3</sup> in mitigating or redressing the harm they cause and, eventually, holding those responsible to account. Attribution is critical in this context because it refers to the process of assigning a particular malicious act to its author: the physical perpetrator, but even more importantly, the mastermind.<sup>4</sup> Attribution therefore acts as a catalyst for taking appropriate and effective technical and legal action to prevent and suppress such activities and to establish responsibility. Conversely, non-attribution undermines the process of assigning responsibility and frustrates response action.

This article will study the legal methodologies and determinants involved in the process of attributing to states malicious cyber operations falling below the use of force and armed attack thresholds as a prerequisite for engaging their responsibility. The discussion is confined to the law of state responsibility because attribution is one of its constitutive elements and because the function of the law of state responsibility is to maintain international legality by holding states responsible for their wrongful acts.<sup>5</sup>

Before doing this, the article will set out the technical methodologies and determinants of attribution, because technical attribution supports, and interacts with, legal attribution, even if the respective methodologies, determinants and goals differ. To explain, technical attribution is about the forensic investigation of a malicious cyber incident to identify the origins of an attack platform, and it underwrites technical decisions and actions to patch vulnerabilities and prevent further attacks, whereas legal attribution is about the legal determination of ‘who did it’ on the basis of defined legal criteria in order to ascribe legal responsibility and initiate legal action. Although

<sup>2</sup> Executive Office of the President of the United States, The Council of Economic Advisers, ‘The Cost of Malicious Cyber Activity to the U.S. Economy’ (February 2018), available at [www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf](http://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf).

<sup>3</sup> The paper uses the phrases ‘cyber operation’, ‘cyber-attack’ and ‘cyber incident’ interchangeably to describe malicious acts below the use of force or armed attack thresholds.

<sup>4</sup> Tsagourias, ‘Cyber Attacks, Self-Defence and the Problem of Attribution’, 17 *Journal of Conflict and Security Law (J. Conflict & Security L.)* (2012) 229, at 233. See also Lin, ‘Attribution of Malicious Cyber Incidents: From Soup to Nuts’, 70 *Columbia Journal of International Affairs* (2016) 75; Clark and Landau, ‘Untangling Attribution’, *Harvard Law School National Security Journal* (2011), available at <https://harvardnsj.org/2011/03/untangling-attribution-2/>.

<sup>5</sup> International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts (2001) Art. 2 (‘ARSIWA’); J. Crawford, *The International Law Commission’s Articles on State Responsibility: Introduction, Text and Commentaries* (2002), at 81–83; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, 26 February 2007, ICJ Reports (2007) 43, paras 179, 379, 385 (‘Bosnia Genocide Case’). As the EU notes: ‘attribution to a State or a non-State actor ... should be established in accordance with international law of State responsibility’: see Council of the European Union, General Secretariat of the Council, ‘Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities’, Doc. No. 9916/17, 7 June 2017, Annex, para. 4, available at <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> (‘Cyber Diplomacy Toolbox’).

technical attribution can provide many clues about the author of a malicious cyber attack, it is not sufficient in itself to hold a state legally responsible unless the legal determinants of attribution are also satisfied.<sup>6</sup> For instance, technical attribution may identify as the source of a cyber attack a threat actor related to a state; however, the cyber attack will not be attributed to that state as a matter of law if the threat actor is not linked to that state according to the legal criteria or if she acted in her private capacity in that instance. Moreover, although legal attribution relies on forensic evidence produced by technical attribution in order to make determinations and justify legal action in the form of indictments, sanctions or countermeasures, forensic evidence needs to be interpreted and assessed according to legal criteria. The article will thus explore the dynamic interaction between the two processes, identify challenges and consider proposals to improve the international law methodology and determinants of attribution in order to make attribution more effective and close some of the responsibility gaps that currently exist.

This article will proceed as follows. Section 2 will discuss the current state of attribution of malicious cyber operations to states and identify their trends. Section 3 will discuss the methodologies and indicia of technical attribution. Section 4 will consider the legal methodology and determinants of attribution and apply them to certain cyber incidents in order to reveal the responsibility gaps to which they give rise. Section 5 will discuss the types of evidence – including technical evidence – and the standards of proof used in international law to establish attribution and will seek to reveal the legal uncertainty surrounding these issues. The article will then proceed in Section 6 to discuss proposals for improving the legal methodology and, eventually, the effectiveness of attribution. More specifically, it will discuss institutional proposals envisioning the creation of an international attribution agency but will conclude that, at this point in time, it is neither desirable nor feasible to create such an agency. It will then consider a number of normative proposals with a view to revising the legal determinants of attribution. Specifically, it will discuss looser thresholds of control in the form of ‘overall control’ and ‘soft control’ and will introduce ‘implicit instructions’ as an attribution determinant. These normative proposals can capture more effectively the dynamics of cyberspace, the prominent role of non-state actors as vectors of malicious cyber operations<sup>7</sup> and the multifaceted interactions between non-state actors and states. Thus, they will assist in closing many of the responsibility gaps that currently exist. Finally, the article will propose the ‘preponderance of evidence’ as the most appropriate standard of proof in cases of cyber attribution because it ensures proper scrutiny of the available evidence without unreasonably obstructing attribution determinations. It is hoped that the article’s key findings and proposals will contribute to improving the methodology and practice of attribution in cyberspace

<sup>6</sup> As Novetta stated in its Sony report, it is unable to determine via technical malware analysis whether or not the attack was carried out by an identified nation-state: see Novetta, ‘Operation Blockbuster: Unravelling the Long Thread of the Sony Attack’ (2016), at 13, available at [www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf](http://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf).

<sup>7</sup> They are referred to as Advanced Persistent Threat (APT) actors.

and enhance the ability of international law to regulate this area and to hold states responsible.

## 2. The Current State of Attribution of Malicious Cyber Operations to States

Attribution in cyberspace has traditionally been presented as a challenge because of anonymization, the falsification of identities, the multi-stage nature of cyber operations, the dynamic landscape of cyber threats, the undifferentiated nature of cyber tools, the human and technical resources required in performing attribution and the lengthy timescales involved. State attribution has been even more challenging for the same reasons but also because of the serious political and legal consequences that attribution or misattribution may trigger. However, the initial rarity of state attributions gradually gave way to ever more frequent attribution claims as a result of improvements in attribution capabilities coupled with the changing attitudes of states towards state attribution.<sup>8</sup> Although we are not going to examine all of these attribution claims in this section, we will highlight certain important features they reveal about the attribution process which will provide some of the context to the discussion that follows.

The first feature relates to the actors involved in attribution, which include governments, civil society<sup>9</sup> and the private sector, working separately or in collaboration.<sup>10</sup> For example, one of the first and most influential attribution reports by a private company was by Mandiant (now FireEye) which named Unit 61398, a unit within the People's Liberation Army (PLA), as being the host of 'Advanced Persistent Threat 1' (APT1), which was linked to acts of cyber espionage. According to the report, '[t]he issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage'. The report then noted that 'it is time to acknowledge the threat is originating in China'.<sup>11</sup> Since then, there has been a substantial increase in attributions of cyber operations to states by private sector companies. Regarding state-to-state attributions, the first took place in 2014 when

<sup>8</sup> See, e.g., Council on Foreign Relations, 'Cyber Operations Tracker: Timeline', available at [www.cfr.org/interactive/cyber\\_operations#Timeline](http://www.cfr.org/interactive/cyber_operations#Timeline) (last visited 10 June 2020). According to research by Georgia Tech's Internet Governance Project, between 2016 and the first quarter of 2018, 85% of the reported incidents were publicly attributed, of which 15% were attributions made by governments. See Mueller et al., 'Cyber Attribution: Can a New Institution Achieve Transnational Credibility?', 4 *Cyber Defense Review* (2019) 107, at 111–112.

<sup>9</sup> Citizen Lab, 'Tracking *GhostNet*: Investigating a *Cyber Espionage* Network' (29 March 2009), available at <https://issuu.com/citizenlab/docs/iwm-ghostnet>.

<sup>10</sup> According to the US National Cyber Security Strategy, '[t]he United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities ...': see The White House, 'National Cyber Strategy of the United States of America' (2018), at 21, available at [www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf](http://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf).

<sup>11</sup> Mandiant Intelligence Center, 'APT1 Exposing One of China's Cyber Espionage Units' (19 February 2013), at 6, available at [www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf](http://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf).

the US government publicly attributed the Sony attack to North Korea.<sup>12</sup> Since then, there have been many more state-to-state attributions, including coordinated ones, such as when the USA, UK, Australia, Canada, New Zealand and Japan attributed WannaCry to North Korea;<sup>13</sup> the UK, USA, Denmark, Australia, Canada and New Zealand attributed NotPetya to Russia;<sup>14</sup> or when the UK and allies attributed the activities of APT10 involving theft of intellectual property and sensitive data in Europe, Asia and the USA to the Chinese Ministry of State Security.<sup>15</sup> There have also been coordinated state and private sector attributions, such as when US government agencies<sup>16</sup> and the private security company CrowdStrike<sup>17</sup> attributed the hacking of the Democratic National Committee (DNC) emails during the 2016 Presidential election to Russian state actors.

Secondly, existing attribution reports show that determinations of attribution are multi-sourced and can differ in the amount of information and evidence they contain. Moreover, their degree of analysis and their assessment methodology is often inconsistent or just unarticulated.<sup>18</sup> This has raised questions about their reliability and validity.<sup>19</sup>

Thirdly, current attribution claims demonstrate that attribution is a multifaceted and interactive process involving different processes each with their own particular determinants and techniques. They also reveal that the majority of existing claims concern technical or political attribution or a combination thereof.

<sup>12</sup> FBI National Press Office, 'Update on Sony Investigation' (19 December 2014), available at [www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation](http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation).

<sup>13</sup> James S. Brady Press Briefing Room, 'Attribution of the WannaCry Malware Attack to North Korea', Press Briefing (19 December 2017), available at [www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/](http://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/).

<sup>14</sup> Office of the Press Secretary, Statement (15 February 2018), available at [www.whitehouse.gov/briefings-statements/statement-press-secretary-25/](http://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/); Foreign and Commonwealth Office, 'Foreign Office Minister Condemns Russia for NotPetya Attacks' (15 February 2018), available at [www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks](http://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks).

<sup>15</sup> National Cyber Security Centre, 'UK and Allies Reveal Global Scale of Chinese Cyber Campaign', Press Release (20 December 2018), available at [www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign](http://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign).

<sup>16</sup> US Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), 'GRIZZLY STEPPE – Russian Malicious Cyber Activity', Joint Analysis Report, Ref. JAR-16-20296A (29 December 2016), available at [www.us-cert.gov/sites/default/files/publications/JAR\\_16-20296A\\_GRIZZLY%20STEPPE-2016-1229.pdf](http://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf); Office of the Director of National Intelligence (ODNI), *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community Assessment, Doc. No. ICA 2017-01D (6 January 2017), at 1, available at [www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](http://www.dni.gov/files/documents/ICA_2017_01.pdf) ('Assessing Russian Activities').

<sup>17</sup> 'CrowdStrike's work with the Democratic National Committee: Setting the record straight', *CrowdStrike* (5 June 2020), available at <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

<sup>18</sup> See, e.g., *Assessing Russian Activities*, *supra* note 16.

<sup>19</sup> With regard to the Sony hack, see, e.g., Schneier, 'We Still Don't Know Who Hacked Sony', *The Atlantic* (5 January 2015), available at [www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/](http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/). See also Jack Goldsmith, 'The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance', *Lawfare* (19 December 2014), available at [www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance](http://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance).

In the previous section, we explained what technical attribution is; but what should be noted here is that not all technical reports attribute cyber attacks to states or to threat actors related to states and, even where they do so, the remedies they contain are technical. Attributing cyber attacks to states is what political attribution can do. Political attribution is the determination of ‘who did it’ in the form of a state or an entity linked to a state on the basis of political analysis and assessment.<sup>20</sup> Political attribution is performed by political institutions, as current state-to-state attributions show, and relies heavily on intelligence. It is also subject to political considerations concerning the question of whether to attribute and when; whether attribution will be public or private; and what will be attributed and to whom.<sup>21</sup> Political attribution may lead to political action such as diplomatic demarches, public denunciations or restrictive measures, without necessarily attaching legal responsibility – this is the aim of legal attribution.

As far as legal attribution is concerned, current practice shows that it is performed within domestic law enforcement paradigms and concerns the gathering of evidence to prosecute individuals as, for example, in the case of Park Jin Hyok, discussed in the next section,<sup>22</sup> or in order to impose sanctions on individuals or non-state actors for malicious cyber attacks.<sup>23</sup> Although domestic legal processes of attribution may identify the links between said individuals and a state, they do not deal with the issue of state attribution and responsibility under international law for lack of competence. What current practice also shows is that states have not so far invoked the issue of legal attribution and responsibility at the inter-state level. This may be due to political considerations as to avoid aggravating the situation, but it may also be due to the uncertainty surrounding the scope of states’ international law obligations in cyberspace,<sup>24</sup> coupled with the difficulties surrounding the application of the legal determinants of

<sup>20</sup> C. Guitton, *Inside the Enemy’s Computer: Identifying Cyber-Attackers* (2017).

<sup>21</sup> According to the UK Advocate-General:

[T]he UK can and does attribute malicious cyber activity where we believe it is in our best interests to do so, and in furtherance of our commitment to clarity and stability in cyberspace. Sometimes we do this publicly, and sometimes we do so only to the country concerned. We consider each case on its merits.

See United Kingdom Attorney General’s Office, ‘Cyber and International Law in the 21st Century’ (23 May 2018), available at [www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century](http://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century).

<sup>22</sup> See also *United States v. Viktor Borisovich Netyksho et al.*, Case No. 1:18-cr-00215-ABJ, Indictment, 13 July 2018, available at [www.justice.gov/file/1080281/download](http://www.justice.gov/file/1080281/download); *United States v. Zhu Hua and Zhang Shilong*, United States District Court, Southern District of New York, Indictment, Case No. 18 CRIM 891, 17 December 2018, available at [www.justice.gov/opa/press-release/file/1121706/download](http://www.justice.gov/opa/press-release/file/1121706/download).

<sup>23</sup> US Department of the Treasury, ‘Treasury Sanctions Russian Federal Security Service Enablers’, Press Release (11 June 2018), available at <https://home.treasury.gov/news/press-releases/sm0410>; US Department of the Treasury, ‘Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups’, Press Release (13 September 2019), available at <https://home.treasury.gov/index.php/news/press-releases/sm774>. See also Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures Against Cyber Attacks Threatening the Union or its Member States, OJ L 129I/13.

<sup>24</sup> See Efrony and Shany, ‘A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice’, 112 *American Journal of International Law* (2018) 583.

attribution alluded to previously. That said, we believe the move to international law is a matter of time, not only because the question of how international law applies to cyber operations is gradually being settled, but also because technical or political determinations of attribution, and any ensuing action, may be legally challenged, and, more importantly, because attribution determinations need to comply with the legal standards of attribution if a state were to use available international law remedies such as countermeasures. It is for this reason that the article will pre-empt the discussion by examining the legal methodologies and determinants of attribution after discussing in the next section the technical ones.

### 3. Technical Cyber Attribution



Attributing a cyber attack begins with a technical analysis of data that results from the attack. A series of actions is required to execute a successful cyber attack. Analysts use this trail of actions and the related data, along with an established body of knowledge based on previous events that includes the methods and tooling of already known malicious actors, to attempt to trace these operations back to their sources. Although there is no standardized model of cyber attack, from existing models<sup>25</sup> we can say that the cycle of a malicious cyber attack includes a number of stages: the preparatory stage of target identification, reconnaissance and weaponization; the engagement and presence stage of delivery, exploitation, installation and actions on objective; and the effects and consequences stage. Analysts collect as many data points as possible from each stage in order to associate them with online personas, individuals and organizations. Data points that demonstrate potential relevance and/or uniqueness to a forensic investigation are considered indicators. Key indicator categories are tradecraft, infrastructure, malware and intent, as shown in [Table 1](#). The US Office of the Director of National Intelligence (ODNI) made this matrix publicly available to demonstrate the concepts behind their internal framework for attributing malicious cyber activity.<sup>26</sup>





























The first indicator category, tradecraft, refers to the collective behaviour frequently used to conduct cyber attacks, which forms a pattern that can be seen across time and location. This is arguably the most important indicator category, because human habits are more difficult to change than technical tools. Examples of tradecraft are payment and financial transactions, email and social media accounts, types of infection and delivery methods (e.g. infected USB drives or compromised websites) or actions on objective (activities inside the target/victim network). However, although an attacker's tools, techniques and procedures (TTPs) can be unique tradecraft indicators, they can diminish in importance once they become public and other actors can mimic them.

<sup>25</sup> ODNI, 'Building Blocks of Cyber Intelligence: Cyber Threat Framework' (2018), available at [www.dni.gov/index.php/cyber-threat-framework](http://www.dni.gov/index.php/cyber-threat-framework).

<sup>26</sup> ODNI, 'A Guide to Cyber Attribution' (14 September 2018), available at [www.dni.gov/files/CTIIC/documents/ODNI\\_A\\_Guide\\_to\\_Cyber\\_Attribution.pdf](http://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf). See also République Française, Ministère des Armées, 'Droit international appliqué aux opérations dans le cyberspace' (9 September 2019), at 11.

**Table 1.** Matrix of competing hypotheses of attribution for five cyber-threat actor groups in relation to four major incidents.

Data to associate with incident:  Sufficient  Limited

CYBER INCIDENT		ADVERSARY	KEY INDICATORS FOR ATTRIBUTION				
			Tradecraft	Infrastructure	Malware	Intent	External Sources
2017	MARCH Major Compromises of Global IT Firms	RUSSIA					
		CHINA*					
		NORTH KOREA					
		IRAN					
		NON-STATE					
	MAY Wannacry Attacks	RUSSIA					
		CHINA					
		NORTH KOREA*					
		IRAN					
		NON-STATE					
	JUNE NotPetya Attacks	RUSSIA*					
		CHINA					
		NORTH KOREA					
		IRAN					
		NON-STATE					
	DECEMBER Saudi Petrochemical Facility Attack	RUSSIA					
		CHINA					
		NORTH KOREA					
		IRAN					
		NON-STATE					

Source: Courtesy of ODNI.

The second indicator category, infrastructure, refers to the physical and/or virtual communication structures used to deliver a cyber capability or maintain command and control (C2) of capabilities. They include, for example, domain names, dynamic DNS services, IP addresses, proxy servers and anonymity services. Attackers can buy, lease, share and compromise servers and networks to build their infrastructure. They frequently establish infrastructure using legitimate online services, from free trials of commercial cloud services to social media accounts. Some cyber-threat actors are reluctant to abandon infrastructure because of habit, cost or time, while others will do so because they can rebuild it within hours. This indicator category is very powerful and is relied upon heavily along with tradecraft in many attribution assessments. Although some attackers routinely change infrastructure between or even within operations to impede detection, skilled analysts actually use this to their advantage by drawing even more nodes and edges in a graph of malicious activity.



The third indicator category, malware, refers to malicious code (aka malware) designed to enable unauthorized functions on a compromised computer system. The functionality of malware is varied and depends on its purpose and target, but example functions include key logging, screen capture, audio recording, remote command and control and establishing a 'backdoor' to ensure persistent access. One challenge with this indicator category is the increasing ease with which cyber-threat actors can modify another attacker's malware and repurpose it and the number of them that can do so, as well as the general availability of feature-rich malware on the dark web or cyber black market. Moreover, automation and machine learning systems are capable of making changes to malware and repurposing it quickly, with little human intervention.<sup>27</sup> Also, as with infrastructure, sophisticated threat actors routinely change malware between or within operations to impede detection and attribution.

The fourth indicator category, intent, refers to an attacker's commitment to carry out certain actions based on the surrounding context: geopolitical, social, economic, religious and so on. For example, covert, deniable cyber attacks are often launched against opponents before or during regional conflicts, as in the case of the conflict between Georgia and Russia in 2008.<sup>28</sup> While some may consider an indicator in this category to be non-technical, it can provide confidence or weight to an indicator from another category. Intent can also be highly useful in suggesting to an analyst where s/he might look to find other relevant, technical indicators. However, a problem with intent is that multiple attackers might share the same intent, thus making it difficult to discriminate amongst and filter possible cyber-threat actors, and for this reason information from other sources is required.

In addition to the above, data or evidence from external sources such as the private sector or academia can be used.

Because of the complexity of actions involved in each stage of a cyber attack, which also require anonymity-enhancing or identity-obfuscating techniques, and because of the time span of actions, mistakes are bound to occur. Forgetting, for example, to turn on a proxy or route through a particular virtual private network (VPN), selecting the wrong stored username or password from an autofill option on a web browser, typing a text string for name or payment information that is from another persona or real identity or using a proper (real) name in correspondence are all examples of simple, small mistakes that can reveal a true identity and/or permit investigators to make an association with a false identity. Mistakes are therefore critical in attribution determinations because they can reveal patterns and relationships. Even one small error can allow a seasoned analyst with access to large data sets to begin to pull a thread through many disparate sources.

These data can be collected via different mechanisms. Companies that operate Internet infrastructure, run services or resell third-party data allow security researchers to purchase data or are compelled by state authorities to provide user,

<sup>27</sup> For more background on automation in cyber defence, see Fraise, 'Cyber Grand Challenge (CGC)', available at [www.darpa.mil/program/cyber-grand-challenge](http://www.darpa.mil/program/cyber-grand-challenge) (last visited 10 June 2020).

<sup>28</sup> White, 'Understanding Cyberwarfare: Lessons from the Russia-Georgia War', *Modern War Institute* (20 March 2018), available at <https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/>.

transaction and other data. Community repositories also exist where analysts can access large amounts of ‘crowdsourced’ data (e.g. VirusTotal<sup>29</sup> for malware). In some cases, data can be scraped from public websites. In the case of attribution done by a government, law enforcement agencies and intelligence agencies can also collect data.

In order to yield results, forensic investigations may require time to scour reams of data and assess them. What the ODNI matrix in [Table 1](#) also shows is that analysts weigh the evidence in terms of both volume and veracity to determine a confidence level for their assessments. Certainty is rarely an option, let alone a realistic goal, in cyber-attack attribution, as the ODNI matrix shows. Indeed, the ODNI matrix attributes levels of confidence to each indicator category, from ‘sufficient’ to ‘limited confidence’. However, there is no published standard as to what constitutes a ‘sufficient’ amount of evidence to support an analytic judgement in making an attribution statement. Anecdotally, many analysts will refrain from making a public assessment when they have limited or no information from one or more of the indicator categories mentioned above and will wait until more evidence is gathered.<sup>30</sup> Forensic investigators may also rely on evidence from external sources, for example think tanks, non-profit groups, academics, media and private industry, in order to confirm a finding or to strengthen the body of supporting evidence for the analytic judgement.

All these issues can be better illustrated by using an example, namely the criminal complaint against Park Jin Hyok<sup>31</sup> who was allegedly behind a series of cyber attacks, including the Sony and WannaCry attacks. According to the affidavit, attribution to the defendant was based, in part, on email and social media accounts that were connected to each other and which were used to send spear phishing messages; aliases; malware ‘collector accounts’, used to store stolen credentials; common malware code libraries; proxy services used to mask locations; and North Korean, Chinese and other IP addresses used across multiple instances of malicious activities. The evidence was collected over many years. It relates to the tradecraft, malware and infrastructure indicator categories and is associated with the preparation and establishing presence and execution stages of the investigated cyber attacks. The complaint was also based on information from reports produced by private security companies, and from various law enforcement agencies and investigatory agencies following search warrants and formal requests for evidence to foreign countries.<sup>32</sup> Mistakes made by Park Jin Hyok were also critical in revealing his real credentials. The affidavit finally concluded that on the basis of the evidence there was sufficient probable cause for the requested complaint.<sup>33</sup>

<sup>29</sup> Virustotal homepage, [www.virustotal.com](http://www.virustotal.com) (last visited 10 June 2020).

<sup>30</sup> See, e.g., the ODNS matrix with regard to NotPetya.

<sup>31</sup> *United States of America v. Park Jin Hyok*, US District Court, Central District of California, Unsealed Criminal Complaint, Case No. MJ-18–1479, 6 September 2018, available at [www.justice.gov/opa/press-release/file/1092091/download](http://www.justice.gov/opa/press-release/file/1092091/download). It should be acknowledged though that the case does not concern state-to-state attribution; it is referenced because of the detailed information it contains.

<sup>32</sup> *Ibid.*, paras 3, 4.

<sup>33</sup> *Ibid.*, para 5. It should be noted, however, that this is not the standard used in a criminal trial.

So far we have looked at the evidence and standards used in technical attribution, but it should be noted that there is no single widely accepted attribution model (although there have been a number of proposals in academic literature).<sup>34</sup> Cyber attacks are dynamic in nature and models quickly breakdown or fail to account for new developments in the defensive and threat landscape. New protections are deployed by software and hardware vendors, while at the same time new weaknesses are discovered and targeted by malicious cyber actors. While some linear approaches have been used to illustrate the set of activities generally required for a successful cyber attack, in reality the process is actually quite non-linear.

In concluding this section, it has been shown that technical attribution can be based on different categories of technical indicators and the extent to which multiple data points in each category are available. It has also been shown that methodological questions remain open and the level of confidence in the evidence varies; there is always a degree of granularity in technical attribution. Moreover, and as was stated in Section 1, the aims and priorities of technical attribution differ from those of legal attribution. For this reason, technical attribution does not automatically translate into legal attribution and is not sufficient in itself to hold a state legally responsible unless the technically attributed malicious cyber attack can also be attributed to a state as a matter of law and the technically produced evidence can also be validated in law. For this reason, the next section will examine the international law methodology and determinants of attribution.

#### 4. Attribution in the Law of State Responsibility and Its Determinants

Attribution in the law of state responsibility is a normative – not a factual or technical – process whose function is to assign a wrongful act to a state in order to engage its responsibility.<sup>35</sup> For this reason, its determinants are moulded by how the state is defined, which in the law of state responsibility is reduced to the structures, entities

<sup>34</sup> Wheeler and Larsen, 'Techniques for Cyber Attack Attribution', Institute for Defense Analyses Paper P-3792 (2003), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf>; Hunker, Hutchinson and Marguiles, 'Role and Challenges for Sufficient Cyber-Attack Attribution', *Institute for Information Infrastructure Protection* (2008), available at <http://cobweb.dartmouth.edu/~thei3p/>; Lin, 'Attribution of Malicious Cyber Incidents', Aegis Series Paper No. 1607 (26 September 2016), available at [www.hoover.org/sites/default/files/research/docs/lin\\_webready.pdf](http://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf); Caltagirone, Pendergast and Betz, 'The Diamond Model of Intrusion Analysis', *Center for Cyber Threat Intelligence and Threat Research*, Technical Report ADA586960 (2013), available at [www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf](http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf); ODNI, Public-Private Analytic Exchange Program, 'Phase II: Cyber-Attribution' (1 September 2017), available at [www.odni.gov/files/PE/Documents/PHASE-II\\_CYBER-ATTRIBUTION.pdf](http://www.odni.gov/files/PE/Documents/PHASE-II_CYBER-ATTRIBUTION.pdf).

<sup>35</sup> ARSIWA, *supra* note 5, Art. 2. Attribution in the law of state responsibility is not about 'assigning responsibility for malicious cyber activity to a specific actor or sponsor', as the EU claims in a recent non-paper: see Council of the European Union, European External Action Service, 'Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of Malicious Cyber Activities – Discussion of a Revised Text', Doc. No. 6852/1/19 REV 1 (18 March 2019), Annex, at 2, available at [www.statewatch.org/news/2019/mar/eu-council-cyber-6852-REV-1-19.pdf](http://www.statewatch.org/news/2019/mar/eu-council-cyber-6852-REV-1-19.pdf).

and functions that make up its legal-political order. This makes the legal determinants of attribution quite narrow, requiring an identifiable, direct and close link between a state and an entity or between a state and the impugned conduct; a link that overrides the latter's independent existence. This occurs when an institutional, functional or agency link between a state and an entity or conduct is established.

The institutional link covers the relationship between a state and its de jure or de facto organs.<sup>36</sup> De jure organs are entities that are defined as such by the state's law. This would be the case, for example, with Russia's Main Intelligence Directorate (GRU) officers indicted in relation to the DNC hacking.<sup>37</sup> It will also cover entities, cyber defence groups or hacker groups incorporated into the state apparatus, such as the Estonian Defence League,<sup>38</sup> Unit 61398 of the Third Department of the Chinese People's Liberation Army,<sup>39</sup> Israel's Unit 8200, or Bureau 121, a hacking unit within the North Korean Reconnaissance General Bureau (RGB).<sup>40</sup>

De facto organs are state instrumentalities. They include entities, groups or individuals who are completely dependent on a state and over whom the state exercises control 'in all fields'.<sup>41</sup> From an examination of existing jurisprudence, it transpires that if an entity has been created by a state, operates on behalf of that state and has no real autonomy in decision-making, it is a de facto organ of that state. Contracted-out cyber groups or companies may also be included, but that would depend on the terms of the contract and how it is executed, in particular whether the outsourced tasks are closely linked to the state such as security tasks, and whether their delivery is controlled by the state. That said, proving such a close relationship is particularly difficult and, as the International Court of Justice (ICJ) has stated, it will be quite 'exceptional' to qualify entities as de facto organs.<sup>42</sup> For example, the US government characterized three North Korean hacker groups including the 'Lazarus Group' as 'agencies, instrumentalities, or controlled entities of the Government of North Korea',<sup>43</sup> which in principle alludes to the attribution criteria discussed here, but it provided no evidence to substantiate the claim.

Moving on to the second modality of attribution, a functional link is established when an entity is empowered by a state to exercise governmental authority.<sup>44</sup> The delegation of authority can be specific or general depending on how it is stipulated in domestic law. For example, if the security of a governmental network is contracted

<sup>36</sup> ARSIWA, *supra* note 5, Art. 4; Bosnia Genocide Case, *supra* note 5, at para 385.

<sup>37</sup> *United States v. Viktor Borisovich Netyksho et al.*, *supra* note 22. Those indicted were members of Unit 26165 and Unit 74455.

<sup>38</sup> Estonian Defence League Act 2013, available at [www.riigiteataja.ee/en/eli/525112013006/consolide](http://www.riigiteataja.ee/en/eli/525112013006/consolide).

<sup>39</sup> See Mandiant, *supra* note 11.

<sup>40</sup> See Ha and Maxwell, 'Kim Jon Un's "All Purpose Sword"', FDD Report (3 October 2018), available at [www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword/](http://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword/).

<sup>41</sup> *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, 27 June 1986, ICJ Reports (1986) 14, para 109 ('Nicaragua Case'); Bosnia Genocide Case, *supra* note 5, paras 390–394.

<sup>42</sup> Bosnia Genocide Case, *supra* note 5, para 393.

<sup>43</sup> US Department of the Treasury, *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, *supra* note 23.

<sup>44</sup> ARSIWA, *supra* note 5, Arts 5 and 6.

out to a private company, the contract between the government and the private company would amount to delegation if executive delegation is permitted by domestic law; otherwise, what would amount to delegation is the general authorizing legislation. In relation to this, it should be noted that judicial authorizations – for example, authorizations to conduct data searches – do not constitute delegation; they only certify the lawfulness of the search. With regard to the second prong of the test, what constitutes a governmental function varies, with the exception perhaps of certain intrinsically governmental functions such as defence. It all depends on the nature and purpose of the activity, the overall context within which such functions are exercised and the state's political identity. For instance, if a private cyber security company is authorized to defend the state against cyber attacks, that would be a governmental function, but not when it is authorized to defend its own property from cyber intrusions. Would, however, ransomware attacks, or cybercrime constitute governmental functions if they support a state's economy or if they are part of a state's governance tools? Is espionage a governmental function?<sup>45</sup> With regard to espionage, one perhaps needs to distinguish political from industrial espionage, but even industrial espionage can be linked to core governmental functions such as the economy or national security. That said, and notwithstanding how such activities are characterized, it is highly unlikely that a state will explicitly authorize an entity to perform such activities – rendering Article 5 of the International Law Commission's (ILC) Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) inapplicable. Equally, Article 5 of the ARSIWA will not apply to attributions performed by private companies because there is no authorization, even if attribution is deemed to be a sovereign prerogative or touches upon a state's foreign relations. Article 5 of the ARSIWA may, however, play a more prominent role if implicit authorization is accepted, i.e. authorization derived from informal relations and practices, but, as was said, it requires formal authorization, which reduces its operational functionality.

Although the narrow definition of what constitutes a state organ or a state empowered entity limits the scope of attribution *rationae personae*, attribution is expanded *rationae materiae* in these two instances because all their acts, including their *ultra vires* acts, are attributed to a state, provided that they were carried out under the cloak of state authority and are not so far removed from official functions to be equated with private conduct.<sup>46</sup> There are many difficulties, however, in establishing when an entity acts with real or apparent authority in cyberspace, when s/he acts whilst on duty or off duty or in establishing which acts fall within official functions and which are private. For example, how can someone impersonating a private person give the impression that s/he operates with apparent authority? Also, is spear phishing or releasing documents stolen from private accounts or selling data acquired through espionage part of official functions? These are difficult questions to answer and, to the extent that these were some of the activities carried out by the indicted GRU officers during

<sup>45</sup> See R. Buchan, *Cyber Espionage and International Law* (2018), at 21–24.

<sup>46</sup> ARSIWA, *supra* note 5, Art 7. *Ultra vires* acts are those acts that exceed an organ's authority or contravene instructions.

the 2016 Presidential election, Russia can plausibly claim that its organs acted in their private capacity. The difficulties in distinguishing private from apparent official conduct can, however, be circumvented if the unauthorized but apparently official conduct is systematic and recurrent, ‘such that the state knew or ought to have known of it’.<sup>47</sup> In this case, said conduct will be attributed to the state concerned as if it were implicitly authorized by that state. This is a case of constructive attribution. One can thus say that if the activities of Russian state organs or agencies during the 2016 US Presidential election were as systematic and widespread as the Mueller indictment revealed,<sup>48</sup> they can be attributed to Russia, even if certain conduct was actually private in nature. Yet, this is a unique case of persistent engagement whereas most cyber operations are instantaneous.

Finally, according to the third modality, an agency link is established when a state instructs or directs a person to commit a wrongful act or when the state exercises control over the wrongful act.<sup>49</sup> Instructions imply orders which should be given in relation to each specific act that constitutes a violation of international law<sup>50</sup> and should be carried out as such by those instructed. Direction means guidance over the entity that commits the wrongful act in the sense of the state taking the lead. In both cases, the perpetrator implements or follows the state’s decision to commit the particular wrongful act and her will is subordinated to the will of the state. Regarding the criterion of control, it should be exercised over the specific conduct in question or over the operation in the course of which unlawful acts are committed and, as the ICJ has repeatedly said, it should be ‘effective’. Although the Court has never defined ‘effective’, it is deemed to amount to domination over the act.<sup>51</sup>

Applying Article 8 of the ARSIWA to current attribution claims reveals the difficulties in establishing state attribution. The 2013 Mandiant Report, for example, says about APT1 that it is ‘government-sponsored’, whereas in other parts it says that it ‘receives direct government support’ or that it acted with the ‘full knowledge and cooperation of the Chinese government’.<sup>52</sup> Such language does not correspond to the descriptors of Article 8 of the ARSIWA and, thus, places ATP1 and its activities outside its scope. At this junction it should be noted that many reports use terms like ‘government-sponsored’ or ‘state-sponsored’ to describe the relationship between a state and a group or a cyber attack; however, these terms are devoid of legal meaning and, in any case, allude to a broader and indeed looser relationship between a state and an entity or an act than what the aforementioned attribution criteria require. To give other examples, it was said previously that, according to the US government, the ‘Lazarus Group’ is controlled by North Korea, but this is not equivalent to ‘effective

<sup>47</sup> Crawford, *supra* note 5, at 108, para 8.

<sup>48</sup> *United States v. Viktor Borisovich Netyksho et al.*, *supra* note 22. See also U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Volume I, Special Counsel Robert S. Mueller, III, Submitted Pursuant to 28 C.F.R. § 600.8(c), Washington, D.C. March 2019 available at <https://www.justice.gov/storage/report.pdf>.

<sup>49</sup> ARSIWA, *supra* note 5, Art. 8; Crawford, *supra* note 5, at 110–113.

<sup>50</sup> Bosnia Genocide Case, *supra* note 5, para 400.

<sup>51</sup> Nicaragua Case, *supra* note 41, paras 116–117; Bosnia Genocide Case, *supra* note 5, paras 398, 402–406, 413–414.

<sup>52</sup> Mandiant, *supra* note 11, at 2, 59.

control'; whereas the ODN's finding that President Putin 'ordered the campaign to influence the US elections'<sup>53</sup> does not satisfy the criterion of 'instructions' in Article 8 of the ARSIWA because, even if there were indeed instructions, they were too general and did not amount to a request to commit unlawful acts.

In addition to the above attribution determinants, Article 11 of the ARSIWA attributes to a state the acts of private actors when that state acknowledges and adopts them as its own. The adoption, however, needs to come from the highest levels of government and needs to be clear and explicit.<sup>54</sup> This would mean that the Stuxnet attack, which undisclosed senior US officials acknowledged in a newspaper article,<sup>55</sup> cannot be attributed to the USA because the acknowledgement was not explicit and clear, there was no adoption and, more importantly, it did not concern an act committed by a third party which is the gist of Article 11 attribution.

The preceding discussion has thus demonstrated that existing attribution claims do not satisfy the attribution determinants found in the law of state responsibility but also that these determinants cannot be fulfilled easily in cyberspace (with the exception, perhaps, of *de jure* organs) which leads to responsibility gaps. These difficulties are compounded further by evidentiary difficulties. As the Russian presidential spokesperson, Dmitry Peskov, said with regard to the accusation that Russia was responsible for the DNC hack, the United States 'should either stop talking about [Russia being responsible for the DNC hack] or produce some proof at last',<sup>56</sup> whereas China reacted to US accusations that it was responsible for the intrusion into the Office of Personnel Management by saying that they were neither 'responsible nor scientific' and stressing that it was 'imperative to stop groundless accusations'.<sup>57</sup> In the next section, we shall discuss evidentiary issues associated with cyber attribution.

## 5. Evidence and the Standard of Proof in Cyber Attribution

As was noted in Section 2, existing attribution reports are quite thin on the evidence they contain, and they are often quite obscure in their assessment methodology. Moreover, certain states, such as the USA, UK and France, claim that they are under no obligation to disclose the evidence upon which attribution is made.<sup>58</sup> However,

<sup>53</sup> *Assessing Russian Activities*, *supra* note 16, at 1.

<sup>54</sup> *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment, 24 May 1980, ICJ Reports (1980) 3, paras 63–74.

<sup>55</sup> Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *New York Times* (1 June 2012), available at [www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html).

<sup>56</sup> Smith-Spark, 'Russia Challenges US to Prove Campaign Hacking Claims or Shut Up', *CNN* (16 December 2016), available at <http://edition.cnn.com/2016/12/16/europe/russia-us-hacking-claims-peskov/index.html>.

<sup>57</sup> Finklea et al., 'Cyber Intrusion into U.S. Office of Personnel Management: In Brief, Congressional Research Service', *Congressional Research Service* (17 July 2015), at 3, available at [https://digital.library.unt.edu/ark:/67531/metadc743551/m1/1/high\\_res\\_d/R44111\\_2015Jul17.pdf](https://digital.library.unt.edu/ark:/67531/metadc743551/m1/1/high_res_d/R44111_2015Jul17.pdf).

<sup>58</sup> Egan, 'International Law and Stability in Cyberspace', 35 *Berkeley Journal of International Law* (2017) 169, at 177; United Kingdom Attorney General's Office, *supra* note 21; Ministère des Armées, *supra* note 26.

employing a methodologically sound process of analysing and assessing evidence, and a cogent standard of proof, are critical for the credibility and validation of attribution because evidence can substantiate attribution determinations and justify subsequent actions. This is true in legal as well as non-legal – technical or political – processes of attribution. As the 2015 UN GGE Report explains, ‘accusations of organizing and implementing wrongful acts brought against States should be substantiated’.<sup>59</sup> It is, therefore, important to examine how cyber attribution can be substantiated as a matter of law because, as was said, states may be called upon to justify their determinations and the lawfulness of any action, for instance countermeasures, they may take.

In this section, we will discuss the types of evidence and the standard of proof required to establish cyber attribution. The discussion will be informed by the relevant jurisprudence which, notwithstanding its relative under-development and its heavy judicial focus, provides the minimum context for understanding how evidence can be legally used and assessed. In our opinion, such discussion is important because it will provide useful insights that can be used beyond the legal context because, as the ODNI document presented in Section 3 shows, there are parallels between legal and non-legal standards of evidence.<sup>60</sup>

With regard to the first issue, the type of evidence, it goes without saying that data and digital evidence obtained through forensic investigations are the primary category of evidence to be used in legal determinations of attribution. As indicated in Section 2, they may include, amongst other things, malware samples, compiler language, programming language, IP addresses, domain names, registration information for infrastructure, payment information for infrastructure, patterns/ordering of execution events, keyboard layout for malware creation, scripts and programmes used on a victim network or host. What can also be used is documentary evidence such as cyber strategies, legislation, attribution reports, directives or intelligence reports (even in redacted form).

However, whether these items will be treated as legally significant depends on their relevance and probative value. The ICJ, for instance, takes into consideration a number of factors, such as the source of the evidence and in particular its independence; the disinterested character of the investigation; whether the evidence is first-hand and contemporaneous or secondary and subsequent to the event; whether the assessment methodology was sound; and whether the evidence has been cross-examined or corroborated.<sup>61</sup> This would mean that most of the existing attribution reports by state

<sup>59</sup> UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. No. A/70/174, 22 July 2015, para 28(f).

<sup>60</sup> ‘Analysts evaluate three components when assigning probabilistic language and confidence levels: the timeliness and reliability of the evidence, the strength of the logic linking the evidence, and the type of evidence (direct, indirect, circumstantial, or contextual) ...’. It also explains that high confidence exists when the evidence is ‘beyond reasonable doubt with no reasonable alternative’; moderate confidence when the evidence is ‘clear and convincing’, and low confidence when ‘more than half of the body of evidence points to one thing, but there are significant information gaps’. See ODNI, *supra* note 26, at 4.

<sup>61</sup> *Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda)*, Judgment, 19 December 2005, ICJ Reports (2005) 168, para 59 (‘Armed Activities Case’); *Pulp Mills on the River*



agencies will fail these tests for lack of independence, impartiality and external scrutiny, for the meagre amount of evidence they contain and for failing to explain their assessment methodology. Likewise, attribution reports by private security companies will most probably fail these tests. The legal significance of such reports also depends on whether they have been endorsed by the concerned government.<sup>62</sup> From existing government reports or statements it transpires that, although they often mention reports by the private sector, they do so in a legally non-committal manner; whereas, on other occasions, they include information or evidence contained in such reports without, however, identifying the provider or the relevant evidence.<sup>63</sup> In our opinion, none of this amounts to endorsement.

In relation to digital evidence, it should be noted that its legal significance can be affected by the fact that its probity depends on verification and authentication. However, for security or other reasons, states may refuse to disclose their attribution technology, or the sources or personnel used to collect and analyse the evidence. Furthermore, the attribution technology used by a state may not be widely available. This means that digital evidence cannot be verified, something that will affect the reliability of attribution claims.

In addition, there may be jurisdictional difficulties with the collection of hard evidence. As indicated in Section 3, malware and scripts may be collected from within systems residing in different jurisdictions; whereas, other items, such as registration information, can be found in databases belonging to third parties that operate on the Internet, and which may reside in different jurisdictions. However, the state that has jurisdiction may not consent to or cooperate with such investigations. This gives rise to three further questions: first, whether illegally obtained evidence can be used; secondly, whether adverse inferences can be made when a state refuses to cooperate; and thirdly, what evidence, other than hard evidence, can be used in cases where obtaining hard evidence proves to be difficult. With regard to the first question, the use of illegally obtained evidence is not usually permitted in domestic legal proceedings but in international law things are perhaps different in light of the fact that the ICJ has not rejected such evidence but assesses its relevance and reliability in context. As to whether adverse inferences can be drawn if a state refuses to cooperate with the production of evidence, there is some support for this view<sup>64</sup> but the ICJ seems to take a more cautious approach, noting that it can draw its own conclusions from the non-production

---

*Uruguay (Argentina v. Uruguay)*, Judgment, 20 April 2010, ICJ Reports (2010) 14, at 72, para 168 ('Pulp Mills Case'); *Bosnia Genocide Case*, *supra* note 5, para 213; A. Riddell and B. Plant, *Evidence before the International Court of Justice* (2009), at 192.

<sup>62</sup> *Case Concerning Application of the International Convention on the Elimination of all Forms of Racial Discrimination (Georgia v. Russian Federation)*, Preliminary Objections, 1 April 2011, ICJ Reports (2011) 70, paras 73, 81.

<sup>63</sup> See DHS and FBI, *supra* note 16, at 1; *United States of America v. Park Jin Hyok*, *supra* note 31; James S. Brady Press Briefing Room, *supra* note 13.

<sup>64</sup> R. A. Clarke and R. K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (2010), at 178.

of evidence.<sup>65</sup> With regard to the third question, the use of circumstantial evidence becomes critical, as the 2010 UN Group of Governmental Experts (GGE) Report<sup>66</sup> confirms. Circumstantial evidence is relational evidence; it includes surrounding factors and circumstances to prove a certain fact. They may include geopolitical factors, indicators of origin, motivation, the degree of sophistication of the attack, the scale and timing of the attack, linguistic indicators, common tooling, infrastructure and so on. In fact, similar evidence is also used to establish technical attribution, as discussed in Section 3. Yet, any inferences made on the basis of circumstantial evidence should be reasonable in light of existing primary evidence.<sup>67</sup> It follows from this that, without hard evidence, geopolitical factors, however persuasive, are not sufficient to attribute the Stuxnet attack to the USA or Israel, and the same can be said about language indicators or IP addresses because they may be false flags.

The second issue to discuss is what standard of proof can clothe attribution determinations with the necessary degree of confidence. As stated in Section 2, existing attribution determinations do not reveal any consistently applied standard of proof, or they just fail to articulate any particular standard.<sup>68</sup> Likewise, the ODNI matrix in Table 1 suggests that technical attribution should be based on sufficient evidence, but it does not explain its threshold. That notwithstanding, existing reports indicate that attribution determinations should enjoy a degree of certainty in order to be credible and reliable. This is exactly what the standard of proof does. However, the law of state responsibility does not set its own evidentiary standards and international law in general is quite undecided, adapting the standard of proof to the facts of the case and the norms involved.<sup>69</sup> The ICJ, for example, opined that for charges of exceptional gravity, evidence needs to be fully conclusive and that this standard also applies to attribution,<sup>70</sup> but it was criticized for introducing criminal law standards to civil law cases.<sup>71</sup>

<sup>65</sup> Bosnia Genocide Case, *supra* note 5, paras 44, 204–206. See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Dissenting Opinion of Vice-President Al-Khasawhen, 26 February 2007, ICJ Reports (2007) 43, at 241 para 35 ('Bosnia Genocide Case, Dissenting Opinion of Vice-President Al-Khasawhen'); *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Dissenting Opinion of ad hoc Judge Mahiou, 26 February 2007, ICJ Reports (2007) 381, paras 56–63.

<sup>66</sup> UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. No. A/65/201, 30 July 2010, at 2 ('GGE Report').

<sup>67</sup> Nicaragua Case, *supra* note 41, para 111; Bosnia Genocide Case, *supra* note 5, Bosnia Genocide Case, Dissenting Opinion of Vice-President Al-Khasawhen, *supra* note 65, para 51.

<sup>68</sup> For example, the UK government stated that 'it is highly likely that North Korean actors known as the Lazarus Group were behind the WannaCry ransomware': Foreign and Commonwealth Office, 'Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks' (19 December 2017), available at [www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks](http://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks). The FBI attributed the Sony attack to North Korea on the basis of 'enough information': see FBI National Press Office, *supra* note 12. Most reports, however, do not state any standard or if there is such a standard it remains unarticulated. See DHS and FBI Report and Assessing Russian Activities, *supra* note 16.

<sup>69</sup> Crawford, *supra* note 5, at 124, para 4, but also see *ibid.*, at 93, para 9.

<sup>70</sup> Bosnia Genocide Case, *supra* note 5, para 209.

<sup>71</sup> Meron, 'Major Developments in International Law: A Conversation on the ICJ's Opinion in *Bosnia and Herzegovina v. Serbia and Montenegro*', 101 *American Society of International Law Proceedings* (2007) 215, at 216.

Elsewhere, the Court used formulations such as ‘sufficient’ or ‘conclusive’ evidence;<sup>72</sup> or variations of ‘on a balance of probabilities’, ‘in all probability’, ‘consistent with the probabilities’ and ‘with a high degree of probability’.<sup>73</sup> As far as the *Tallinn Manual* is concerned, it relegates this issue to judicial processes and admonishes states to act reasonably in the circumstances.<sup>74</sup>

What the preceding discussion thus demonstrates is that, although international law takes a more relaxed approach to evidence which may, in principle, assist cyber attribution, the absence of well-articulated standards of proof and their mutability create uncertainty which may affect the credibility, reliability and also the validity of legal determinations.

## 6. Proposals for Improving the Attribution Process

In the light of the challenges surrounding cyber attribution, we will now consider a number of proposals and whether they can make cyber attribution and its methodology more efficient and effective. The first proposal is of an institutional nature and envisages the establishment of an international attribution agency to centralize and streamline attribution determinations; the second proposal is normative and envisages the revision of the attribution determinants to capture the reality of cyber-threat actors and their connections to states; whereas the third proposal seeks to identify a standard of proof that can facilitate the making of reliable and credible attribution determinations.

### A. International Attribution Agency

There are many blueprints for such an agency, ranging from an agency with purely private-sector membership, an agency with private-public membership and a purely intergovernmental agency.<sup>75</sup> For its proponents, an international agency that

<sup>72</sup> Nicaragua Case, *supra* note 41, para 110; Armed Activities Case, *supra* note 61, paras 91, 172; Bosnia Genocide Case, *supra* note 5, para 209.

<sup>73</sup> *Case Concerning the Land, Island and Maritime Frontier Dispute (El Salvador v. Honduras: Nicaragua Intervening)*, Judgment, 21 September 1992, ICJ Reports (1992) 351, paras 121, 155, 248; *Case Concerning Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia v. Malaysia)*, Judgment, 17 December 2002, ICJ Reports (2002) 625, para 72; Nicaragua Case, *supra* note 41, para 158.

<sup>74</sup> M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., 2017), at 81–82.

<sup>75</sup> Davis II et al., *Stateless Attribution: Toward International Accountability in Cyberspace* (2017), available at [www.rand.org/pubs/research\\_reports/RR2081.html](http://www.rand.org/pubs/research_reports/RR2081.html); Microsoft, ‘From Articulation to Implementation: Enabling Progress on Cyber Norms’ (June 2016), available at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVMc8>; Healy, Mallery, Jordan and Youd, ‘Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security’, *Atlantic Council* (2014), available at [www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building-Measures\\_in\\_Cyberspace.pdf](http://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building-Measures_in_Cyberspace.pdf); ‘An Attribution Organization to Strengthen Trust Online’, Microsoft Policy Papers, available at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI> (last visited 10 June 2020); Droz and Stauffacher, ‘Trust and Attribution in Cyberspace: A Proposal for an Independent Network of Organisations Engaging in Attribution

centralizes and streamlines attribution determinations and processes will engender trust in attribution against the current state of decentralized, often inconsistent and methodologically obscure determinations. It will also lead to the standardization of attribution by establishing its own attribution methodology, rules of evidence and decision-making process. Moreover, such an agency can assist governments or courts in making more informed and persuasive decisions. Other advantages are that it will contribute to the depoliticization of attribution but also to its democratization in view of the inequities in states' cyber capabilities. However, whether such an agency can attain these aims depends on its independence; the nature of its membership and its representative character; its financial transparency; its decision-making process and standards; its investigatory competence; its technical, political and legal expertise; its attribution methodology; the standard of proof it applies; and the vigorousness of its oversight mechanisms.<sup>76</sup>

In our opinion, the above represent a rather demanding set of conditions and it is doubtful whether they can ever be satisfied. There are also other factors that cast doubt on the desirability as well as the feasibility of such an agency. The first and perhaps most important factor is that the functioning, utility, authority and effectiveness of such an agency will ultimately depend on the willingness of states to cooperate and accept its findings. Yet, many states view attribution as part of their sovereign prerogative, and do not feel obligated to provide information when they make attributions. This is the US, UK and French position and also the position of the European Union and NATO.<sup>77</sup>

Secondly, even if states exhibit some cooperative spirit in this regard, they will still want to protect their networks from prying eyes, something that will hinder the work of such an agency. Furthermore, victim or perpetrator states may demand access to the information the agency used in order to make its determinations, which the agency may not be able to provide if such information is classified.

Thirdly, there is the danger that such an agency may substitute its own attribution determination for that of courts or governments, even if its avowed function is to facilitate attribution determinations rather than to make conclusive determinations. To explain, the agency's determinations may have a direct bearing on legal determinations of attribution because of the close link between facts and the law in this area, particularly if courts or other legal institutions lack the resources or expertise to

---

Peer-Review', ICT4Peace Foundation (2018), available at <https://ict4peace.org/wp-content/uploads/2019/07/ICT4Peace-2019-Trust-and-Attribution-in-Cyberspace.pdf>; Chernenko, Demidov and Lukyanov, 'Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms', Council on Foreign Relations (23 February 2018), available at [www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms](http://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms).

<sup>76</sup> See Davis II et al., *supra* note 75, at 25–34.

<sup>77</sup> See Cyber Diplomacy Toolbox, *supra* note 5. See also Council of the European Union, *supra* note 35, at 13: 'Every Member State is free to make its own determination with respect to attribution of a malicious cyber activity'; NATO, 'Brussels Summit Declaration', Press Release (2018) 074 (11 July 2018), para 20, available at [www.nato.int/cps/en/natohq/official\\_texts\\_156624.htm](http://www.nato.int/cps/en/natohq/official_texts_156624.htm). For the US, UK and French position, see Smith-Spark, *supra* note 56.

scrutinise the agency's findings.<sup>78</sup> Likewise, states that lack the required technological or intelligence capacity may not be able to verify the agency's determinations. Even more worryingly, states may be compelled to take action following the agency's attribution determination, against their more prudent judgement. If this were to happen, it would raise questions about the legitimacy of the agency, the legality of its determinations and its accountability.

Fourthly, the timeline within which such an agency will produce its findings may affect the application of international law. In international law, there needs to be some form of temporal proximity between action and reaction, as in the case of self-defence or countermeasures. Likewise, judicial proceedings should be completed within a reasonable time. Long timelines in making attribution determinations will either frustrate prospective legal action or delay it to such an extent that the temporal link would break down and the action would lose its legal justification. For these reasons, states or courts may ignore the agency and rely on their own attribution determinations unless, of course, the temporal requirements inscribed in law are also revised.

In light of the above, we believe that the creation of such an agency is quite premature and will just add another layer in the already fractured attribution process.

### ***B. Revision of the Attribution Determinants***

The second proposal concerns the revision and readjustment of the attribution determinants, focusing mainly on Article 8 of the ARSIWA. It should be said, in this respect, that revising the attribution determinants is neither unreasonable nor against the law, and we will explain why. First, regarding the criterion of 'control', Article 8 of the ARSIWA does not specify its scope, whereas the commentary notes that this standard should apply with a degree of flexibility. This means that there is room for readjustment.

Secondly, the emergence of special responsibility and, for this reason, the emergence of special attribution regimes have been recognised by the ILC, whereas the ICJ admitted that the attribution determinants may vary depending on the area.<sup>79</sup>

Thirdly, it should be recalled that the determinants of Article 8 of the ARSIWA were developed in an era when states created armed groups to fight proxy wars and these groups were dependent on states for direction and resources, such as weapons. The descriptors in Article 8 of the ARSIWA thus reflect such unequal and vertical relations between states and non-state actors. However, the circumstances where Article 8 of the ARSIWA is called upon to be applied have changed and more so in cyberspace. Cyberspace offers a particularly facilitative environment for non-state actors to emerge and operate, and many non-state actors in cyberspace are often self-sufficient,

<sup>78</sup> See *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Dissenting Opinion of Judge ad hoc Vinuesa, 20 April 2010, ICJ Reports (2010) 266, para 71; *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Joint Dissenting Opinion of Judges Al-Khasawneh and Simma, 20 April 2010, ICJ Reports (2010) 108, para 4.

<sup>79</sup> ARSIWA, *supra* note 5, Art. 55; Crawford, *supra* note 5, at 110–112; Bosnia Genocide Case, *supra* note 5, at para 405.

autonomous and pursue their goals either independently from states or in alignment with them, but such alignment can be, variously, formal or informal, vertical or horizontal, continuous or ad hoc, attached or detached.<sup>80</sup> In this context, states may just offer political or ideological direction and support to non-state actors rather than material support.

Fourthly, the current attribution determinants are conceptually informed by the distinction between the public and the private domain.<sup>81</sup> However, the dividing line between private and public has nowadays been displaced and the relationship between non-state actors and states often resembles a networked relationship where non-state actors complement state policies and goals materially, functionally or ideologically. This is particularly true in cyberspace.

Fifthly, the facilitative environment that cyberspace offers and the networked relationship between states and non-state actors can be exploited by states to achieve their policy goals by maintaining a certain level of plausible deniability and thus evade their responsibility.

Consequently, if attaching responsibility to non-state actors as independent legal persons<sup>82</sup> or attaching responsibility to states without attribution<sup>83</sup> is not currently on the international law agenda, and if international law is to maintain its relevance as a governance tool in cyberspace, it is necessary to start thinking about how to approach the attribution determinants in order to capture the role and place of non-state actors in cyberspace and the more subtle modes of interaction between states and non-state actors in order to close the responsibility gaps that currently exist.

Amplifying the level of control a state needs to exercise over organized non-state actors in cyberspace, and moving away from ‘effective control’, can assist significantly in achieving these aims. The ‘overall control’ standard introduced by the International Criminal Tribunal for the former Yugoslavia (ICTY) is particularly apposite in this regard. ‘Overall control’ is established when a state equips, finances, coordinates or helps in the general planning of the activities of an organized group, short of issuing specific instructions.<sup>84</sup> From the ICTY’s judgment, it transpires that the ‘overall control’ standard applies to all organized groups and is not restricted to armed groups only; whereas, more recent legal commentary views ‘overall control’ not only as a criterion for the classification of armed conflicts but also as an attribution criterion.<sup>85</sup>

<sup>80</sup> T. Maurer, *Cyber Mercenaries* (2018).

<sup>81</sup> Crawford, *supra* note 5, at 91.

<sup>82</sup> See Tsagourias, ‘Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts’, 21 *J. Conflict & Security L.* (2016) 455.

<sup>83</sup> Healey, ‘Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council Issue Brief’, *Atlantic Council* (22 February 2012), available at [www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace](http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace).

<sup>84</sup> Appeal Judgement, *Prosecutor v. Tadić*, Case No. ICTY-94-1-A, Appeal Chamber, 15 July 1999, § 131; Schmitt, *supra* note 74, Rule 82, paras 3–8.

<sup>85</sup> ICRC, Commentary on the Second Geneva Convention: Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 2nd edition, 2017, Article 2, paras 287–295, available at <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=1A35EE65211A18AEC12581150044243A>. Although the

The advantages of an ‘overall control’ standard is that it takes a holistic, long-term, multi-factored and, indeed, cumulative view of the relationship between states and organized non-state actors, in contrast to the ‘effective control’ test which requires specific and overwhelming state input. Secondly, it attributes all the acts of the group to a state without the need to prove the state’s input in each and every act as is the case with ‘effective control’.

Its merits can be demonstrated by considering a number of scenarios. The first concerns APT actors committing technically sophisticated attacks on a global scale; for instance, espionage, attacks on critical infrastructure systems or other high-end attacks. In order to design and execute such attacks, APTs need resources, time, technical knowledge, intelligence information, platforms and organisational capabilities. In other words, such operations require long-term investment and close coordination in order to be executed. Previously we said that the sophistication of the attack and of the APT actor can provide evidence of state involvement<sup>86</sup> but the question to ask is how this can lead to attribution. It transpires that the ‘overall control’ indices of equipping, resourcing and planning can indeed provide the most probable description of the type of relationship between states and APTs that can support such action when institutional, functional or agency links are missing, and if the targets and goals of the operation are also taken into account. It follows that when the UK said that APT10 has an ‘enduring relationship with the Chinese Ministry of State Security and operates to meet Chinese State requirements’,<sup>87</sup> the ‘overall control’ criterion could form the basis of attributing its malicious cyber activities to China. Equally, Stuxnet, one of the most sophisticated cyber attacks, can be attributed to the USA and/or Israel on that basis.

The second scenario concerns acts of cyber theft committed by privately-owned Chinese enterprises (POEs). Any discussion of attribution in this case should take into consideration China’s expansive notion of national security, which also includes its economy,<sup>88</sup> as well as its National Intelligence Law according to which ‘any organization or citizen shall support, assist and cooperate with the state intelligence’.<sup>89</sup> It should also take into account China’s economic model, which does not distinguish

---

ICJ rejected the ‘overall control’ for purposes of responsibility, it acknowledged the existence of some flexibility, as was said previously: see Bosnia Genocide Case, *supra* note 5, paras 405–406; Cassese, ‘The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia’, 18 *European Journal of International Law* (2007) 649.

<sup>86</sup> The Australian Prime Minister for example announced in June 2020 that Australia’s government and institutions are being targeted by ongoing sophisticated state-based cyber hacks and that officials had identified them as a state hack ‘because of the scale and nature of the targeting and the trade craft used’. ‘Australia cyber attacks: PM Morrison warns of “sophisticated” state hack’. BBC News, 19 June 2020, available at [www.bbc.co.uk/news/world-australia-46096768](http://www.bbc.co.uk/news/world-australia-46096768).

<sup>87</sup> National Cyber Security Centre, *supra* note 15.

<sup>88</sup> National Security Law of the People’s Republic of China Promulgated by Order No. 29 of the President of the People’s Republic of China (1 July 2015), Art. 2, available at [http://eng.mod.gov.cn/publications/2017-03/03/content\\_4774229.htm](http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm).

<sup>89</sup> National Intelligence Law of the People’s Republic of China (Promulgated by Order No. 69 of the President of the People’s Republic of China on June 27, 2017), Art. 7, available at <https://en.pkulaw.cn/display.aspx?cgid=313975&lib=law>. But see Jihong Chen and Jianwei Fang, Declaration on behalf of Huawei before the Federal Communications Commission (27 May 2018), available at <https://thechinacollection.org/wp-content/uploads/2019/03/Huawei-Declaration.pdf>.

clearly between private and public enterprises but establishes a network of relations between the state and these companies.<sup>90</sup> These factors blur the distinction between the state and the private sector and make the current attribution determinants inapplicable. To explain, POEs are not de jure organs, whereas the network of relations between POEs and the government do not amount to complete dependence and control in order to make them de facto organs since the companies can make their own business decisions. There are no instructions, at least no explicit and direct ones, and no direction since POEs make their own decisions. There is also no ‘effective control’ by the government over acts of cyber theft. Finally, there is no authorization to commit cyber theft and, of course, questions can be asked as to whether cyber theft is part of commercial or governmental functions.<sup>91</sup> If, however, one takes into account the material support POEs receive from the government in the form of aid or preferential loans, the government’s or the party’s participation in the planning of their activities through managerial or party appointments as well as all the surrounding laws, administrative guidelines and informal rules, it can be said that the government exercises ‘overall control’ over them and thus acts of cyber theft should be attributed to China.

It should be noted however that, even if the ‘overall control’ standard can extend the attribution net, it does not necessarily address all the difficulties surrounding cyber attribution. As was said, the ‘overall control’ standard applies to organized groups; however, purely cyber groups may not exhibit the requisite level of organization. This means that the ‘overall control’ standard is more useful in relation to offline groups which also operate online. Furthermore, the required level of state input is still demanding but, as was said, a cyber actor may not need financial support, training or other assistance. Instead, non-state actors may lend their services to a state out of a sense of allegiance without the state participating in the planning of their activities.

The case of patriotic hackers is indicative in this regard. Patriotic hackers are individuals or groups who act in support of their country’s policies or goals.<sup>92</sup> As the Honker Union of China, a now disbanded patriotic hacker group, declared, its campaign was to ‘safeguard national unity, protect China’s national sovereignty, resist foreign bullies, and deflate anti-China arrogance’.<sup>93</sup> Patriotic hackers are not state organs; they are not empowered by the state; they are not explicitly and directly instructed by the state; they do not act under the state’s direction in the form of leadership; and the state’s input is below the ‘overall control’ or ‘effective control’ thresholds<sup>94</sup> – even if

<sup>90</sup> Milhaupt and Zheng, ‘Beyond Ownership: State Capitalism and the Chinese Firm’, 103 *Georgetown Law Journal* (2015) 665; Williams, ‘The “China, Inc.+” Challenge to Cyberspace Norms’, Aegis Series Paper No. 1803 (22 February 2018), at 69, available at [www.hoover.org/sites/default/files/research/docs/williams\\_webready.pdf](http://www.hoover.org/sites/default/files/research/docs/williams_webready.pdf). See also: FireEye iSight Intelligence, ‘Red Line Drawn: China Recalculates Its Use of Cyber Espionage’, FireEye Special Report (June 2016), available at [www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf](http://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf).

<sup>91</sup> For public/commercial functions, see *Emilio Agustín Maffezini v. the Kingdom of Spain*, Award on the Merits, ICSID Case No. ARB/97/7 (13 November 2000), paras 52–83.

<sup>92</sup> P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014), at 111.

<sup>93</sup> X. Wu, *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications* (2007), at 56.

<sup>94</sup> Hang, ‘Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism’, 5 *Yale Review of International Studies* (2014) 47.



the state encourages them or condones their actions. However, what defines their relationship with the state is their shared values and goals which, on the one hand, allows the state to influence their behaviour and to shape their actions, whilst, on the other hand, makes patriotic hackers receptive and responsive to such influence. This shows that even softer versions of control which are value-oriented can be equally effective in aligning non-state actors and states and in engendering desired outcomes.

We thus propose a criterion of 'soft control'<sup>95</sup> to capture cases where a state exerts influence over non-state actors due to shared values who then act in pursuance of a state's policies or goals, thus complementing state action. On the basis of this criterion, attacks by Chinese patriotic hackers can be attributed to China, and attacks by Russian patriotic hackers following President Putin's call that '[i]f they [hackers] are feeling patriotic, they will start contributing, as they believe, to the justified fight against those speaking ill of Russia'<sup>96</sup> will be attributed to Russia.

The case of patriotic hackers reveals another gap in the attribution determinants of Article 8 of the ARSIWA, namely the role of implicit instructions. Reverting to the example of Chinese patriotic hackers, their actions can also be assessed against China's military strategy, which views civilians and the army working together in times of peace or in times of war to support and defend the nation.<sup>97</sup> Within such a context where the dividing lines between state and private and between civilian and military are blurred, it can be said that Chinese patriotic hackers operate within a system of authority and submit to the will of the state willingly or sometimes unwillingly. Consequently, when the Chinese government identifies enemies of the state which are then attacked by patriotic hackers, the plausible inference that can be made is that they have acted under the implicit instructions of the government. The existence of instructions in this case can be proved through circumstantial evidence, such as communications in governmental outlets, the type of attacks and their targets, the tempo of attacks, their timing or the beginning and end of such attacks. The same reasoning can apply to Chinese POEs in the light of the formal and informal regulatory and managerial framework within which they operate, as mentioned above, but there should be a case-by-case analysis to establish whether the POE implemented in the particular instance a governmental (implicit) instruction. In light of the above, we believe that implicit instructions should be included in the attribution determinants of Article 8 of the ARSWIA.

### C. Standard of Proof

The third proposal tries to identify a suitable standard of proof for cyber attributions. It was said in Section 5 that current attribution claims do not rely on any particular standard of proof and that international law is quite ambiguous in this regard. This

<sup>95</sup> It draws from the concept of soft power. See Nye, 'Soft Power', 80 *Foreign Policy* (1990) 153.

<sup>96</sup> 'Putin Concedes "Patriotic" Hackers Might Target Foreign Elections', *Financial Times* (1 June 2017), available at [www.ft.com/content/f607ac6c-46e6-11e7-8519-9f94ee97d996](http://www.ft.com/content/f607ac6c-46e6-11e7-8519-9f94ee97d996).

<sup>97</sup> Guang Qian, 'The Twenty-First Century War: Chinese Perspectives', in Y. Boyer and J. Lindley-French (eds), *The Oxford Handbook of War* (2012) 279.

offers a degree of flexibility, but, in order to identify a standard of proof which is suitable for cyber attribution, it is important to understand the nature and function of the ‘standard of proof’. Regarding its nature, the standard of proof is context-specific and may vary depending on the domain or the circumstances. Also, the standard of proof is gradated; it describes degrees of confidence but never absolute certainty. This is as true in law as it is in political (intelligence) assessments, which use standards of low, medium or high confidence, and it is also true in technical assessments, as noted in Section 3. Regarding its function, the standard of proof assists decision-makers to make reasonable determinations on the basis of the available evidence, which is especially important when the quantity of evidence is low and its quality needs to be assessed, as in the case of cyber evidence.

It follows from this that applying a very high standard of proof to cyber attribution, such as that of ‘beyond a reasonable doubt’, may increase its factual and legal reliability but may frustrate determinations and consequential action, whereas applying a low standard may affect its reliability and may lead to erroneous decisions with serious repercussions for the acting as well as the victim state.

In our opinion, the ‘preponderance of the evidence’ is the most appropriate standard for proving attribution in cases of less serious malicious cyber operations which are the focus of this article. According to this standard, attribution will be established if more evidence supports a particular attribution finding than contradicts it. The ‘preponderance of the evidence’ is not a new standard but one that has already been used in international jurisprudence, as was shown in Section 5, and it is a standard which is also employed outside the legal context. For example, with regard to the attribution of the WannaCry attack, the US National Security Agency determined that the ‘preponderance of the evidence’ pointed to North Korea.<sup>98</sup>

The main reason why we propose this standard is because it balances the need for reliable attributions and the need for making such determinations and for holding states responsible. To explain, this standard ensures diligent scrutiny of the evidence which a lower standard cannot achieve but it does not unnecessarily impede decisions or action which a higher standard would. Furthermore, it ensures that states will incur responsibility for their malicious cyber operations which a higher standard cannot do because states would be able to operate below that higher standard but, at the same time, it does not trivialise the institution of state responsibility and preserves its regulatory compass which a lower threshold would fail to do. Finally, from a practical perspective, it recognizes the difficulties in obtaining and assessing cyber evidence and the need to make use of circumstantial evidence. In our opinion, the ‘preponderance of the evidence’ standard reconciles legal, policy and factual considerations and ensures that reasonable determinations are made on the basis of available and sufficient evidence.

<sup>98</sup> E. Nakashima, ‘The NSA Has Linked the WannaCry Computer Worm to North Korea’, *The Washington Post* (14 June 2017) available at [www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c\\_story.html](http://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html).

## 7. Conclusion

The preceding discussion has shown that attribution matters for the suppression of malicious cyber operations but also that it is a multifaceted process. The article has presented the methodology and determinants of the technical and legal processes of attribution and explained how they interact. It has also considered what body of evidence can be used to prove attribution and what the applicable standards of proof are. The discussion identified flaws and gaps in the existing methodology, determinants and evidentiary standards which lead to responsibility gaps.

For this reason, the article discussed a number of institutional, normative and evidentiary proposals with the aim of improving the methodology and process of legal attribution in order to close the identified responsibility gaps. The article discussed first the possible contribution of an international attribution agency to the streamlining and standardization of attribution, but concluded that the creation, operation and effectiveness of such an agency would depend on state cooperation which is not forthcoming at this point in time. The article then put forward a number of normative proposals to re-adjust the legal determinants of attribution. They include amplified standards of control in the form of 'overall control' and 'soft control' and the inclusion of implicit instructions as an attribution determinant. In the authors' opinion, these proposals can capture better the realities of cyberspace, the place and role of non-state actors therein and their multi-layered relationship with states, and, thus, address the responsibility deficit that the narrowness of the existing determinants generates. The article finally proposed the 'preponderance of evidence' as the most appropriate standard for proving attribution because it guarantees adequate scrutiny of the evidence whilst also facilitating attribution determinations.

All in all, the article is informed by our belief that international law should not withdraw from cyberspace, but that it should face and shape cyber reality by establishing a regulatory framework within which states, individuals and other entities can operate and be held to account. Our normative and evidentiary proposals assist in building a legal framework for ensuring responsibility and for inculcating a culture of responsibility in cyberspace.