Attribution of Cyber Operations: An International Law Perspective on the *Park Jin Hyok* Case

Tomohiro Mikanagi[*] and Kubo Mačák[†]

Abstract

States are increasingly willing to publicly attribute hostile cyber operations to other States. Sooner or later, such claims will be tested before an international tribunal against the applicable international law. When that happens, clear guidance will be needed on the methodological, procedural, and substantive aspects of attribution of cyber operations from the perspective of international law. This article examines a recent high-profile case brought by the United States authorities against Mr Park Jin Hyok, an alleged North Korean hacker, to provide such analysis.

The article begins by introducing the case against Mr Park and the key aspects of the evidence adduced against him. It then considers whether the publicly available evidence, assuming its accuracy, would in principle suffice to attribute the alleged conduct to North Korea. In the next step, this evidence is analysed from the perspective of the international jurisprudence on the standard of proof and on the probative value of indirect or circumstantial evidence. This analysis reveals the need for objective impartial assessment of the available evidence and the article thus continues by considering possible international attribution mechanisms.

Before concluding, the article considers whether the principle of due diligence may provide an alternative pathway to international responsibility, thus mitigating the deficiencies of the existing attribution law. The final section then highlights the overarching lessons learned from the *Park* case for the attribution of cyber operations under international law, focussing particularly on States' potential to make cyberspace a more stable and secure domain through the interpretation and development of the law in this area.

Keywords

attribution, cyber operations, due diligence, evidence, standard of proof, State responsibility

---

[*] Deputy Director-General, International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan. This article is based on the research at the Lauterpacht Centre for International Law, Cambridge, and the views expressed herein do not represent the official position of the Japanese Government.

[†] Legal Adviser, International Committee of the Red Cross (ICRC), and Associate Professor of Public International Law, University of Exeter. This article was entirely researched and written prior to the author's engagement in the Legal Division of the ICRC and the views expressed herein do not represent the official position of the ICRC or its Legal Division. The authors would like to thank Ana Beduschi, Isabella Brunner, Russell Buchan, Andraz Kastelic, Tomáš Minárik, and Hitoshi Nasu for their valuable comments on earlier drafts. We also acknowledge with gratitude Matthew Kuningas's research assistance and Barbora Ruščin's help with designing the infographic in Figure 1.

1 INTRODUCTION

In the time that it will take you to read this article, numerous hostile cyber operations will be launched around the world, some of which will inevitably impact on individual States' political interests or national security.[1] Not so long ago, it was generally thought that those responsible for such cyber incidents 'can cover their traces, stay anonymous online, and hide behind the attribution problem'.[2] Accordingly, victim States maintained an uneasy and nervous silence about who, in their view, was to blame. However, since the early 2010s, the tide has been turning[3] and multiple States have come forward with—sometimes detailed, sometimes less so—public statements attributing malicious cyber operations to other States.[4] The next milestone will be the first case before an international tribunal where such claims will be tested against the applicable international law. When that happens, clear guidance will be urgently needed on the methodological, procedural, and substantive aspects of attribution of cyber operations from the perspective of international law. This article examines a recent high-profile case brought by the US authorities against Mr Park Jin Hyok, an alleged North Korean hacker, to provide such analysis.

Reflecting the trend noted earlier, the incidents of which Mr Park stands accused in the US have been subject to public attribution by several of the victim States. On 19 December 2017, the UK Foreign Office Minister Lord Ahmad of Wimbledon attributed the WannaCry ransomware incident to the so-called Lazarus Group, an actor linked to North Korea.[5] According to Minister Ahmad, the WannaCry incident impacted 300,000 computers in 150 countries including 48 National Health Service (NHS) trusts.[6] Although he noted that it was highly likely that 'North Korean actors' had orchestrated the ransomware campaign, his statement stopped short of attributing the incident to North Korea itself.[7] By contrast, that same day, a US government official said: 'After careful investigation, the United States is publicly attributing the massive WannaCry cyberattack to North Korea.'[8] This difference between the two statements reflects the difficulty of attributing cyber operations by States *to other States*.

To that end, international law has gradually developed standards, which determine whether an act of a particular individual is to be characterized in law as an act of the State[9]—in other words,

---

[1] For a vivid graphic visualization see, eg, Digital Attack Map, <http://digitalattackmap.com/> (updated daily).

[2] T Rid and B Buchanan, 'Attributing Cyber Attacks' (2014) 38 Journal of Strategic Studies 1, 31.

[3] See, eg, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (11 October 2012) <https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> (warning potential perpetrators that the US now had 'the capacity to locate them and to hold them accountable for their actions that may try to harm America').

[4] See FJ Egloff and A Wenger, 'Public Attribution of Cyber Incidents' (2019) 244 CSS Analyses in Security Policy 1.

[5] Foreign Office Minister condemns North Korean actor for WannaCry attacks (19 December 2017) <https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks>.

[6] ibid.

[7] ibid.

[8] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (19 December 2017) <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>.

[9] This process of legal attribution—the subject of this article—should be distinguished from technical attribution,

whether that act is to be *attributed* to the said State.[10] These standards, codified in the 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts (hereafter 'Articles on State Responsibility' or ASR), are very much a product of the pre-cyber era.[11] Hence, the requirements that they impose are an uneasy match for the fluid and flexible relationships that have come to characterize the online world.[12] What is more, if the responsible State uses an individual or an entity ostensibly unrelated to that State and then does not permit outside investigation, it becomes exceedingly difficult for foreign States to gather the factual evidence that they may need for attribution purposes.

The problem is further compounded by the uncertainty as to the precise interpretation of specific substantive rules of international law in the cyber context. While there is a broad consensus to the effect that existing international law applies in cyberspace,[13] much controversy remains with respect to individual international legal rules. The most contentious ongoing debate surrounds the application of the principle of sovereignty in the cyber environment.[14] For some, including the UK, cyber operations do not violate the sovereignty of a State per se, because sovereignty is a principle of international law that guides State interactions, but does not add to other prohibitive legal rules, including the prohibition of intervention.[15] For others, including France and the Netherlands, the prohibition on the violation of the sovereignty of other States is a primary rule of international law, the breach of which is an internationally wrongful act.[16] The difference between these two positions is crucial with respect to incidents such as those discussed in this

---

which refers to the attribution of a particular cyber operation to a specific machine and to the person operating that machine. Technical attribution 'normally precedes legal attribution [and] is the precondition for imputing the act to a certain State'. Z Huang, 'The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations' (2014) 14 Baltic Yearbook of International Law 41, 43.

[10] See also L Condorelli and C Kress, 'The Rules of Attribution: General Considerations', in J Crawford, A Pellet and S Olleson (eds), *The Law of International Responsibility* (OUP 2010) 221 ('by the term "attribution", reference is made to the body of criteria of connection and the conditions which have to be fulfilled … in order to conclude that it is a State … which has acted in the particular case').

[11] UNGA Res 56/83 annex 'Articles on the Responsibility of States for Internationally Wrongful Acts' (12 December 2001) (hereafter ASR).

[12] See, eg, Huang (n 9) 45–46 (discussing the difficulties for the application of the Articles posed by the 'notable peculiarities' of cyber operations); J D'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought' (2016) 21(3) JCSL 575, 592 (suggesting that 'the rules on attribution inherited from the law on state responsibility' would benefit from a reform that would 'design specific attribution mechanisms for cyber operations').

[13] 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 A/68/98 (24 June 2013) (hereafter UN GGE 2013) para 19. The report was later endorsed by a unanimously adopted resolution of the UN General Assembly. See UNGA Res 68/243 (27 December 2013).

[14] On sovereignty in cyberspace in general, see UN GGE 2013 (n 13) para 20 ('State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.').

[15] See, eg, J Wright, 'Cyber and International Law in the 21st Century' (23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

[16] See, eg, France, Ministry of the Armies, 'Droit international appliqué aux opérations dans le cyberspace' (September 2019) <https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf> (hereafter French 2019 Position Paper), 6–7; Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace – Appendix: International Law in Cyberspace <https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf> (hereafter Dutch 2019 Letter to Parliament) 2; see also MN Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Operations 2.0* (CUP 2017) (hereafter *Tallinn Manual 2.0*) rule 4, commentary para 2.

article, which do not amount to coercion against a State, thus rendering rules on intervention inapplicable.[17] The law governing cyber operations which fall below the threshold of intervention certainly needs further clarity, but this is not the place to address these issues and this article will accordingly not consider issues of primary law any further.[18]

By contrast, our focus is on issues related to attribution. We acknowledge that it is controversial whether all operations discussed herein constitute breaches of specific international obligations. However, our analytical approach is based on the fact that the question of attribution logically precedes the assessment of conformity of a given act with the applicable international obligations.[19] Accordingly, this article examines the law of attribution and does not consider, except where expressly noted, the element of breach.

A final preliminary remark is in order as regards the evidentiary standards and rules discussed in this article. In that respect, it should be cautioned that there is at present no universal and coherent body of law that can be described as the international law of evidence.[20] Every international adjudicative organ is subject to its own standards for the production, collection, and evaluation of evidence, some of which are established in their statutes or rules of procedure, while others have evolved through the practice of these tribunals.[21] In this article, we focus on the International Court of Justice (ICJ) due to its undoubted prominence on the international plane as the principal judicial organ of the United Nations.[22] We believe that this analysis illustrates the extent of flexibility accepted in proving attribution in inter-State disputes. However, it should be borne in mind that other tribunals may well use slightly or markedly different approaches to the procedural issues we discuss, including the applicable standard of proof and the admissibility of indirect evidence. By the same token, outside of the judicial context, the 'attribution' of cyber operations might achieve its political aims whether or not it satisfies the legal standards applied by any of these tribunals including the ICJ. In that regard, each State must determine 'for itself its legal situation vis-à-vis other States'[23] and it is then accountable for any measures taken on the basis of that determination.[24]

---

[17] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* (Merits) [1986] ICJ Rep 14, para 205.

[18] See further H Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention' Chatham House Research Paper (December 2019) <https://www.chathamhouse.org/publication/application-international-law-state-cyberattacks-sovereignty-and-non-intervention> 8–36 (analysing the application of the sovereignty and non-intervention principles in relation to cyber operations below the threshold of the use of force); K Mačák, 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (2019) 113 AJIL 81, 82–84 (analysing why States find it difficult to choose between different conceptualizations of specific primary rules in the area of international cyber law).

[19] Similarly B Stern, 'The Elements of An Internationally Wrongful Act' in Crawford, Pellet, and Olleson (n 10) 201 ('This sequence is logical since an act on its own cannot be assessed against the rules of public international law; it is first necessary to ensure that an act is attributable to the State before examining whether that act is in conformity with what is required from that State under international law.'). This understanding is also in line with the drafting history of the ILC Articles on State Responsibility: see, eg, ILC Yearbook 1973, vol I, UN Doc A/CN.4/SERA/1973, 28, para 18 (1207th mtg, Ago).

[20] A Riddell, 'Evidence, Fact-Finding, and Experts', in CPR Romano, K Alter and Y Shany (eds) *The Oxford Handbook of International Adjudication* (OUP 2013) 868.

[21] R Wolfrum and M Möldner, 'International Courts and Tribunals, Evidence' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2008) <www.mpepil.com> (updated August 2013) para 3.

[22] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS 16, art 92.

[23] *Air Services* (1978) 18 RIAA 417, 443 para 81; see also *Affaire du lac Lanoux* (1957) 12 RIAA 281, 310 para 16 ('il appartient à chaque Etat d'apprécier, raisonnablement et de bonne foi, les situations et les règles qui le mettent en cause' ['it is for each State to assess for itself, reasonably and in good faith, the situations and rules which relate to it']).

[24] cf ASR (n 11) art 49, commentary para 3 ('A State which resorts to countermeasures based on its unilateral

To summarize, the purpose of this article is to examine the existing substantive and procedural international law on attribution against the backdrop of the alleged North Korean hostile cyber operations including WannaCry. We base our analysis on the evidence produced in the US domestic criminal proceedings against Mr Park. Due to the nature of those proceedings, that evidence does not directly concern the attributability of Mr Park's alleged conduct to North Korea as a matter of international law. However, the FBI's affidavit presented in that case stands out for its detailed and wide-ranging information on the attribution of cyber operations. Given the absence of other comparable documents published by governments on the issue of attribution, we chose this affidavit as the vehicle for our analysis.

The article is structured as follows. We begin by introducing the case against Mr Park and the relevant aspects of the evidence adduced against him (section 2). We then consider whether the publicly available evidence, assuming its accuracy, would in principle suffice to attribute the alleged conduct to North Korea (section 3). In the next step, we analyse this evidence against the ICJ's jurisprudence on the standard of proof and on the probative value of indirect or circumstantial evidence (section 4). This analysis reveals the need for objective impartial assessment of the available evidence and we thus continue by considering possible international attribution mechanisms (section 5). In the final step, we ask to what extent the principle of due diligence may mitigate the deficiencies of the existing attribution law (section 6).

2 *PARK JIN HYOK* CASE: SALIENT FEATURES

There has so far been no case before the ICJ or other international tribunals addressing the State responsibility arising from cyber operations.[25] However, in domestic criminal proceedings, there are cases where investigators provide evidence to establish who the attacker was.[26] The *United States of America v Park Jin Hyo*k is a paradigmatic example. In a 172-page-long affidavit published in June 2018, a special agent of the FBI argued that Mr Park was a member of the conspiracy behind many cyber incidents, including the 2014 operation against Sony Pictures Entertainment (SPE), the 2016 operation against the Bangladesh Bank, and the 2017 WannaCry incident.[27] According to the affidavit, the operation against SPE rendered thousands of SPE computer terminals inoperable[28] and the operation against Bangladesh Bank caused a loss of approximately $81,000,000.[29] With respect to WannaCry, the affidavit echoed the UK assessment mentioned earlier and noted that dozens of NHS trusts and hundreds of other NHS organizations in the UK were infected by the

assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment.'). See also Dutch 2019 Letter to Parliament (n 16) 6 ('A state that takes countermeasures or relies on its inherent right of self-defence … in response to a cyber operation may eventually have to render account for its actions, for example if the matter is brought before the [ICJ]. In such a situation, it must be possible to provide evidence justifying the countermeasure or the exercise of the right of self-defence.').

[25] But see *Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination (Ukraine v Russian Federation)*, CR 2017/1 (6 March 2017) para 5 (Zerkal) (accusing the Russian Federation of engaging in 'cyber-attacks' against Ukraine). The case remains pending before the ICJ.

[26] For a general discussion of the US practice of attribution by indictment, see CI Keitner, 'Attribution by Indictment' (2019) 113 AJIL Unbound 207.

[27] *United States of America v Park Jin Hyo*k, Case No MJ 18-1479, Criminal Complaint (filed 8 June 2018) <https://www.justice.gov/opa/press-release/file/1092091/download>, Annex (hereafter Affidavit).

[28] ibid, para 61.

[29] ibid, paras 144–46.

virus, resulting in issues with diagnostic equipment and thousands of patient appointment cancellations.[30]

For greater clarity, we have designed a visual representation of the evidence adduced in the affidavit (Figure 1). As this affidavit concerns the criminal prosecution of an individual and it does not focus on the North Korean government, the evidence showing the attribution to the North Korean government is relatively limited. The figure is thus necessarily a simplification, but we include it here in order to illustrate the logic and methodology that may be used to establish attribution of cyber operations.

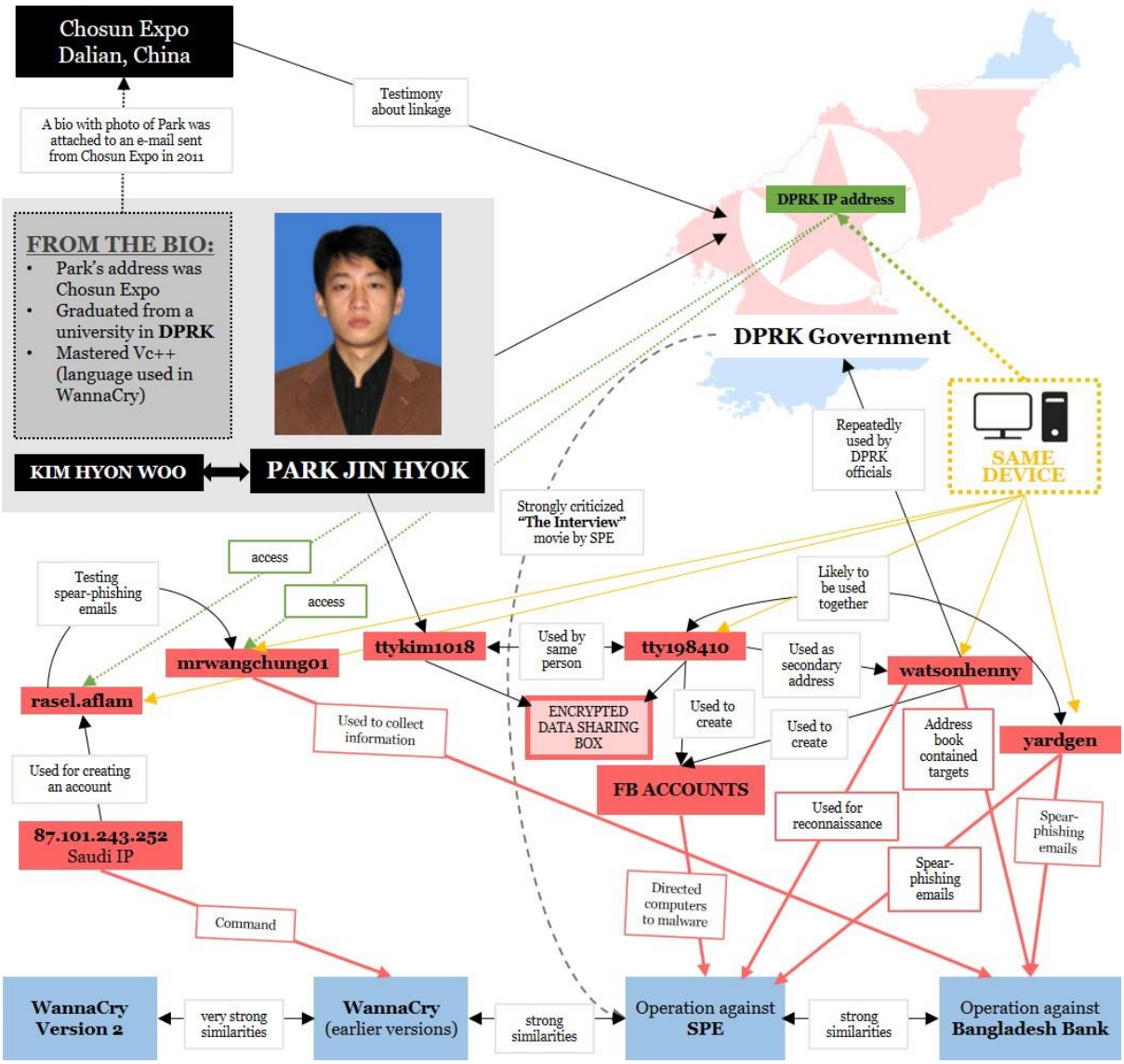

Figure 1

At the bottom of the figure, WannaCry Version 2 is shown as a blue box. The WannaCry ransomware used in the widespread incidents in 2017 exploiting the vulnerability of Microsoft

[30] ibid, para 225.

Windows called 'CVE-2017-0144', was called WannaCry Version 2.[31] The earlier versions of WannaCry are shown in the blue box next to WannaCry Version 2, while the two major cyber operations, which are believed to have connections with Mr Park, are shown in blue boxes further to the right, namely the operation against SPE and the operation against Bangladesh Bank. Red boxes represent IP addresses as well as e-mail and Facebook accounts used directly or indirectly in the cyber operations. Black and red arrows indicate the links between the various elements, and white boxes explain these links.

The affidavit explains that WannaCry Version 2 has very strong similarities with WannaCry Versions 0 and 1, which indicates that these versions were all created by the same author or authors.[32] The affidavit also explains the similarities between the earlier versions of WannaCry and other malware used in other operations, including those against SPE and Bangladesh Bank.[33]

The suspect in this case is Mr Park, shown in the top left part of Figure 1.[34] According to the affidavit, Mr Park and Kim Hyon Woo were using the same e-mail account of 'ttykim1018' and are believed to be the same person with a different alias.[35] This e-mail address and another address 'tty198410' shared a large encrypted data box and this latter e-mail address is also believed to be used by the same person.[36] The 'tty198410' account was also used as a secondary account in the registration of another account named 'watsonhenny', seen on the right-hand side of the figure, which had been used in the cyber operations against SPE and Bangladesh Bank.

The affidavit does not adduce any specific evidence relating to the IP address or e-mail account actually used for the WannaCry Version 2 operation. However, it does refer to several IP addresses used in connection with the earlier versions of WannaCry, one of which was the Saudi Arabian IP address '87.101.243.252'.[37] This IP address was used for creating an e-mail account 'rasel.aflam',[38] which was then used to send test spear-phishing e-mails to another e-mail account 'mrwangchung01' used in the operation against Bangladesh Bank.[39] As to the cyber operations against SPE and Bangladesh Bank, the affidavit shows considerable evidence relating to the IP addresses as well as e-mail and Facebook accounts used in actual operations. The e-mail accounts used for these two operations included 'rasel.aflam', 'watsonhenny' and 'yardgen'.[40] These accounts were accessed from DPRK IP addresses, which were accessed by the same devices used to access 'tty198410' and 'watsonhenny' believed to be used by Mr Park or Mr Kim.

In summary, the evidence adduced in the affidavit indicates the following features:

1. Because perpetrators utilize many layers of aliases and proxies, available evidence tends to be circumstantial or indirect.

---

[31] ibid, paras 221–25.

[32] ibid, para 230.

[33] ibid, para 236

[34] The photograph used in Figure 1 reproduces the one published by the FBI on its Most Wanted list: see FBI, 'Most Wanted: Park Jin Hyok' <https://www.fbi.gov/wanted/cyber/park-jin-hyok>.

[35] Affidavit (n 27), para 297.

[36] ibid, para 291.

[37] ibid, para 240b.

[38] ibid, para 240b.

[39] ibid, para 162.

[40] ibid, paras 102, 118, 148, 152, 162.

2. Due to the multiple layers of aliases and proxies, the evidence on the use of various IP addresses and e-mail accounts across many States plays a crucial role in connecting cyber operations to a certain individual or entity. In the affidavit, there are several references to evidence provided by other States, including the UK and Poland,[41] which highlights the importance of international cooperation in this regard.
3. As direct evidence showing connection to actual cyber operations is difficult to find, the similarity of the programmes used for various operations plays a key role in proving the connection.

According to the affidavit, the evidence on the connections among all the red boxes on Figure 1 show that they constitute the same overall conspiracy involving Mr Park or Mr Kim in all of these cyber operations.[42] The malware used in these operations displays strong similarities, and, according to the affidavit, the similarities between different samples of malware demonstrate that their authors very likely had access to the same collection of original source code. [43] Therefore, the evidence adduced in the affidavit strongly indicates that all these cyber operations had the same authors, including Mr Park.

By contrast, as the affidavit is not against the North Korean government, it does not concentrate on proving links between these operations and the North Korean government. Accordingly, the evidence contained in the affidavit is rather limited as far as those connections are concerned. Still, it points out the following:

1. Chosun Expo was originally established as a joint venture between North Korea and South Korea and, following the South Korean withdrawal from the business, it was maintained by North Korea.[44] A number of Chosun Expo's employees, including Mr Park, were dispatched to Dalian, China, and while there, they were being monitored by a 'separate political attaché' from North Korea.[45] The affidavit additionally stated that these employees kept only a very small fraction of their salary, remitting the rest to the North Korean government.[46]
2. Some of the e-mail accounts used in hostile cyber operations had also been accessed by North Korean government officials. For example, the e-mail account 'watsonhenny' played a key role in operations targeting SPE, Bangladesh Bank, and other victims.[47] This same account was repeatedly used by a North Korean government representative for official DPRK business.[48]
3. Due to the strict control of the access to and use of the internet in North Korea, any extensive reliance on cyber capabilities from North Korean IP addresses is very likely regime-sanctioned. Given that many of the operations discussed in the affidavit were in

[41] See, eg, ibid, paras 189–90 (Poland), 225 (United Kingdom).
[42] ibid, para 150.
[43] ibid, para 184.
[44] ibid, para 270.
[45] ibid, para 271
[46] ibid, para 271.
[47] ibid, paras 103–10; 152–54.
[48] ibid, para 276.

fact launched from such IP addresses, it is likely that the DPRK government had at least known of and possibly approved these operations.[49]

4. After SPE announced the release of the movie 'The Interview', which was to depict a fictional Kim Jong-Un in unfavourable light, the North Korean government threatened retaliation in a letter sent to the US National Security Council.[50] Following the operation against SPE, North Korea issued a long statement praising the authors, while carefully disavowing any responsibility for the operation.[51]

In the following section, we focus on these alleged linkages and analyse whether, if accepted at face value, they would suffice for the attribution of the conduct underlying the relevant hostile cyber operations to North Korea under international law.

3 SUBSTANTIVE ASPECTS: ATTRIBUTION OF CONDUCT

As shown in the preceding section, the affidavit in the *Park* case suggests a number of connections between the alleged authors of the relevant hostile cyber operations and North Korea. In its executive summary, the affidavit even asserted that Mr Park and his accomplices were working 'on behalf of' the North Korean government.[52] Such a formulation is particularly significant from the perspective of international law as the question of attribution essentially relates to 'which persons should be considered as acting *on behalf of* the State, i.e. what constitutes an "act of the State" for the purposes of State responsibility'.[53] Accordingly, the question analysed in this section is whether any of the alleged linkages might suffice to establish attribution of Mr Park's and others' wrongdoing to North Korea under international law.

At a political level, the United States has made it clear that it held North Korea accountable for these incidents. In particular, the US Department of the Treasury sanctioned Chosun Expo on the same day as the criminal charges against Mr Park were unsealed.[54] It stated that it was sanctioning the company 'for being an agency, instrumentality, or controlled entity of the Government of North Korea'.[55] The statement made it clear that the US did not see Chosun Expo as an autonomous actor; instead, the statement noted that it was 'North Korea [who] has demonstrated a pattern of disruptive and harmful cyber activity' and that the US policy was 'to hold North Korea accountable'.[56] In a press briefing held a few months later at the White House, the then Homeland Security Adviser Tom Bossert added expressly that 'the United States [was] publicly attributing the

[49] ibid, para 272.

[50] ibid, para 84 ('We remind you once again that the production of such kind of movie defaming the supreme dignity that our Army and people sanctify is itself the evilest deed unavoidable of the punishment of the Heaven. … Once our just demand is not put into effect, the destiny of those chief criminals of the movie production is sure to be fatal and the wire-pullers will get due retaliation.').

[51] Full Text of Statement From North Korea's National Defence Commission (21 December 2014) <https://variety.com/2014/film/asia/full-text-of-statement-from-north-koreas-national-defence-commission-1201385111/> (hereafter DPRK NDC statement).

[52] Affidavit (n 27) para 6.

[53] ASR (n 11) art 2, commentary para 5 (emphasis added).

[54] Treasury Targets North Korea for Multiple Cyber-Attacks (6 September 2018) <https://home.treasury.gov/news/press-releases/sm473>.

[55] ibid.

[56] ibid.

massive WannaCry cyberattack to North Korea'.[57] In addition, several private actors were of the same view,[58] including, most prominently, Microsoft.[59]

Modern international law begins from the presumption that the conduct of non-State actors such as private companies or individuals is not attributable to States.[60] In this respect, the law is based on the voluntaristic premise that only acts willed by an autonomous person may be attributed to that person.[61] Accordingly, a legally meaningful and sufficient link must be found between a particular conduct and a State in order for that State to be deemed in law to have willed for that conduct to occur. In this regard, several such forms of linkages between Mr Park's alleged behaviour and North Korea should be considered to determine the attribution issue concerning these incidents.

The first of these linkages—or, more precisely, modes of attribution—is the connection that exists between the conduct of a State organ and the State that that organ is a part of (Article 4 of the Articles on State Responsibility). For instance, cyber operations conducted by the US Cyber Command personnel are attributable to the US given that the Cyber Command is part of the US armed forces and thus a State organ.[62] Similarly, operations conducted by North Korea's intelligence agency, the Reconnaissance General Bureau, are attributable to North Korea.[63] However, publicly available sources give little indication that Mr Park belonged to any particular organ of North Korea. The affidavit comes closest to such assessment when it says that Mr Park 'was a programmer *employed by the government* of North Korea'.[64] To be sure, if he had formally been an employee of the North Korean government, that would have made him a State organ and his conduct in that capacity would have been attributable to North Korea.[65] However, this sentence is found in the executive summary section of the affidavit and a careful examination of the remainder of the document reveals that the sentence—likely inadvertently—omits a crucial link in the chain of connection between Mr Park and the government: the company Chosun Expo. The rest of the text makes it clear that he was in fact employed by that company, which the investigators described only as a 'front' of the North Korean government.[66] In any event, there seems to be no direct

---

[57] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (19 December 2017) <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>.

[58] Z Shoorbajee, 'Private sector played critical role in WannaCry attribution, ODNI official says' *CyberScoop* (20 July 2018) <https://www.cyberscoop.com/wannacry-north-korea-odni-ctiic-tonya-ugoretz/>.

[59] N Harley, 'North Korea behind WannaCry attack which crippled the NHS after stealing US cyber weapons, Microsoft chief claims' *The Telegraph* (14 October 2017) <https://www.telegraph.co.uk/news/2017/10/14/north-korea-behind-wannacry-attack-crippled-nhs-stealing-us/>.

[60] ASR (n 11) art 8, commentary para 1.

[61] cf O de Frouville, 'Attribution of Conduct to the State: Private Individuals', in Crawford, Pellet, and Olleson (n 10) 261.

[62] cf J-M Henckaerts and L Doswald-Beck (eds), *Customary International Humanitarian Law* (CUP 2005) vol 1, 530–31 ('The armed forces are considered to be a State organ, like any other entity of the executive, legislative or judicial branch of government.').

[63] On the structure and functioning of the RGB, see further Kong, Jim, and Lim, 'The All-Purpose Sword: North Korea's Cyber Operations and Strategies' in T Minárik et al, *Silent Battle* (CCD COE 2019) 147–48.

[64] Affidavit (n 27) para 6.

[65] cf ASR (n 11) art 4, commentary para 6 (noting that the notion of a State organ is intended in the most general sense and extends to all individuals or legal persons, however classified, who make up the organization of the State).

[66] Affidavit (n 27) para 6 ('PARK was employed by Chosun Expo Joint Venture, which is also known as "Korea Expo Joint Venture" or simply "Chosun Expo" (as it is referred to herein), a company that is a front for the North Korean government.'); similarly ibid paras 264, 269, 289, 322, 334.

evidence suggesting that Mr Park was either formally employed by the government or otherwise formally integrated in the structure of the North Korean government at the time of these cyber operations. As such, there seems to be no direct evidence showing that his conduct was attributable to North Korea under Article 4.

The second potentially applicable mode of attribution relates to entities empowered to exercise the governmental authority of a State (Article 5 of the Articles on State Responsibility). Such entities need not be part of the formal structures of a State and they normally enjoy a legal personality separate from that of the State.[67] In theory, a company such as Chosun Expo could thus qualify—but it would have to be established that it was actually empowered by the North Korean domestic law to exercise prerogatives of public power on behalf of the State.[68] In practice, there is no direct evidence that Chosun Expo was given such powers. It appears that all known links between the North Korean government and the company were of an operational and practical, rather than formal or legislative, nature.[69] Accordingly, there is no direct evidence showing that Mr Park's conduct while in employment of Chosun Expo was attributable to North Korea under Article 5.

The third mode of attribution relevant to Mr Park's case concerns attribution of the conduct of persons acting under the instructions, direction, or control of a State (Article 8 of the Articles on State Responsibility). These three standards are disjunctive—in other words, it suffices that one of them be met for the relevant conduct to be imputed to the State in question.[70] Each of the standards is slightly different, but they share a common feature in the need to establish a form of subordination between the non-State actor and the potentially responsible State.[71]

With respect to the first standard of 'instructions', Mr Park and his collaborators would have to have been factually subordinate to North Korea at the specific moment when the government had supposedly decided to commit the incidents in question. In addition, the hackers would had to have been 'specifically charged'[72] by North Korea to undertake the relevant cyber operations—but no such 'smoking gun' appears to have materialized. By contrast, the mere fact that the hackers and the government have shared their political goals and aims[73] does not suffice for the purposes of attribution under the 'instructions' heading.[74]

There are some indications that the connection between Mr Park and North Korea might have fulfilled the second criterion of 'directions'. This standard is met if an organ of a State 'provided the direction pursuant to which the perpetrators of the wrongful act acted'.[75] With respect to the

---

[67] D Momtaz, 'Attribution of Conduct to the State: State Organs and Entities Empowered to Exercise Elements of Governmental Authority', in Crawford, Pellet, and Olleson (n 10) 244.

[68] cf ASR (n 11) art 5, commentary para 3 (noting that for attribution under Article 5, an entity must be 'empowered, if only to a limited extent or in a specific context, to exercise specified elements of governmental authority').

[69] See Affidavit (n 27) para 269 et seq.

[70] ASR (n 11) art 8 commentary para 7.

[71] K Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (2016) 21 JCSL 405, 426–27.

[72] cf *Nicaragua* (n 17) sep op Judge Ago, para 16.

[73] See, eg, DPRK NDC statement (n 51) ('Fighters for justice including 'guardians of peace' … turned out in the sacred drive for cooperation in the fight against the U.S. to defend human justice and conscience and to dismember the U.S. imperialists').

[74] Mačák (n 71) 415 ('the fact of a goal shared by the State and the private actor is insufficient without further evidence establishing the subordination between the two').

[75] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina*

WannaCry incident, the US Homeland Security Adviser Tom Bossert expressly said that '[w]e're comfortable in this case … that is [sic] was *directed by* the government of North Korea.'[76] As the WTO Appellate Body stated in the 2005 *US-DRAMS* report, the fact of such direction is normally evidenced by 'some form of threat or inducement'.[77] With respect to Chosun Expo, there is some evidence of financial and disciplinary subordination of its employees to the North Korean government, suggesting that these employees had to remit a large part of their salary to the government while they were dispatched to China and that their actions in China were monitored by a North Korean political attaché.[78] In our view, this does not by itself suffice to establish a continuous relationship of subordination between North Korea and Chosun Expo required by the law.[79] However, if such additional evidence was found, particularly if it demonstrated that North Korea led the steps to be taken in the commission of the operations in question,[80] a plausible case could be made that the incidents were attributable under the 'directions' criterion.

Next, the conduct of Mr Park and his accomplices could be attributed through the third criterion of 'control'. In this regard, it would have to be proved that North Korea had 'effective control'[81] of the operations in the course of which the relevant potential violations of international law were committed.[82] This means that North Korea would have had to go beyond merely supporting Chosun Expo through financing, organizing, training or equipping;[83] it would have to have been able to control the beginning of the relevant operations, the way they were carried out, and their end.[84] This is obviously a very high bar and the information in the public domain seems to fall well short of it. For instance, the affidavit mentions that the accounts from which the hostile operations were launched were used without much restriction, which in the specific heavily-monitored North Korean context suggests that the use of these accounts 'was likely regime-sanctioned and approved'.[85] However, even if a State knows of certain acts of a non-State actor, those acts could still have been committed without the control of the State in question.[86] General approval of the use of accounts, which happen to be used for such acts, does not necessarily establish 'effective control' for the purposes of attribution under international law either.

As a final possible mode of attribution, it should be considered whether North Korea could be deemed to have acknowledged and adopted the relevant malicious operations as its own (Article

v Serbia and Montenegro) (Judgement) [2007] ICJ Rep 43, para 406 (hereafter *Bosnian Genocide*).

[76] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (19 December 2017) <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>.

[77] *United States — Countervailing Duty Investigation on Dynamic Random Access Memory Semiconductors (DRAMS) from Korea* Report of the Appellate Body (27 June 2005) WT/DS296/AB/R, para 116.

[78] Affidavit (n 27) para 271.

[79] cf Mačák (n 71) 417–19 (discussing the criterion of 'direction' in the cyber context).

[80] cf L Cameron and V Chetail, *Private Military and Security Companies under Public International Law* (CUP 2013) 209 ('in the case of "direction" it is necessary that the state leads the steps to be taken in the commission of the unlawful conduct').

[81] On the propriety of the 'effective control' test in this context (as opposed to the 'overall control' test and other possible standards), see generally Mačák (n 71) 420–26.

[82] cf *Nicaragua* (n 17) para 115; *Bosnian Genocide* (n 75) para 400.

[83] *Nicaragua* (n 17) para 115; *Armed Activities on the Territory of the Congo (DRC v Uganda)* (Judgment) [2005] ICJ Rep 116, para 160 ('training and military support' does not suffice for the finding of control).

[84] S Talmon, 'The Responsibility of Outside Powers for Acts of Secessionist Entities' (2009) 58 ICLQ 493, 503.

[85] Affidavit (n 27) para 272.

[86] cf *Nicaragua* (n 17) para 115 (holding that acts that were not 'directed or enforced' by the United States 'could well be committed by members of the *contras* without the control of the United States').

11 of the Articles on State Responsibility). There is no doubt that the North Korean government was elated about the SPE hack. In fact, in a December 2014 statement, the North Korean National Defence Commission praised the hackers for having 'meted out a stern punishment of justice' and added expressly that it 'highly estimates the righteous action taken'.[87] However, for attribution under Article 11, a mere expression of a State's verbal endorsement of conduct does not suffice—by contrast, the State must clearly indicate its intention to accept responsibility for that conduct.[88] This can be done expressly, but in that regard the statement remained adamant that North Korea had nothing to do with the hack.[89] In addition, the assumption of responsibility may also be inferred from the conduct of the State in question,[90] particularly if it 'deci[des] to perpetuate' the facts on the ground.[91] For instance, if North Korea had intentionally employed its cyber capabilities to protect Chosun Expo against counter-cyber operations while the attacks were underway, this would have been a strong indicator of adoption of Chosun Expo's conduct as North Korea's own.[92] However, nothing of the sort was reported in the affidavit in connection with any of the incidents. Therefore, it appears that the high bar of acknowledgment and adoption has not been met and, consequently, there is no direct evidence showing that the conduct underlying the relevant operations was attributable to North Korea under Article 11 either.

Overall, it is our view that the evidence adduced in the affidavit and otherwise available in the public domain, even if accepted at face value, does not amount to direct evidence meeting any of the relevant standards of attribution under international law. Consequently, further evidence, particularly on the relationship between Mr Park and Chosun Expo on the one hand and North Korea on the other hand, would need to be identified in order to substantiate a claim on attribution. But what standard of proof would apply to the production of such evidence and what types of evidence would a claimant State be permitted to adduce? These are the questions to which we turn in the next section.

4 EVIDENTIARY MATTERS: STANDARD OF PROOF AND INDIRECT EVIDENCE

The ILC's Articles on State Responsibility, discussed in the preceding section, have clarified the substantive rules of attribution under international law. However, the Articles expressly excluded from their scope evidentiary issues such as the degree of proof required to establish attribution or any other aspects of State responsibility.[93] In the context of adjudication, the required level of proof is called the standard of proof.[94] Although related, the notion of standard of proof is different from the burden of proof.[95] The burden of proof determines which of the parties to a

[87] DPRK NDC statement (n 51).

[88] ASR (n 11) art 11, commentary para 6.

[89] DPRK NDC statement (n 51) ('[T]he U.S. and its followers are groundlessly trumpeting that the recent cyber attack was made by the DPRK. […] U.S. President Obama is recklessly making the rumor about "DPRK's cyber-attack on Sony Pictures" a fait accompli').

[90] ASR (n 11) art 11, commentary para 9.

[91] *United States Diplomatic and Consular Staff in Tehran (Tehran Hostages)* (Judgment) [1980] ICJ Rep 3, para 74.

[92] *Tallinn Manual 2.0* (n 16) rule 17(b), commentary para 16.

[93] ASR (n 11) ch III, commentary para 4 ('Questions of evidence and proof of such a breach fall entirely outside the scope of the articles.'); ibid, art 19, commentary para 8 ('Just as the articles do not deal with questions of the jurisdiction of courts or tribunals, so they do not deal with issues of evidence or the burden of proof.').

[94] See A Riddell and B Plant, *Evidence before the International Court of Justice* (BIICL 2009) 80, 123.

[95] On the allocation of the burden of proof in the cyber context, see further I Brunner, M Dobrić and V Pirker, 'Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards before the ICJ' (2014–2015) 25 Finnish

dispute must present evidence on a certain issue before the court, whereas the standard of proof determines whether the party bearing the burden of proof has discharged its burden and thus convinced the court on that issue.[96] In this section, we examine the standard of proof required in ICJ cases in order to assess the extent of flexibility accepted in proving attribution in inter-State disputes.[97]

Different international tribunals have taken different approaches to the question of standard of proof. In the area of international criminal law, the 'beyond reasonable doubt' standard has been established as the required standard of proof,[98] as reflected in the Rome Statute of the International Criminal Court (ICC): 'In order to convict the accused, the Court must be convinced of the guilt of the accused beyond reasonable doubt.'[99] By contrast, there is no equivalent provision in the ICJ Statute and the ICJ itself has so far refrained from laying down a clear set of rules relating to the standard of proof.[100] However, the issues relating to the standard of proof before the ICJ have been addressed to some extent in the scholarly literature and it is possible to draw out some tendencies in the ICJ's approach on that basis.[101]

In the *Corfu Channel* judgment, with respect to a UK allegation that Albania was responsible for laying mines that later exploded and caused damage to two UK vessels, the ICJ held that '[a] charge of such exceptional gravity against a State would require a degree of certainty that has not been reached here.'[102] This statement implies that the gravity of a charge against a State affects the required standard of proof. Confirming this understanding, Judge Higgins noted in her separate opinion to the *Oil Platforms* judgment that there is a general agreement that 'the graver the charge the more confidence must there be in the evidence relied on'.[103] Therefore, it appears that more serious charges require a higher standard of proof.[104]

This general approach seems to be supported in individual cases of the Court. Accordingly, in the *Bosnian Genocide* case, the ICJ noted that the allegations of genocide, as 'charges of exceptional gravity', had to be 'proved by evidence that is fully conclusive'.[105] In assessing questions of

---

Yearbook of International Law 75, 95–96 and 98–100.

[96] See, eg, M Benzing, 'Evidentiary Issues' in A Zimmermann and CJ Tams (eds), *The Statute of the International Court of Justice: A Commentary* (OUP 2019) 1382, 1403.

[97] See also text to nn 20–24 above.

[98] D Jacobs, 'Standard of Proof and Burden of Proof' in G Sluiter et al (eds), *International Criminal Procedure: Principles and Rules* (OUP 2013) 1143.

[99] Rome Statute of the International Criminal Court (opened for signature 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90, art 66(3). Other international criminal tribunals have included the identical standard in their rules of procedure and confirmed it through case-law building on the presumption of innocence established in their statutes. See, eg, ICTY Rules of Procedure and Evidence, rule 87(A); Statute of the International Criminal Tribunal for the former Yugoslavia, UN Doc S/RES/827 (25 May 1993) (last amended 7 July 2009) art 21(3); *Prosecutor v Delić*, Case No. IT-04-83-T, Judgement (15 September 2008) para 23.

[100] R Teitelbaum, 'Recent Fact-Finding Developments at the International Court of Justice' (2007) 6 LPICT 119, 124; Riddell and Plant (n 94) 125–26; M Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50 Texas ILJ 233, 248.

[101] See generally A Gattini, 'Evidentiary Issues in the ICJ's *Genocide* Judgment' (2007) 5 JICJ 889, Riddell and Plant (n 94); Roscini (n 100); Brunner, Dobrić and Pirker (n 95); Benzing (n 96).

[102] *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 17.

[103] *Oil Platforms (Islamic Republic of Iran v United States of America)* (Merits) [2003] ICJ Rep 161, sep op Judge Higgins, para 33.

[104] Riddell and Plant (n 94) 132–36; Brunner, Dobrić and Pirker (n 95) 84; JJ Quintana, *Litigation at the International Court of Justice* (Brill 2015) 405–08.

[105] *Bosnian Genocide* (n 75) para 209.

attribution of specific genocidal acts to the Federal Republic of Yugoslavia, the Court then applied a standard approximating the 'beyond reasonable doubt' criterion.[106] In cases concerning the use of armed force, the ICJ seems to have applied the slightly lower 'clear and convincing evidence' standard.[107] For example, in *Nicaragua*, it required that the facts of the claim be supported by convincing evidence.[108] By contrast, in cases relating to boundary and maritime delimitation, where the assertions made by parties do not primarily concern allegations of violation of international law, the ICJ seems to apply the 'balance of probabilities' or 'preponderance of evidence' standard, which is similar to the standard of proof adopted in civil cases in common law.[109]

Although discussions on cyber operations have mostly tended to focus on the use of force and self-defence, in reality, cyber operations that are less grave than an unlawful use of force or an armed attack but nevertheless cause damage to the economy or other vital aspects of foreign States are likelier to occur than those that could plausibly amount to an unlawful use of force or an armed attack.[110] The 'graded' approach to the standard of proof developed in the ICJ's case-law[111] would thus suggest that in order to establish responsibility for operations causing damage but not amounting to unlawful use of force, a standard lower than 'clear and convincing evidence' would be used. However, going one notch lower would mean applying the 'preponderance of evidence' standard, which would thus equate cyber interferences below the threshold of use of force with matters of border delimitation which do not primarily concern allegations of violation of international law.

In our view, neither of the possibly applicable standards is without its difficulties in cases such as this one. As noted by Roscini, endorsing the 'preponderance of evidence' standard in the cyber context risks inviting specious claims and intentionally false attribution.[112] By contrast, the 'clear and convincing evidence' standard may be too stringent given that, as seen so well in the *Park* case, the potentially responsible State's refusal to cooperate may frustrate much of the evidence gathering by the injured State.[113] At present, the law in this regard is unsettled and it will have to develop on a case-by-case basis.

The unwillingness of one of the parties to cooperate poses particular difficulties in the proceedings before the ICJ. Unlike a domestic court or even the ICC, whose States Parties are obliged to cooperate with the ICC under Articles 86, 87 and other provisions of the Rome Statute,[114] the ICJ is in a much weaker position when it comes to compelling the parties to provide it with relevant evidence.[115] Article 49 of the ICJ Statute reads: 'The Court may, even before the

---

[106] *Bosnian Genocide* (n 75) para 422.

[107] J Green, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice' (2009) 58 ICLQ 163, 173; Roscini (n 100) 249–50.

[108] *Nicaragua* (n 17) para 29.

[109] See, eg, *Case Concerning the Land, Island and Maritime Frontier Dispute (El Salvador v Honduras, Nicaragua intervening)* (Merits) [1992] ICJ Rep 351, para 248.

[110] See further K Mačák, 'From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law' in H Rõigas et al (eds) *Defending the Core* (CCD COE 2017) 140–41 (arguing that the framework of the law of war is not applicable to the vast majority of the existing cyber operations).

[111] Benzing (n 96) 1404 MN 111.

[112] Roscini (n 100) 252.

[113] See also Brunner, Dobrić and Pirker (n 95) 102 (cautioning that obtaining such evidence 'one-sidedly', i.e., without the consent of the allegedly responsible State, would constitute a violation of that State's sovereignty).

[114] See generally O Bekou and D Birkett (eds), *Cooperation and the International Criminal Court: Perspectives from Theory and Practice* (Brill 2016).

[115] See, eg, Benzing (n 96) 1394 (noting that the Court has no power to compel a party to cooperate with an expert);

hearing begins, call upon the agents to produce any document or to supply any explanations. Formal note shall be taken of any refusal.' This 'cautious wording' suggests that parties are under no legal obligation to comply with the Court's requests made under that provision.[116] However, the ICJ has held that the parties have a general duty to cooperate in the provision of evidence relevant to the resolution of the dispute before it.[117]

The Court has on occasion permitted reliance on indirect and circumstantial evidence. In this respect, the *Corfu Channel* case judgment held that '[b]y reason of this exclusive [territorial] control, the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence.'[118] The Court has later extended the applicability of this principle to all cases in which 'the Respondent may be in a better position to establish certain facts'.[119] This would normally be the case in the cyber context, where it is often impossible to ascertain the actual factual situation without the assistance of the potentially responsible State.[120] Indirect and circumstantial evidence is to be accorded 'special weight' when it is based on a series of facts which are linked together and which lead logically to a single conclusion.[121]

Therefore, in our view, the similarities between the various cyber operations and evidence on the use of IP addresses and e-mail accounts could be accorded some probative value if they fulfil these criteria. In this regard, it is interesting to revisit the evidence discussed earlier in this article.[122] As noted, the evidence available taken individually is insufficient for the purposes of establishing attribution of the relevant cyber operations to North Korea. However, if the present case was litigated before a tribunal such as the ICJ and the respondent State would not discharge its general duty to cooperate with the Court, it is conceivable that the judges would be more inclined to make further inferences from the evidence taken collectively.[123]

---

ibid 1399 (noting that the Court has no power to compel parties to allow a site visit).

[116] CJ Tams and JG Devaney, 'Article 49' in A Zimmermann and CJ Tams (eds), *The Statute of the International Court of Justice: A Commentary* (OUP 2019) 1424. See also ibid 1423 (arguing that the 'real sanction of non-compliance' is that 'the Court may be inclined to draw adverse inferences from a party's refusal' to cooperate).

[117] *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment) [2010] ICJ Rep 14, para 163; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v Serbia)* (Judgment) [2015] ICJ Rep 3, para 173. The obligation of the litigating parties to cooperate with the adjudicative body in question is not limited to the ICJ: see, eg, *Parker Case* (1951) 4 RIAA 35, 39, para 6; *Argentina — Measures Affecting Imports of Footwear, Textiles, Apparel and Other Items* Report of the Panel (25 November 1997) WT/DS56/R, para 6.40.

[118] *Corfu Channel* (n 102) 18.

[119] *Ahmadou Sadio Diallo (Republic of Guinea v Democratic Republic of the Congo)* (Compensation) [2012] ICJ Rep 332, para 15; *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua)* (Compensation) General List 150, Judgment of 2 February 2018, para 33.

[120] See also Brunner, Dobrić and Pirker (n 95) 102–106 (suggesting that the inability of the parties to produce sufficient evidence may be alleviated through the ICJ's power to appoint experts).

[121] *Corfu Channel* (n 102) 18. The ICJ added that such inferences of fact must, however, leave '*no room* for reasonable doubt' (ibid, emphasis original). See further Brunner, Dobrić and Pirker (n 95) 86–87 (interpreting this statement as meaning that where the ICJ allows recourse to indirect evidence, the standard of proof will be elevated to 'beyond reasonable doubt').

[122] See sections 2 and 3 above.

[123] See, eg, *Bosnian Genocide* (n 75) para 206 (noting that the non-disclosure of a requested document places the Court at liberty to draw the relevant conclusions).

5 PROCEDURAL CENTRALIZATION: PROPOSALS OF ATTRIBUTION MECHANISMS

In the light of the limited availability of evidence attributing cyber operations to a State, an independent third-party analysis of the available evidence would be desirable to strengthen its probative value. With respect to the FBI's affidavit in the *Park* case, the FBI Cyber Behavioral Analysis Centre (CBAC) seems to have played an important role.[124] Analysis by such private security researchers as Symantec, BAE Systems and Kaspersky has also been frequently quoted.[125] However, today there is no independent specialized international entity, which would provide impartial analysis of evidence on cyber attribution. In this section, we highlight three possible models that may be considered in this regard.

Firstly, the UN Security Council may establish, on an ad hoc basis, investigative bodies for cyber operations as part of its responsibility for the maintenance of international peace and security.[126] With respect to the situation in North Korea, in 2009 the Council mandated a Panel of Experts with the gathering, examination, and analysis of information regarding the implementation of sanctions against North Korea.[127] The Panel has recently documented several cyber operations that had been attributed to North Korea by third States, including those allegedly conducted by Mr Park.[128] In its present structure, the Panel does not conduct independent investigation and it has to rely on the information provided to it by the States. For example, although it requested information concerning the *Park* case from China, it then simply reproduced the received response that 'China has not found any company registered as Chosun Expo Joint Venture, and currently does not have information regarding Park Jin Hyok'.[129] Nonetheless, it is conceivable that some member of the Council will in the future propose to extend the mandate and resources of this Panel to engage in cyber attribution or to create other similar bodies to do so.

Secondly, recent developments in the context of the Organization for the Prohibition of Chemical Weapons (OPCW) provide some inspiration for the purposes of attribution of cyber operations. In 2013, in order to strengthen the OPCW's mandate in the inspection of chemical weapons in Syria, the UN Security Council adopted resolution 2118 deciding that Syria shall cooperate fully with the OPCW and UN.[130] In 2014, the OPCW's Director-General established a Fact-Finding Mission (FFM) 'to establish facts surrounding allegations of use of chlorine in the Syrian Arab Republic'.[131] In 2015, the UN Security Council's resolution 2235 provided the legal basis for the establishment of an OPCW-UN Joint Investigative Mechanism, which was specifically mandated to identify the users of chemical weapons in Syria.[132] After its mandate expired in 2017, the UK and other States proposed a resolution of the Conference of the States Parties (CSP) mandating the OPCW to establish an arrangement for the attribution of the use of

[124] Affidavit (n 27) para 233.

[125] ibid para 228.

[126] For the role of the Security Council in investigation and fact-finding, see generally H Nasu, 'Investigation *Proprio Motu* for the Maintenance of International Peace and Security' (2004) 23 Aust YBIL 105.

[127] UNSC Res 1874 (2009) op para 26.

[128] See, in particular, UN Doc S/2019/171 (5 March 2019) paras 109–15.

[129] UN Doc S/2019/171 (5 March 2019) para 111.

[130] UNSC Res 2118 (2013) op para 7.

[131] Note by the Technical Secretariat and Summary Report of the Work of the OPCW Fact-Finding Mission in Syria Covering the Period from 3 to 31 May 2014 (OPCW, Office of the Director-General, S/1191/2014, 16 June 2014).

[132] UNSC Res 2235 (2015) op para 5.

chemical weapons in Syria and it was adopted on 27 June 2018.[133] This resolution is now being implemented by the OPCW and the Investigation and Identification Team (IIT) has been carrying out its investigations.[134] It is not yet clear if this mechanism will prove successful and effective, but it is interesting to see such a mechanism established by a two-thirds majority vote in a CSP within the framework of a multilateral treaty. This decision was made possible because the 1993 Chemical Weapons Convention (CWC) provides for decision-making by a two-thirds majority of the present and voting CSP members[135] and because the CWC subjects the State Parties to a general obligation to cooperate with the OPCW.[136] By contrast, there is at present no treaty framework relative to cyber operations, which could be used to set up an analogical attribution mechanism in the cyberspace context.

Thirdly, a further possible solution is to ground an international attribution mechanism on a public-private partnership between States and industry. The earliest proposal in this regard was made in 2016 by Microsoft, which suggested the creation of an organization consisting of experts from governments, industry, academia, and civil society.[137] Since then, several other proposals of international attribution mechanisms have also been made, but Microsoft's attribution organization probably remains the most prominent one among them.[138] According to the original proposal, this organization's peer-reviewed outputs would provide a technical analysis of major hostile cyber operations and, where appropriate, evidence of attribution to States.[139] In a later policy paper, Microsoft clarified that although the organization would work with government experts, 'governments would have no power to veto a final report'.[140] It remains to be seen what comes out of this initiative. Among the hurdles that it would have to overcome is ensuring that the technical competence needed to determine the origin of hostile operations would be

---

[133] See Decision Addressing the Threat from Chemical Weapons Use, OPCW Doc C-SS-4/DEC.3 (27 June 2018) op para 10.

[134] OPCW, 'Note by the Technical Secretariat: Work of the Investigation and Identification Team established by Decision C-SS-4/DEC.3 (dated 27 June 2018)', OPCW Doc EC-91/S/3 (28 June 2019); see also OPCW, Opening Statement by the Director-General to the Ninety-First Session of the Executive Council, OPCW Doc EC-91/DG.24 (9 July 2019) para 17.

[135] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (signed 13 January 1993, entered into force 29 April 1997) 32 ILM 800, art VIII(18).

[136] ibid, art VII(7). With regard to the use of chemical weapons, under the CWC, State Parties have an obligation to allow inspection by the OPCW in principle under the Verification Annex. For example, paragraph 45 of Part II of the Verification Annex provides: 'The inspection team shall, in accordance with the relevant Articles and Annexes of this Convention as well as with facility agreements and procedures set forth in the inspection manual, have the right to unimpeded access to the inspection site. The items to be inspected will be chosen by the inspectors.'

[137] S Charney et al, *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms* (Microsoft 2016) <mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf> 11.

[138] See, eg, J Healey et al, *Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security* (Atlantic Council 2014) 7 (a multilateral 'attribution and adjudication council for cyberattacks rising to the level of "armed conflict"'); JS Davis et al, *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND 2017) 25–42 (a 'Global Cyber Attribution Consortium' composed of non-State actors); E Chernenko, O Demidov, and F Lukyanov, 'Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms' (23 February 2018) <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms> (an 'independent, international cyber court' that would deal with government-level cyber operations); S Droz and D Stauffacher, *Trust and Attribution in Cyberspace* (ICT4Peace 2018) 7–8 (an 'independent network of organisations engaging in attribution peer-review').

[139] Charney et al (n 137) 11–12.

[140] Microsoft, An Attribution Organization to Strengthen Trust Online (undated) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI> 1.

complemented with the sufficient legal competence needed to assign responsibility under international law.[141]

Overall, it appears reasonably clear that there is a growing appetite for the establishment of some independent organization for the attribution of hostile cyber operations.[142] In the long run, an institution of this kind may facilitate the process of assigning responsibility for such operations on the international plane. Until then, States will have to make do with the current decentralized, 'messy and unsystematic' system of accountability.[143] One final aspect of this system is the legal responsibility of States for acts emanating from their territories or from infrastructure under their control—also known as the principle of due diligence—to which we turn in the next section.

6 ALTERNATIVE PATHWAY: DUE DILIGENCE

This section considers the principle of due diligence as a possible alternative pathway to responsibility under international law. The ICJ confirmed the existence of the principle of due diligence in its judgment in the *Corfu Channel* case.[144] The essence of this principle is that every State must ensure that spaces under its jurisdiction are not used in ways detrimental to other States.[145] However, it is a matter of some controversy whether the principle of due diligence reflects a binding obligation applicable to cyber operations.[146] This is reflected in the ambiguity with which the UN-mandated Group of Governmental Experts (GGE) referred to the principle in their most recent consensus report in 2015.[147]

On the one hand, the report contained a phrase that 'States *should* not knowingly allow their territory to be used for international wrongful acts using ICTs'[148]—thus replicating, almost word-for-word, the relevant dictum of the *Corfu Channel* ruling.[149] The report also specified that if the critical national infrastructure of one State is subject to malicious cyber operations emanating from another State and if the latter receives an appropriate request, it is expected to take appropriate

---

[141] cf V Jeutner, 'The Digital Geneva Convention: A Critical Appraisal of Microsoft's Proposal' (2019) 10 JIHLS 158, 164–67 (arguing that the technological expertise that private sector firms would bring to such an organization does not equate to the necessary legal competence).

[142] See also Y Shany et al, 'The Prospects for an International Attribution Mechanism for Cyber Operations' <https://csrcl.huji.ac.il/book/prospects-international-attribution-mechanism-cyber-operations> (introducing an ongoing research project run by the Federmann Cyber Security Research Center at the Hebrew University of Jerusalem, which 'explores the viability of the notion of an international attribution mechanism; its possible structure, authority, process, and scope of consideration; and the role that such a mechanism could play in light of the legal framework governing cyber operations').

[143] KE Eichensehr, 'Decentralized Cyberattack Attribution' (2019) 113 AJIL Unbound 213, 216.

[144] *Corfu Channel* (n 102) 22.

[145] T Stephens and D French, 'ILA Study Group on Due Diligence in International Law: Second Report' (July 2016) <http://www.ila-hq.org/index.php/study-groups> 5–6.

[146] See, eg, MN Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017) 42 Yale Journal of International Law Online 1, 11 (noting that some States reject 'the application of due diligence to cyberspace as a matter of customary law').

[147] 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 A/70/174 (22 July 2015) (hereafter UN GGE 2015).

[148] ibid, para 13(c).

[149] *Corfu Channel* (n 102) 22 ('every State [has the] obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States').

measures to mitigate those acts.[150] On the other hand, the chapeau of the relevant paragraph expressly stated that the cited sentences were merely 'recommendations for consideration by States for voluntary, non-binding norms, rules or principles'.[151] Moreover, the use of the word 'should' in those sentences (as opposed to, for instance, 'must'[152]) seems to indicate the weakness of the obligation.[153] As such, it is clear that the GGE report does not provide unambiguous authority for the binding nature of the principle of due diligence in the cyber context.

By contrast, the Tallinn Manual 2.0 expressly provided that, as a matter of *lex lata*, every State 'must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.'[154] As a corollary of that rule, the Manual considered States to be obliged 'to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States.'[155]

According to the Manual, a State would be in breach of its due diligence obligation with respect to malicious cyber operations such as those in the *Park* affidavit if the following cumulative elements are met: (1) The existence of an act or a series of acts affecting the rights of a victim State;[156] (2) these acts are conducted from or through the territory of the potentially responsible State;[157] (3) they would have been unlawful if conducted by the potentially responsible State;[158] (4) they have serious adverse consequences for the victim State;[159] (5) the potentially responsible State has actual or constructive knowledge of the acts;[160] and (6) the potentially responsible State fails to take feasible measures in response.[161]

While the available facts are not conclusive, the evidence adduced in the affidavit gives some grounds for the construction of a claim for a violation of due diligence in accordance with the Tallinn Manual approach. In particular, the affidavit alleged that the relevant malicious cyber operations were launched from the cyber infrastructure located in the territory of North Korea[162] (condition 2). The affidavit further referred to the extensive monitoring of internet activities emanating from North Korea,[163] which strongly suggests that the government knew or must have

---

150 UN GGE 2015 (n 147) para 13(h).

151 ibid, para 13, chapeau.

152 cf also ibid, para 28(e) ('States *must* not use proxies to commit internationally wrongful acts using ICTs, and *should* seek to ensure that their territory is not used by non-State actors to commit such acts') (two emphases added).

153 See also Schmitt, 'Grey Zones' (n 146) 11 (suggesting that the word 'should' in the GGE report indicates a 'hesitancy to accord the rule *lex lata* status'); Moynihan (n 18) 24–25 (noting, in this connection, the view 'that in the cyber context there is no legal obligation but that applying due diligence would be good practice').

154 *Tallinn Manual 2.0* (n 16) rule 6.

155 ibid, rule 7.

156 *Corfu Channel* (n 102) 22; *Tallinn Manual 2.0* (n 16) rule 6, commentary paras 2 and 15.

157 *Tallinn Manual 2.0* (n 16) rule 6.

158 ibid, rule 6, paras 18–24.

159 ibid, rule 6; see also ET Jensen and S Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer' (2017) 95 Texas Law Review 1555, 1566 (asserting that the notion of serious adverse consequences is 'generally accepted').

160 *Tallinn Manual 2.0* (n 16) rule 6, paras 37–42.

161 ibid, rule 6, para 43; ibid, rule 7, commentary paras 2 and 18.

162 Affidavit (n 27) para 272.

163 ibid, para 272.

known about the operations[164] (condition 5). Given the apparent absence of any measures in response, it would be fair to conclude that the government also failed to undertake its best efforts to terminate the operations[165] (condition 6).

As for the three remaining conditions, the effect on the rights of the victim States as well as the putative unlawfulness of the operations (conditions 1 and 3, respectively) both relate to matters of primary law, which fall outside of the scope of this article.[166] Nonetheless, we are of the view that, assuming that cyber operations below the threshold of prohibited use of force or intervention may violate some rule of international law,[167] these two conditions could well be met, too. Finally, it might also be questioned whether the malicious cyber operations in question resulted in 'serious adverse consequences' (condition 4). After all, even the Tallinn Manual experts admitted that the exact contours of this criterion, borrowed from international environmental law,[168] are unsettled in international law.[169] Of the incidents referred to in the affidavit, the one that arguably comes the closest to meeting the criterion is WannaCry, which allegedly affected over 1,000 pieces of diagnostic equipment in the UK and necessitated the cancellation of thousands of patient appointments.[170] This is because prompt and efficient patient care is a critical government service, the denial of which would likely be perceived by States as a serious adverse consequence.[171]

In sum, where all of the applicable conditions are met, due diligence may provide an alternative pathway to international responsibility—or, in other words, a 'palliative to the attribution problem'.[172] However, the precise legal framework of cyber due diligence in international law remains in need of further clarification and development.[173]

7 CONCLUSIONS

Despite the undeniable effort that went into the preparation of the case against Mr Park, it is exceedingly unlikely that he will ever be tried in person on American soil.[174] By contrast, we can be virtually certain that incidents such as those with which he has been charged will continue to plague inter-State relations in the foreseeable future. It is therefore useful to summarize the lessons learned from the *Park* case for the attribution of cyber operations in international law.

---

[164] cf *Tallinn Manual 2.0* (n 16) rule 7, commentary para 10 ('should a State elect to monitor cyber activities on its territory, the fact that it is doing so may bear on whether it has knowledge of any cyber operations directed at another State from its territory').

[165] cf F Delerue, *Cyber Operations and International Law* (CUP 2020) 367 (noting that under the due diligence obligation, 'the State is expected to undertake its "best efforts" to terminate the cyber operation').

[166] See text to nn 18 above.

[167] On which see text to nn 14–17 above.

[168] *Tallinn Manual 2.0* (n 16) rule 6, commentary para 25; see also *Trail Smelter Case* (1941) 3 RIAA 1905, 1965 ('[N]o State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of *serious consequence*') (emphasis added).

[169] *Tallinn Manual 2.0* (n 16) rule 6, commentary para 25.

[170] Affidavit (n 27) para 225.

[171] cf *Tallinn Manual 2.0* (n 16) rule 6, commentary para 27 (considering that the requisite harm would be met if a malicious cyber operation rendered unusable 'a website providing critical government services').

[172] Delerue (n 165) 374.

[173] Schmitt, 'Grey Zones' (n 146) 11–13.

[174] See also T Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018) 142 (noting that while the arrest and prosecution of hackers living abroad is highly unlikely, the indictments serve an important naming and shaming function).

To begin with, the evidence adduced against Mr Park confirms that the technical side of attribution might be non-trivial, but it is not impossible. The difficulties include the availability of human and technical resources as well as the need for effective international cooperation. Yet, provided that these obstacles can be overcome, the *Park* case indicates that at least some States now have the capacity to uncover the origin of specific malicious cyber operations and identify their authors (section 2).

While dramatic progress has been made with respect to technical attribution in cyberspace, the same has not happened with respect to the legal attribution to States. The international law of attribution, as reflected in the 2001 Articles on State Responsibility, appears too stringent for the attribution of cyber operations to States. Analysis of the evidence contained in the affidavit against Mr Park strengthens this impression (section 3).

The apparent stringency of the substantive standards is exacerbated by the lack of clarity of the applicable international procedural law. Even if a case was brought before one of the international tribunals, the relevant rules concerning the applicable standard of proof and the admissibility of indirect or circumstantial evidence are unsettled and ambiguous. However, the jurisprudence of the ICJ indicates that indirect and circumstantial evidence can be relied upon if direct evidence is not available due to the lack of cooperation from the territorial State and the required standard of proof can be lowered in the cases of lesser gravity (section 4).

To facilitate the collection of credible evidence the establishment of an independent international body that would be tasked with the attribution of malicious cyber operations would be useful. Several such attribution mechanisms have been proposed recently and it is clear the appetite for an institution of this kind is growing. However, for now the decentralized system based on an *omnium gatherum* of private and public stakeholders, each conducting their own attribution assessment, is likely to persist (section 5).

Another solution is to look, so to speak, outside of the attribution box and consider other pathways to responsibility. In the international law context, this could be achieved by reference to the principle of due diligence. As Mr Park's case demonstrates, the available evidence might suffice, except for the unsettled issues on the threshold for the application of the due diligence principle, to meet some of the conditions for a claim that a State has violated its international legal obligations by failing to take feasible measures in order to stop or at least mitigate malicious cyber operations with adverse effects on other States (section 6).

Overall, the challenges of attribution of cyber operations discussed in this article confirm the need, expressed time and again in the literature, for States to clarify their views on the interpretation of the existing international law to cyber issues.[175] A few States have already done so;[176] others should follow, as well. An excellent opportunity to drive the development of the law in this area presents in the two UN-mandated processes that commenced their work in 2019: the

[175] See, eg, K Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace', in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace* (CCD COE 2013) 175; MN Schmitt and S Watts, 'The Decline of International Humanitarian Law *Opinio Juris* and the Law of Cyber Warfare' (2015) 50 Texas International Law Journal 189, 230–31; K Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (2017) 30 Leiden Journal of International Law 877, 896–98.

[176] See, eg, BJ Egan, 'International Law and Stability in Cyberspace' (10 November 2016) <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> (United States); Wright (n 15) (United Kingdom);; 'President of Estonia: International Law Applies Also in Cyber Space' (29 May 2019) <https://www.president.ee/en/meedia/press-releases/15243-president-of-estonia-international-law-applies-also-in-cyber-space/> (Estonia); Dutch 2019 Letter to Parliament (n 16); French 2019 Position Paper (n 16).

renewed UN GGE and a newly established Open-Ended Working Group (OEWG).[177] In addition to soliciting the relevant *opinio juris* from the participating States, these groups should discuss how to facilitate the attribution of cyber operations in general, including the possible establishment of an international attribution mechanism. In doing so, they can contribute further to addressing the attribution problem, and thus to making cyberspace a more stable and secure domain.

[177] See further UN, 'Developments in the field of information and telecommunications in the context of international security' (undated) <https://www.un.org/disarmament/ict-security/>.