How can evidentiary standards be regulated at the international level for verifiable and transparent attributions of cyberattacks to states?

Blauth, Tais; Gstrein, Oskar Josef

CfDS
CENTER FOR DIGITAL SOCIETY

Data Research Centre
University of Groningen Campus Fryslân

university of groningen
campus fryslân

Nuffic
meet the world

How can evidentiary standards be regulated at the international level for verifiable and transparent attributions of cyberattacks to states?

Taís Fernanda Blauth and Dr Oskar J. Gstrein

This project is funded by
the Netherlands' Ministry of Foreign Affairs
and managed by **Nuffic Neso**.

Introduction

Individuals, private organisations, and the public sector are increasingly reliant on digital technologies and infrastructures to function. This scenario of reliability on technology and growing digital data sets is explored by hackers, who can cause extensive harms. A cyberattack might affect, for instance, the data of one individual, but it can also affect the security and critical infrastructure of a state.[1] For this reason, there is a general interest in holding the perpetrator(s) accountable and suppressing future attacks. In this context, the attribution of a cyberattack is critical, considering its purpose of assigning responsibility for conducting a cyberattack. The process of attribution has technical, legal, and political aspects. Technical attribution involves forensic investigation to identify the origin of an attack; legal attribution refers to the legal determination of responsibility; and political attribution involves attributing cyberattacks to states or to entities linked to a state.[2] This essay will focus on political attributions, which have emerged as a possible course of action for foreign policy when responding to attacks such as "Wannacry" and "NotPetya".[3]

Political cyberattack attributions, which are increasingly common,[4] are critical (1) to maintain strategic stability through deterrence and escalation control and (2) as a way for states to assign responsibility and denounce violations of norms in cyberspace.[5] However, such attributions might suffer from a lack of credibility if they are not accompanied by sufficient evidence. Consequently, such declarations often cannot produce the desired effect of "naming and shaming".[6]

One way of making political cyberattack attributions more credible and trustworthy is by establishing evidentiary standards that states should follow when making public declarations. More substantiated attributions could lead to a better understanding of cyberattacks and increase trust. However, substantiating attributions would require states to disclose their sources and methods, which can be undesirable for reasons of confidentiality and secrecy.

---

1 In this essay "cyberattack" describes (malicious) intrusions of a network or a computer. Throughout the essay the term does not necessarily refer to an "attack" that would evoke the international law on the use of force. For similar usages of the term, see Kristen E Eichensehr, 'The Law and Politics of Cyberattack Attribution' [2020] U.C.L.A. Law Review 520-598.

2 Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31 The European Journal of International Law 941, 942–946.

3 Florian J Egloff, 'Contested Public Attributions of Cyber Incidents and the Role of Academia' (2020) 41 Contemporary Security Policy 55-81; Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks' (2015) 38 Journal of Strategic Studies 4-37; Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge University Press 2020).

4 Eichensehr (n 1) 522; Tsagourias and Farrell (n 2) 945.

5 Florian J Egloff and Andreas Wenger, 'Public Attribution of Cyber Incidents' [2019] CSS Analyses in Security Policy <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse244-EN.pdf> accessed 19 January 2021.

6 Martha Finnemore and Duncan B Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' [2020] Working Draft <https://ssrn.com/abstract=3347958> accessed 27 January 2021.

The process of attribution, including the procedural and substantive elements, has been widely debated. Scholars, private organisations, and civil society have provided a number of suggestions regarding the creation of institutional mechanisms for public attribution of cyberattacks.[7] It has also been argued that the focus of this discussion should shift towards the development of evidentiary standard guidelines.[8]

This essay explores how evidentiary standards can be regulated at the international level in order to establish verifiable and transparent attributions of cyberattacks to states. It will first analyse current practices for providing evidence, which contributes to understanding the current practice as well as the main issues at stake. Subsequently, the main advantages and difficulties in regulating the presentation of evidence will be analysed and discussed. This overview helps to understand what could hinder regulation, as well as why standards for evidence are important. Finally, I will explore the possibility of regulating this procedure based on customary international law, arguing that such regulation could lead to more verifiable and transparent attributions. To this end, I will reflect on the two constitutive elements of customary international law, namely (1) consistent, general state practice and (2) a sense of legal obligation *(opinio juris)* and how they relate to the current practice.[9]

Current Practice

The current practice of political attribution is not standardized across countries. Currently, States can decide *if* they want to publicly provide evidence when attributing responsibility, *how much* evidence will be given, and *what form* such attribution will take.[10] For instance, in a recent case the United Kingdom, the United States, and Canada decided to jointly condemn the activities performed by the cyber espionage group APT29. This group targeted several organisations working on the development of a COVID-19 vaccine with the alleged goal of stealing information.[11]

---

[7] Egloff and Wenger (n 5); Lahmann (n 4).

[8] 'A Digital Rights Approach to the Tech Accord and the Digital Geneva Convention' (AccessNow 2018) 5 <https://www.accessnow.org/cms/assets/uploads/2018/08/DGC-tech-accord-human-rights.pdf> accessed 19 January 2021.

[9] Eichensehr (n 1) 583; International Law Commission, 'Draft Conclusions on Identification of Customary International Law: With Commentaries' (United Nations 2018) A/73/10 135–138 <https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf> accessed 9 February 2021.

[10] Kristen E Eichensehr, 'The Law and Politics of Cyberattack Attribution' [2020] U.C.L.A. Law Review 520-598; 'Cyber Warfare' (Advisory Council of International Affairs; Advisory Committee on Issues of Public International Law 2011) 77, AIV/No 22 <https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare> accessed 15 January 2021.

[11] 'Advisory: APT29 Targets COVID-19 Vaccine Development' (United Kingdom's National Cyber Security Centre (NCSC); Canada's Communications Security Establishment (CSE); United States' National Security Agency (NSA) 2020) <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development> accessed 15 January 2021.

The states reported that the group is "almost certainly part of the Russian intelligence services".[12] The attribution for the cyberattacks included some evidence that justified this claim, which was made in the form of a joint advisory. This format was a matter of choice, as well as substantiating the declaration.

Considering that providing proof in attributions is not mandatory according to international law, it is not surprising that their form differs as well. It is noteworthy that joint attributions by a coalition of states have demonstrated to be particularly effective, especially due to an added degree of legitimacy.[13] Thus, states might decide to provide evidence as a means to convince others to jointly condemn the incident, aiming to create even stronger political pressure. Nonetheless, this is a matter of policy choice and potentially subject to change. Some states - such as the Netherlands or the United Kingdom[14] - have stressed in the past that political attributions do not require disclosing the underlying evidence at all. Others, such as Switzerland,[15] have provided a detailed report of a cyber incident, even without publicly attributing responsibility to any specific actor. The amount of evidence that is currently provided varies not only according to the country, but also according to the format of the attribution. In the United States, for instance, attributions can take different forms: less detailed press releases,[16] and more detailed technical alerts by the Department of Homeland Security and FBI.[17] Although states usually provide evidence to substantiate political attributions, this is not a legal obligation. Hence, it cannot be expected or required at all times.

Political factors play an important role in the decision of public attribution. Nevertheless, international public law and specific regulation could have a prominent role in determining the adequate procedure to unify requirements across states and to establish standards.[18]

---

[12] ibid 3.

[13] The general understanding is that the more states join an attribution, the more credible the statement. It is expected that these states evaluated the evidence provided in the statement or have gathered proof themselves. See Lahmann (n 4) 277.

[14] 'Letter to the Parliament on the International Legal Order in Cyberspace' (Government of the Netherlands, 26 September 2019) <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> accessed 15 January 2021; Jeremy Wright, 'Cyber and International Law in the 21st Century' (*UK Government*, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 15 January 2021.

[15] GovCERT.ch, 'APT Case Ruag: Technical Report' (MELANI: GovCERT 2016) Technical Report About the Espionage Case at RUAG <https://perma.cc/2XKP-4FAX> accessed 21 January 2021; Egloff (n 4) 74.

[16] 'Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security' (US Department of Homeland Security, 7 October 2016) <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> accessed 19 January 2021.

[17] 'Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors - Alert (TA18-074A)' (Cybersecurity & Infrastructure Security Agency, 15 March 2018) <https://us-cert.cisa.gov/ncas/alerts/TA18-074A> accessed 19 January 2021.

[18] Eichensehr (n 1).

Advantages and difficulties of regulating evidentiary requirements

One of the main advantages of compelling states to provide evidence is that it prevents wrong and false accusations.[19] Such inaccurate accusations could be harmful to the accused state, especially because they are difficult to refute. For instance, the lack of evidentiary support raised doubts in 2015, when the United States claimed that the People's Republic of China (PRC) was responsible for an intrusion of the Office of Personnel Management. The Foreign Ministry of the PRC argued that this claim was mere speculation, calling the use of terms such as *likely* or *suspected* neither "responsible nor scientific". This response concluded with a pledge to "refrain from making groundless accusations".[20] In such situations statements might not have the effect of "naming and shaming",[21] since attributions without proof can be disregarded as speculation. This shows how the political bias embedded in such manifestations induces a lack of trust. Without proper evidence, contestation (or corroboration) is not possible. To reach the desired effect with political statements states should adequately substantiate attributions.

In addition to the contestation problem, political motivations coupled with scarce evidence lead to a skewed understanding of the underlying cyber conflict.[22] Since attributions are important sources to understand more about actors and types of cyberattacks, the risks related to the possibility of wrong accusations should not be taken lightly. For instance, states might make use of false attributions to claim that others believe certain actions (e.g. espionage) are acceptable, which could negatively impact (1) the establishment of norms of responsible behaviour in the cyberspace and (2) the threat perception of the general public.[23] Transparent and verifiable attributions are important to develop a more secure cyberspace, in which state responsibility for incidents are condemned according to internationally recognised standards. For these reasons, adapting or creating standards of evidence in international law would allow a process of contestation, giving more credibility to statements and causing stronger political repercussions. Furthermore, it could lead to a better understanding of the cyber conflict.

---

[19] Kristen Eichensehr, 'Cyberattack Attribution and International Law' (Just Security, 24 July 2020) <https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/> accessed 19 January 2021.

[20] 'Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on June 5, 2015' (*Ministry of Foreign Affairs of the People's Republic of China*, 5 June 2015) <https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1270836.shtml> accessed 19 January 2021.

[21] Finnemore and Hollis (n 6).

[22] Egloff (n 4) 60–62.

[23] Eichensehr (n 19); Egloff (n 4) 56; Eichensehr (n 1) 567–568.

In contrast, one of the main arguments against the establishment of evidentiary standards is the fact that identification of cybercriminals can be technically challenging. Therefore, public attribution might only be possible in a handful of cases.[24] Considering that technical evidence tends to be the basis of the attribution process, this is also a relevant aspect for political attributions.[25] Attribution is a complex, time and resource-consuming forensic process.[26] The reason behind such complex process is mainly the technical efforts of uncovering the details about a given attack. Among the many technical challenges is, for instance, the level of anonymity attackers are able to achieve.[27] This process can be facilitated by the development of cyber forensics, a field that has seen many advancements in recent years.[28] As suggested by *Rid and Buchanan*, multidisciplinary, skilful, resourceful, and adequately managed teams are key to overcome technical difficulties and achieve successful attributions.[29] Thus, even though substantiating attributions might be more technically challenging, the quality of the declarations also increases when they are accompanied with an adequate level of evidence. In this respect, the "quality" of the attributions (i.e. the level of political impact) should be considered more important than the quantity of statements.

Another aspect to consider is that if evidentiary standards were to be established, states would have to reveal sources and methods used to analyse and assess responsibility.[30] The defensive and offensive capabilities of States might be unclear to their competitors, and the confidentiality of technical means available can be a reason to oppose any mandatory requirement for providing proof of responsibility. In other words, States might be resistant to recognise the merits of an obligation to substantiate attributions. However, as many states already provide evidence to some degree, legal procedures might not provoke a significant change in behaviour. Rather, a change in their motivation for providing evidence, from policy choice to a legal requirement could take place. Besides, openness comes with benefits such as increased credibility of "the messenger", increased quality of the attribution, and better defence since open communication can contribute to the improvement of collective security.[31]

---

[24] Egloff and Wenger (n 5).
[25] Rid and Buchanan (n 4) 15.
[26] Egloff and Wenger (n 5).
[27] ibid; Kosmas Pipyros and others, 'Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare' (2016) 24 Information & Computer Security 38-52, 46.
[28] Jawwad A Shamsi and others, 'Attribution in Cyberspace: Techniques and Legal Implications' (2016) 9 Security and Communication Networks 2886; Rid and Buchanan (n 4); Eichensehr (n 1) 529–532.
[29] Rid and Buchanan (n 4).
[30] Eichensehr (n 1) 569; Jack Goldsmith, 'Cybersecurity Treaties: A Skeptical View' in Peter Berkowitz (ed), Future Challenges in National Security and Law (2011) 11 <www.futurechallengesessays.com> accessed 1 February 2021.
[31] Rid and Buchanan (n 4) 26–30.

In summary, regulating evidentiary standards might have more benefits than downsides. Establishing legal requirements will certainly make the process of attribution more complex. At the same time, substantiated public attributions would be more credible and it is likely that they would also provoke stronger political effects. Thus, it is necessary to evaluate how evidentiary standards can be regulated.

Establishment of evidentiary rules via customary international law

Currently, States tend to avoid invoking international law when making political attributions of cyberattacks.[32] *Finnermore and Hollis* suggested that the absence of international law in accusations could mean that "the law is weak – or worse, irrelevant – in holding states accountable for their cyber operations".[33] In fact, international law is unclear regarding the standard of evidence that states must follow when accusing others of internationally wrongful acts.[34] Even in more traditional contexts, such as the use of force in self-defence, evidentiary rules are still unclear.[35]

The UN Group of Governmental Experts (GGE) made some efforts to establish a necessity to provide proof when attributing responsibility for a cyberattack. In a 2015 report it suggests that "accusations of organizing and implementing wrongful acts brought against States should be substantiated".[36] The Experts considered that, by doing so, states would avoid political tensions. However, they also recognised that this is not an obligation under international law.[37] Despite the lack of a legal obligation, scholars, civil society, and political representatives stressed the importance of substantiating accusations against states.[38] This demonstrates a willingness to advance the discussions on the topic. Due to the importance of the topic and the current lack of clarity it is relevant to discuss how this standard can be regulated via international law.

---

[32] Finnemore and Hollis (n 6) 1; 3. Also see 'Advisory: APT29 Targets COVID-19 Vaccine Development' (n 11).

[33] Finnemore and Hollis (n 6) 5.

[34] James A Green, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice' (2009) 58 International and Comparative Law Quarterly 163, 165.

[35] ibid 163; Eichensehr (n 1) 524; 559.

[36] 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations General Assembly 2015) A/70/174 13 <https://undocs.org/A/70/174> accessed 15 January 2021.

[37] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 83 <https://www.cambridge.org/core/product/identifier/9781316822524%23CT-bp-5/type/book_part> accessed 3 February 2021.

[38] 'Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on June 5, 2015' (n 20); Eichensehr (n 1) 583; Egloff and Wenger (n 5) 3.

Standards of proof could be regulated via a dedicated cybersecurity treaty. However, such treaties and agreements have been rejected by some states, such as the United States, due to the difficulties in verifying compliance of the parties.[39] However, when it comes to regulating evidence in attributions, violations of the rule are arguably easier to monitor because statements and proofs are publicised. If a state decides to publish a public attribution without the accompany evidence, it will be immediately clear that the rule of proof is not being followed. Hence, it might be reasonable to discuss the development of a rule of evidence independent from dedicated regulation, such as a cybersecurity treaty. One possible alternative is to form a rule via customary international law. In order to establish it, it is necessary to identify (1) a consistent and general state practice (2) carried out with a sense of legal obligation (opinio juris).[40] Even though the establishment of customary international law takes time and depends greatly on state behaviour, it is considered a particularly relevant way of regulating developing legal issues.[41] Thus, standards of evidence could crystallise as a norm of customary international law.[42]

Currently, there is insufficient state practice and a lack of *opinio juris* when it comes to standards of evidence in political attributions.[43] For this reason, it is necessary to evaluate what should change in state practice. Regarding the first requirement (i.e. consistent and general state practice), it is noteworthy that states already tend to provide some level of evidence in attributions, as previously described.[44] However, even though some level of state practice can be identified, the current practice cannot be considered consistent and general. Thus, this needs to be further developed. For instance, states could agree that all future public attributions will be substantiated by sufficient evidence to enable corroboration and crosschecking. This would lead to a more consistent and general practice, which would then be expected from states making public attributions going forward.

---

[39] Eichensehr (n 1) 570.

[40] ibid 583; International Law Commission (n 9) 135–138.

[41] Gary Brown and Keira Poellet, 'The Customary International Law of Cyberspace' (2012) 6 Strategic Studies Quarterly 126-145, 126.

[42] Eichensehr (n 1) 576–586.

[43] Schmitt (n 37) 83.

[44] As described in section I, many countries' current policy is to provide some level of evidence, sometimes even a sufficient level of evidence that allows crosschecking. See 'Advisory: APT29 Targets COVID-19 Vaccine Development' (n 11); *United States of America v Li Xiaoyu (a/k/a 'Oro0lxy') and Dong Jiazhi* [2020] Eastern District of Washington 4:20-CR-6019-SMJ; GovCERT.ch (n 15).

When it comes to the second requirement (opinio juris), there is currently no general sense that a legal obligation to present evidence exists.[45] Therefore, the understanding of some states that providing evidence is a matter of policy would have to change.[46] In other words, substantiating attributions should be considered as the norm to which states will adhere to. As *Eichensehr* suggests,[47] future attributions and public statements could contain references to customary international law, while states and non-governmental actors should widely criticise evidence-free attributions. If the sense of legal obligation can be recognised, along with state practice, a legally binding rule of customary international law can crystallise over time. Substantiated attributions can serve as proof of practice and, if they "persist and spread over time, states may come to assume that these accusations are evidence of opinio juris".[48] This means that the attributions themselves might serve as building blocks for the creation of international law.

Finally, it is necessary to assess how much evidence should be required. Given the current technical challenges, it is not expected that states should provide an absolute and irrefutable statement: public attributions are part of ongoing processes.[50] This means that after the public political attribution, the evidence provided by the state can undergo further analysis (to be corroborated or refuted). Other states may also join in condemnation, or they may criticise the declaration (depending on their own assessment of the content, format, and evidence). For this reason a "mix of fact and judgement" would still prevail in many cases.[51] Although complete certainty is not expected from cyberattack attributions, states should provide "sufficient evidence".[52] This would be the minimum amount of proof that enables other states, non-governmental organisations, and academic researchers to crosscheck the assessment of the incident.[53] Therefore, an internationally recognised rule should require states to include sufficient evidence (sources and methods) in political attributions in order to make them open to criticism or corroboration. This should be the case even if that statement contains estimative language.

---

[45] For instance, past statements of the Netherlands, United Kingdom, United States, and France demonstrate the understanding that providing evidence is not a legal requirement, but rather a political one. Wright (n 14); 'Letter to the Parliament on the International Legal Order in Cyberspace' (n 14); Eichensehr (n 1) 525–526.

[46] However, note that it is not required that all states accept the rule as an obligation for the development of customary international law; a broad acceptance, coupled with no or little objection, is enough. See International Law Commission (n 9) 135; Brown and Poellet (n 41) 127.

[47] Eichensehr (n 1) 584–585.

[48] Finnemore and Hollis (n 6) 16–17.

[49] ibid 7.

[50] Rid and Buchanan (n 4); Goldsmith (n 30) 10.

[51] Sherman Kent, Sherman Kent and the Board of National Estimates: Collected Essays (Center for the Study of Intelligence 2003) 57 <https://www.hsdl.org/?abstract&did=2903> accessed 28 January 2021.

[52] Eichensehr (n 1) 578.

[53] ibid 578–579; Egloff (n 4) 62–64.

Conclusion

Political attributions of cyberattacks are relevant tools that help to maintain stability through deterrence. They function as a way of denouncing acts that violate acceptable behaviour in cyberspace. Even though the current practice of states is to provide some level of evidence in attributions, this is the reflection of domestic policies rather than an act based on a standardised procedure. In summary, evidentiary standards can be regulated via customary international law, which can only be formed over time. A consistent and general practice of providing an adequate level of evidence, made in compliance with a legal obligation, is a necessary requirement. The process of consolidating a rule as customary international law is cumbersome, but broad agreement on this matter can shift the attribution from a subject of policy to a subject of international law.[54] This would prevent states from shifting their practice of substantiating attributions when convenient. Once attributions are sufficiently substantiated, the crosschecking processes will likely follow. Finally, political statements would become more verifiable and transparent, which could contribute to more stability in cyberspace and the international system.

[54] Eichensehr (n 1) 558.

Bibliography

- 'A Digital Rights Approach to the Tech Accord and the Digital Geneva Convention' (AccessNow 2018) <https://www.accessnow.org/cms/assets/uploads/2018/08/DGC-tech-accord-human-rights.pdf> accessed 19 January 2021
- 'Advisory: APT29 Targets COVID-19 Vaccine Development' (United Kingdom's National Cyber Security Centre (NCSC); Canada's Communications Security Establishment (CSE); United States' National Security Agency (NSA) 2020) <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development> accessed 15 January 2021
- Brown G and Poellet K, 'The Customary International Law of Cyberspace' (2012) 6 Strategic Studies Quarterly 126
- 'Cyber Warfare' (Advisory Council of International Affairs; Advisory Committee on Issues of Public International Law 2011) 77, AIV/No 22 <https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare> accessed 15 January 2021
- Egloff FJ, 'Contested Public Attributions of Cyber Incidents and the Role of Academia' (2020) 41 Contemporary Security Policy 55
- Egloff FJ and Wenger A, 'Public Attribution of Cyber Incidents' [2019] CSS Analyses in Security Policy <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse244-EN.pdf> accessed 19 January 2021
- Eichensehr K, 'Cyberattack Attribution and International Law' (Just Security, 24 July 2020) <https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/> accessed 19 January 2021
- Eichensehr KE, 'The Law and Politics of Cyberattack Attribution' [2020] U.C.L.A. Law Review 520
- Finnemore M and Hollis DB, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' [2020] Working Draft <https://ssrn.com/abstract=3347958> accessed 27 January 2021
- 'Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on June 5, 2015' (*Ministry of Foreign Affairs of the People's Republic of China*, 5 June 2015) <https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1270836.shtml> accessed 19 January 2021
- Goldsmith J, 'Cybersecurity Treaties: A Skeptical View' in Peter Berkowitz (ed), *Future Challenges in National Security and Law* (2011) <www.futurechallengesessays.com> accessed 1 February 2021
- GovCERT.ch, 'APT Case Ruag: Technical Report' (MELANI: GovCERT 2016) Technical Report About the Espionage Case at RUAG <https://perma.cc/2XKP-4FAX> accessed 21 January 2021
- Green JA, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice' (2009) 58 International and Comparative Law Quarterly 163

- International Law Commission, 'Draft Conclusions on Identification of Customary International Law: With Commentaries' (United Nations 2018) A/73/10 <https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf> accessed 9 February 2021
- 'Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security' (*US Department of Homeland Security*, 7 October 2016) <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> accessed 19 January 2021
- Kent S, *Sherman Kent and the Board of National Estimates: Collected Essays* (Center for the Study of Intelligence 2003) <https://www.hsdl.org/?abstract&did=2903> accessed 28 January 2021
- Lahmann H, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge University Press 2020)
- 'Letter to the Parliament on the International Legal Order in Cyberspace' (*Government of the Netherlands*, 26 September 2019) <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyber-space> accessed 15 January 2021
- Pipyros K and others, 'Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare' (2016) 24 Information & Computer Security 38
- 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (United Nations General Assembly 2015) A/70/174 <https://undocs.org/A/70/174> accessed 15 January 2021
- Rid T and Buchanan B, 'Attributing Cyber Attacks' (2015) 38 Journal of Strategic Studies 4
- 'Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors - Alert (TA18-074A)' (*Cybersecurity & Infrastructure Security Agency*, 15 March 2018) <https://us-cert.cisa.gov/ncas/alerts/TA18-074A> accessed 19 January 2021
- Schmitt MN (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, Cambridge University Press 2017) <https://www.cambridge.org/core/product/identifier/9781316822524%23CT-bp-5/type/book_part> accessed 3 February 2021
- Shamsi JA and others, 'Attribution in Cyberspace: Techniques and Legal Implications' (2016) 9 Security and Communication Networks 2886
- Tsagourias N and Farrell M, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31 The European Journal of International Law 941
- Wright J, 'Cyber and International Law in the 21st Century' (*UK Government*, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 15 January 2021
- *United States of America v Li Xiaoyu (a/k/a 'Oro0lxy') and Dong Jiazhi* [2020] Eastern District of Washington 4:20-CR-6019-SMJ