

2020 Policy brief

Application of International Law to Cyber Operations: A Comparative Analysis of States' Views

Przemysław Roguski



THE HAGUE
PROGRAM
for Cyber Norms



Universiteit
Leiden

Table of contents

Executive Summary	1
Introduction	2
Obligations of States under International Law with respect to Cyberspace	4
<i>Sovereignty</i>	4
<i>Non-intervention</i>	7
<i>Prohibition of the Use of Force</i>	9
<i>Due Diligence in Cyberspace</i>	11
State Responsibility	13
<i>Attribution – General Overview</i>	13
<i>Attribution – Standard of Proof</i>	14
<i>Attribution – Indicators</i>	16
<i>Attribution – Duty to Provide Evidence</i>	17
Response Options for States	18
<i>Retorsion</i>	18
<i>Countermeasures</i>	18
<i>State of Necessity</i>	20
<i>Self-defence</i>	21
Conclusion	24
Annex	25

Suggested citation:

Roguski, P. (2020). *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague Program For Cyber Norms Policy Brief. March 2020.

Application of International Law to Cyber Operations: A Comparative Analysis of States' Views

Executive Summary

This policy brief offers a comparative analysis of the positions of seven States on how international law applies to cyber operations. The scope of analysis is limited to peacetime cyber operations; questions regarding the applicability of International Humanitarian Law in cyberspace are not covered. The policy brief analyses States' views with regard to the legal qualification of cyber operations, their attribution and the response options which States have under international law. Upon this analysis, the following (inexhaustive) conclusions can be drawn:

- States mostly agree on the applicability and interpretation of the prohibition of use of force. In this regard, the use of the “scale and effects” test to determine the comparability of cyber attacks to “traditional” examples of use of force is advocated.
- All States agree on the existence of the right to self-defence in the cyber context, but vary on the precise conditions for its application.
- States mostly agree on the applicability and interpretation of the obligation not to intervene in the internal affairs of other States, finding that cyber operations which target the *domaine réservé* and have a coercive effect may constitute such a prohibited intervention.
- States mostly agree on the applicability of the rules on the responsibility of States for internationally wrongful acts, both with respect to the standards of attribution of conduct to a State, as well as to the circumstances precluding wrongfulness (countermeasures, state of necessity).
- States disagree (or did not formulate an opinion) on the existence and applicability of an obligation to respect the sovereignty of another State in cyberspace.
- States disagree (or did not formulate an opinion) on the existence of a right to take collective countermeasures.
- With respect to the following issues, States have formulated varying opinions or did not formulate a position and further clarification is therefore needed: the existence and scope of a duty of due diligence in cyberspace; the technical indicators for attribution of cyber conduct to a State; the standard of proof for attributing cyber conduct to a State; the conditions for the invocation of a state of necessity in cyberspace.

To increase the stability of international relations, it is necessary that not only the general applicability of international law in cyberspace is affirmed, but that there exists a widespread understanding and agreement as to the applicability and interpretation of specific rules of conduct in the context of cyberspace. States can and should contribute to achieving this result by presenting their detailed and reasoned views on the application and interpretation of international law in cyberspace both in general statements (such as those analysed in this brief), as well as with respect to actual cyber attacks. The statements analysed in the present policy brief form the necessary first step; but much remains to be done and more States from around the world should make their voices heard.

Introduction

The question how international law applies to State conduct in cyberspace is one of the most pressing issues of international law today. After the consensus reports of the United Nations Group of Governmental Experts (UN GGE) of 2013¹ and 2015,² which confirmed the applicability of international law to cyberspace, the failure of the 2016-2017 UN GGE to produce a report stopped UN deliberations on this matter for nearly two years. In 2019, the issue has been put back on the agenda and the United Nations General Assembly established not one, but two Groups with the mandate to study how international law applies to States' operations in cyberspace – a new Group of Governmental Experts³ and an Open-ended Working Group (OEWG).⁴ It seems clear from the proceedings of the UN GGE and OEWG so far that there is both great interest in and a need to further clarify how international law applies to State conduct in cyberspace, which could be achieved *inter alia* through the sharing of States' views on this matter,⁵ as included in the mandate of the 2019 UN GGE.⁶

To date, many States have already set out their views on how international law applies to State conduct in cyberspace, either in written responses to the UN Secretary-General pursuant to requests by the UN General Assembly,⁷ speeches by legal advisors, diplomats or politicians, letters to parliament or dedicated policy and strategy documents.⁸ Regardless of their form, these documents and statements, insofar as they contain assertions of rights and obligations under international law, may be taken as evidence of a State's position with respect to its interpretation of the rules of international law applicable to conduct in cyberspace.⁹

-
- 1 UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, UN Doc. A/68/98 (hereinafter *UN GGE Report 2013*).
 - 2 UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015, UN Doc. A/70/174 (hereinafter *UN GGE Report 2015*).
 - 3 UN General Assembly, *Advancing responsible State behaviour in cyberspace in the context of international security*, Resolution of 22 December 2018, UN Doc. A/RES/73/266.
 - 4 UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, Resolution of 5 December 2018, UN Doc. A/RES/73/27.
 - 5 Cf. OEWG, *Chair's working paper in view of the Second substantive session*, suggesting that delegations address the question whether there should be a central repository of national practice in the application of international law, p. 2 [consulted 25.02.2020]; see also the Summary of Consultations with member States of the Organization of American States (OAS), 15-16 August 2019, Washington D.C., observing that “[participants] also noted the that the sharing of views on how States believed international law applies in cyberspace [...] would contribute to better transparency and an environment of mutual understanding”, p. 17 [consulted 25.02.2020].
 - 6 UN General Assembly, *Advancing responsible State behaviour in cyberspace in the context of international security*, Resolution of 22 December 2018, UN Doc. A/RES/73/266, p. 3.
 - 7 See, for instance, the replies from governments listed in UN Documents A/65/154 (2010), A/66/152 and Add. 1 (2011), A/67/167 (2012), A/68/156 and Add. 1 (2013), A/69/112 and Add. 1 (2014), A/70/172 (2015), A/71/172 (2016), A/72/315 (2017) and A/74/120 (2019).
 - 8 It should be added that the *Tallinn Manual 2.0*, while being a very thorough study of international law applicable in cyberspace, represents an academic effort and does not necessarily reflect the views of any particular State or international organisation such as NATO.
 - 9 See Michael Wood, *Second report on identification of customary international law*, UN Doc. A/CN.4/672, para. 75 *et seq.*, where he lists examples of practice reflecting a State's position on (customary) international law.

Out of these examples, this policy brief offers a comparative analysis of the views of seven States, which – in the opinion of the present author – to date have presented the most detailed and comprehensive positions on how international law applies in cyberspace: Australia,¹⁰ Estonia,¹¹ France,¹² Germany,¹³ the Netherlands,¹⁴ the United Kingdom,¹⁵ and the United States¹⁶. The aim of the brief is to discuss observable trends, commonalities and differences between the analysed States in their understanding of the applicability of international law to cyber operations and to offer recommendations with regard to policy options open to States which may be currently in the process of formulating their own views on this matter. The brief is thus not intended to be a scholarly discussion of the matters at hand, although problems with certain positions taken by States may be addressed where appropriate.

This brief's analysis proceeds in three main parts. The first part will address which rules of international law may be implicated by cyber operations. In line with that, questions of internet governance, law enforcement, respect for human rights online and combating terrorism or cybercrime, will not be addressed. Rather, the brief will concentrate on the question which types of State actions in cyberspace (or lack thereof) may violate international law. The second part of the brief will address the question who may be responsible for such violations and how is State conduct to be attributed. The third part will cover the question which response options does the victim State have.

-
- 10 Commonwealth of Australia, Department of Foreign Affairs and Trade. (2017). "Annex A: Australia's position on how international law applies to State conduct in cyberspace", in: *Australia's International Cyber Engagement Strategy*, (hereinafter *Australia: Cyber Engagement Strategy*) [25.02.2020]; and the *2019 International Law Supplement*, (hereinafter *Australia: 2019 Supplement*) [25.02.2020].
 - 11 "President of the Republic at the opening of CyCon 2019". (2019). Speech of Estonian President Kersti Kaljulaid in Tallinn on 29 May 2019 (hereinafter *Estonia: Kaljulaid Speech*) [23.11.2019].
 - 12 French Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (hereinafter *France: Operations in Cyberspace*) [23.11.2019]; for further interest, see also: Secrétariat Général de la Défense et de la Sécurité Nationale, *Revue Stratégique de Cyberdéfense*, 12 February 2018 (in French) [25.02.2020]; and *France's response to Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security" and Resolution 73/266 "Advancing responsible State behaviour in cyberspace in the context of international security"* [25.02.2020].
 - 13 "Cyber Security as a Dimension of Security Policy". (2015). Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London (hereinafter *Germany: Riedel Speech*) [23.11.2019].
 - 14 *Letter to the parliament on the international legal order in cyberspace*. (2019). 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 (hereinafter *Netherlands: Letter to Parliament*) [23.11.2019].
 - 15 "Cyber and International Law in the 21st Century". (2018). Speech by Attorney General Jeremy Wright QC MP on 23 May 2018 (hereinafter *UK: Wright Speech*) [23.11.2019]; UK Ministry of Defence. (2016). *Cyber Primer*, 2nd ed. (hereinafter *UK: Cyber Primer*) [25.02.2020].
 - 16 "International Law in Cyberspace". (2012). Remarks by Harald Hongju Koh, Legal Adviser to the US Department of State, on 18 September 2012, (hereinafter *USA: Koh Speech*) [23.11.2019] and in *Harvard Int'l LJ Online*, 54, December 2012, pp. 1-12 [25.02.2020]; also: "Remarks on International Law and Stability in Cyberspace". (2016). Remarks by Brian J. Egan, Legal Adviser to the U.S. Department of State, on 10 November 2016 (hereinafter *USA: Egan Speech*) [23.11.2019] and in *Berkeley Journal of Int'l Law*, 35 (1), pp. 169-180 (for ease of use, all references in this policy brief will point to page numbers as found in the journal versions of both speeches).

Obligations of States under International Law with respect to Cyberspace

Based on the positions of the analysed States, four distinct rules, which may be applicable in the context of cyber operations, can be identified: the obligation to respect the sovereignty of other States, the obligation not to intervene into the internal affairs of other States, the prohibition of the use of force and an obligation of due diligence. These obligations will therefore constitute the focus of the present comparative analysis.

Sovereignty

One of the most controversial issues with regard to sovereignty in cyberspace is the question whether cyber operations affecting networks in another State's territory violate that State's sovereignty. The answer to this question has a significant impact on a range of other legal issues: from the legality of extraterritorial law enforcement activities (direct access to digital evidence stored abroad, takedown of botnets, takedown of child pornography, terrorist content or otherwise criminal material stored extraterritorially etc.) through the legality of surveillance measures within foreign networks, to the framework of State responsibility. However, only a handful of States have presented detailed views on the matter. Out of the views presented thus far by States, two main approaches can be identified:

- 1) the **sovereignty-as-a-principle approach**, stating that sovereignty is a principle of international law from which certain prohibitive rules (non-intervention, prohibition of the use of force) flow, but does not itself constitute such a rule; and
- 2) the **sovereignty-as-a-rule approach**, stating that there is a primary rule of international law which requires States to respect the (territorial) sovereignty of another State, which is also applicable to State conduct in cyberspace.

Within the **sovereignty-as-a-rule approach**, States differ on when a cyber operation may be found to violate the sovereignty of another State. Here, again, two main approaches can be distinguished:

- a) the ***de minimis* approach**, stating that sovereignty of other States has to be respected when conducting cyber operations, but that there is a *de minimis* threshold for cyber operations, which must be crossed to find a violation of sovereignty; and
- b) the **penetration-based approach**, which argues that every penetration of computer networks located within the territory of a State violates that State's sovereignty.

The sovereignty-as-a-principle approach has been advocated by the **United Kingdom**. In his speech of 23 May 2018, UK Attorney General Jeremy Wright stated that he is “not persuaded that we can currently extrapolate from that general principle [of sovereignty] a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention”.¹⁷ It would follow from this approach that certain types of cyber operations – which fall below the use-of-force threshold and do not constitute an intervention into the internal affairs of a State – are not prohibited under international law, even if they affect the confidentiality, integrity or availability of computer systems or produce physical effects. Whether the result would be the same if the cyber attacks

¹⁷ UK: Wright Speech.

affected critical infrastructure (e.g. power utilities, water supplies etc.), produced widespread effects (e.g. power outage) or interfered with the functioning of (public or private) healthcare facilities (e.g. hospitals) or whether this would be considered as an intervention, is thus far unclear.

Thus far, no other State has directly followed the United Kingdom's position with regard to territorial sovereignty in cyberspace. Three States (**France, Germany and the Netherlands**) have presented views which affirm the existence of a rule of territorial sovereignty in cyberspace, while the United States' position remains unclear. Out of the three States, the Netherlands seems to apply the *de minimis* approach, France the penetration-based approach, while Germany only affirmed that "the use of cyber capabilities might constitute a violation of sovereignty",¹⁸ without elaborating further.

The **Dutch** position on international law in cyberspace firmly rejects the United Kingdom's view (without naming the UK directly), stating that "respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act."¹⁹ It refers in particular to the case law of the International Court of Justice (ICJ), which in the *Nicaragua* case ruled that the US actions with respect to Nicaragua breached the customary international law obligation not to violate the territorial sovereignty of another State.²⁰ With respect to the precise threshold when such a violation occurs, the Dutch government endorses the view of the International Group of Experts in the commentaries to Rule 4 of the *Tallinn Manual 2.0*, whereby a violation of sovereignty is deemed to occur if there is:

- 1) a sufficient degree of infringement upon the target State's territorial integrity; or
- 2) there has been an interference with or usurpation of inherently governmental functions of another state.²¹

The *Tallinn Manual 2.0* continues to discuss when such infringement upon the territorial integrity of a State is sufficient, analysing such factors as physical damage, loss of functionality and infringements falling below the threshold of loss of functionality.²² However, the Dutch position does not elaborate further, only stating that the precise interpretation of these criteria is a matter for debate.²³

The **French** position is also contrary to the UK's view, albeit on different grounds. According to France, "[a]ny cyber attack against French digital systems or any effects produced on French territory by digital means by a State organ [or otherwise attributable to a State] constitutes a breach of sovereignty".²⁴ It is important to note that in the French view, already an unauthorised penetration of "French systems" – and not the effect produced by this penetration in form of physical damage or interference with governmental functions – is sufficient to find a violation of sovereignty. France thus implicitly rejects the view stated by the Netherlands and the

18 *Germany: Riedel Speech.*

19 *Netherlands: Letter to Parliament*, p. 2.

20 *Case concerning military and paramilitary activities in and against Nicaragua* (Nicaragua v. United States of America), Judgment, 27 June 1986, ICJ Rep. 1986, p. 14 [hereinafter *Nicaragua*], paras 213, 252 and 292(5).

21 Michael N Schmitt and Liis Vihul (eds). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, p. 20 (hereinafter: *Tallinn Manual 2.0*).

22 *Ibid.*

23 *Netherlands: Letter to Parliament*, p. 3.

24 *France: Operations in Cyberspace*, p. 7.

Tallinn Manual 2.0 requiring more than *de minimis* effects upon the target State's territorial integrity for a breach of sovereignty. The penetration-based approach is a consequent application of the French cybersecurity incident classification system,²⁵ which qualifies any breach of the confidentiality, integrity or availability of a computer system as a cybersecurity incident. In turn, any cybersecurity incident constitutes a baseline violation for the purposes of both domestic and international law. The precise legal qualification of the incident depends on its level of gravity, ranging from 0 (negligible impact) to 5 (extreme impact), applied on a case-by-case basis.

Two questions remain with regard to the French position. Many remote cyber espionage operations include the penetration of targeted computer systems. Would this mean that such cyber espionage operations violate the sovereignty of the targeted State? And if this is the consequence, how does this relate to the mainstream view that intelligence collection, including by cyber means, is not *per se* regulated by international law?²⁶

Lastly, the **United States'** position with regard to violations of sovereignty in cyberspace appears not to be fully settled. On the one hand, two legal advisers to the US Department of State have confirmed that "States conducting activities in cyberspace must take into account the sovereignty of other States".²⁷ However, not every remote operation involving computers located in another State's territory would be considered *per se* a violation of international law, especially if it has no effects or only *de minimis* effects. These statements seem to support the view that cyber operations may violate a State's sovereignty, albeit only under the *de minimis* approach. However, more recently the US military doctrines of "persistent engagement"²⁸ and "defending forward"²⁹ seem to suggest that the United States deem it permissible under international law to be active in networks located on the territories of third States even preventively and without invoking a ground for justification, such as necessity or countermeasures. In particular, the US Department of Defense General Counsel has recently stated that "there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits (...) non-consensual cyber operations in another State's territory" and that "[t]he DoD OGC view (...) shares similarities with the view expressed by the UK Government in 2018."³⁰ While it is not clear whether this position represents the view of the United States as a whole or only of one governmental department, it seems safe to assume that actions currently undertaken in cyberspace by the US military are informed by this approach and thereby form the current practice of the United States in this regard.

25 See: Secrétariat Général de la Défense et de la Sécurité Nationale. (2018). *Revue Stratégique de Cyberdéfense*, 12 February 2018, p. 80, (in French) [25.02.2020].

26 Cf. USA: Egan Speech, p. 174; *Tallinn Manual 2.0*, p. 168.

27 USA: Koh Speech, p. 9.

28 C. Todd Lopez. (2019). *Persistent Engagement, Partnerships, Top Cybercom's Priorities*, 14 May 2019 [10.01.2020].

29 C. Todd Lopez. (2019). *DOD More Assertive, Proactive in Cyber Domain*, 28 June 2019 [10.01.2020].

30 Paul C. Ney. (2020). *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, Speech of 2 March 2020 [08.03.2020].

Conclusions and Recommendations on Sovereignty

The preceding analysis shows that the discussion about the existence and application of the rule of territorial sovereignty to cyber operations is still ongoing and no majority position has yet been established, with a plurality of countries supporting the existence of a duty to respect the territorial sovereignty of a State in cyberspace. It is thus recommended that:

- 1) States present their view on whether sovereignty is only a principle of international law, or whether there is a rule of international law requiring States to respect the sovereignty of other States in cyberspace;
- 2) in presenting their views, States be mindful about the jurisprudence of the International Court of Justice, in particular the *Nicaragua* case;
- 3) if States consider that sovereignty is a principle, but not a prescriptive rule of international law, they should explain whether they view cyber attacks below the threshold of use of force and intervention, for instance, cyber attacks against computer systems in banks or private hospitals, as generally in accordance with international law or whether they would adjust the threshold for intervention and/or use of force to include certain types of attacks against private targets;
- 4) if States consider that there is a rule of territorial sovereignty in cyberspace, they should state what the threshold for such a violation is, specifically whether
 - a) State sovereignty is already violated through the penetration of a computer system on the territory of the targeted State, or
 - b) State sovereignty is violated if the penetration of a computer system produces more than *de minimis* effects;
- 5) if States consider that the penetration of a computer system breaches the targeted State's sovereignty only if it produces more than *de minimis* effects, they should explain what the *de minimis* threshold is;
- 6) if States consider that there is a rule of territorial sovereignty in cyberspace, they should elaborate on the territorial scope of this rule in cyberspace, specifically whether it applies only to computer systems located on the territory of the State or whether it encompasses any computer system used in the exercise of governmental functions (for instance so-called digital embassies, cloud systems etc.) as well as other sovereign platforms such as warships and State aircraft.

Non-intervention

Nearly all analysed States share a widespread consensus that the principle of non-intervention applies to State conduct in cyberspace. Only the Estonian President's speech did not mention non-intervention, but it seems safe to assume that given Estonia's participation in the 2013-2015 UN GGE, it shares the UN GGE's view that in their use of ICTs States must observe the principle of non-intervention.³¹ With regard to the applicable standard, States broadly endorse the findings of the ICJ in the *Nicaragua* case, whereby an action constitutes a prohibited intervention if two conditions are met cumulatively:

- 1) the action constitutes a coercive interference
- 2) into the *domaine réservé* of a State, i.e. into matters "which each State is permitted, by the principle of State sovereignty to decide freely"³².

31 UN GGE Report 2015, UN Doc. A/70/174, para 28(b).

32 *Nicaragua*, para. 205.

Both elements of this definition face steep hurdles when it comes to their application to State conduct, even outside the context of cyberspace. This is because on the one hand, it is hard to fix a catalogue of affairs which fall into the *domaine réservé* of a State and on the other hand, the element of coercion provides a high threshold.

Addressing the question which matters are included in the *domaine réservé* in a cyberspace setting, States have affirmed that the matters on which a State is permitted to decide freely include the freedom to choose its own political, social, economic and cultural system,³³ foreign policy,³⁴ national elections, the recognition of States and membership in international organizations.³⁵ With regard to the element of coercion, States acknowledge the difficulties with its precise definition. **Australia** describes coercive means as means which “effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature”,³⁶ while the **Netherlands** define coercion as “compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue”.³⁷ Both States therefore conceptualise coercion through its effects on the free exercise of the sovereign will of the State, which may occur either by compelling the State to undertake actions it would normally not undertake or by depriving it of the possibility or space to exercise its sovereign will. **Some States** give examples of cyber operations, which may constitute a breach of the non-intervention rule. These include:

- operations to manipulate the electoral system, including interference with another country’s ability to hold an election;³⁸
- operations to alter the results of an election in another State;³⁹
- intervention in the fundamental operation of Parliament;⁴⁰
- interference which causes or may cause harm to a State’s political, economic, social and cultural system;⁴¹
- intervention in the stability of a State’s financial system.⁴²

In the author’s opinion, some issues relating to the application of the principle of non-intervention in cyberspace require further elaboration. For instance, it is not clear whether all States apply the same threshold of coercion or whether some States – in particular those which deny the existence of a rule of territorial sovereignty in cyberspace – might apply a broader standard to compensate for the lack of a prohibition of low-intensity cyber operations. Secondly, questions remain about the precise scope of “coercion” in cyberspace, for instance in the context of influence operations.

33 UK: Wright Speech; France: *Operations in Cyberspace*, p. 7.

34 Australia: 2019 Supplement; France: *Operations in Cyberspace*, p. 7.

35 Netherlands: Letter to Parliament, p. 3.

36 Australia: 2019 Supplement.

37 Netherlands: Letter to Parliament, p. 3.

38 UK: Wright Speech; USA: Egan Speech, p. 175.

39 Australia: 2019 Supplement; USA: Egan Speech, p. 175.

40 Australia: 2019 Supplement.

41 France: *Operations in Cyberspace*, p. 7.

42 Australia: 2019 Supplement.

Does a cyber operation entail a coercive element only if it is directed against the organs of a State with the aim of influencing the exercise of the sovereign free will of that State or would States also consider such cyber operations which aim at influencing the democratic process – and thus the composition of State organs – as coercive?

Conclusions and Recommendations on Non-intervention

The preceding analysis shows that there is widespread support for the application of the principle of non-intervention in cyberspace, but its precise contours require further elaboration. It is thus recommended that:

- 1) States should be mindful of, and ideally endorse and apply, the two elements of the principle of non-intervention as laid down by the International Court of Justice in *Nicaragua*;
- 2) States should present their views on the interpretation of both elements of said test – *domaine réservé* and coercion – in the context of cyberspace, especially with regard to cyber influence operations;
- 3) States should present their views on the interplay between the obligation to respect the territorial sovereignty of a State and the principle of non-intervention.

Prohibition of the Use of Force

All States endorse the applicability of the prohibition of the use or threat of force under Article 2(4) UN Charter to cyber operations. Furthermore, with regard to the question which actions may constitute the use of force in cyberspace, **Australia, Germany, France, the Netherlands, the United Kingdom and the United States** specifically or implicitly endorse⁴³ the “scale and effects” test (or a version thereof) employed by the International Court of Justice in the *Nicaragua* case.⁴⁴ Under this test, a cyber operation constitutes a use of force if its scale and effects are comparable to the scale and effects of a “traditional” use of kinetic force.

Based on the analysed State submissions, factors to assess the comparability of scale and effects may include:

- the origin of the operation and the nature of the instigator (military or not);⁴⁵
- the extent of intrusion / seriousness of the attack;⁴⁶
- the actual or intended effects of the operation;⁴⁷

43 *Australia: Cyber Engagement Strategy*, p. 90; *Germany: Riedel Speech*; *France: Operations in Cyberspace*, p. 8 (speaking of “scale and severity”); *Netherlands: Letter to Parliament*, pp. 3-4; *UK: Cyber Primer*, p. 12; *USA: Koh Speech*, p. 4 (listing effects of a cyber operation as one of the factors to be included in an assessment whether an event constituted a use of force in or through cyberspace); see also *Tallinn Manual 2.0*, Rule 69.

44 *Nicaragua*, para. 195; it should be noted that in *Nicaragua* the ICJ employed this test to determine the existence of an armed attack, rather than a use of force.

45 *France: Operations in Cyberspace*, p. 7.

46 *France: Operations in Cyberspace*, p. 7; *Germany: Riedel Speech*.

47 *Australia: Cyber Engagement Strategy*, p. 90; *France: Operations in Cyberspace*, p. 7.

- the immediacy of the effects;⁴⁸
- the depth of penetration of the cyber infrastructure;⁴⁹
- the nature of the intended target, for instance the military character of the attacked infrastructure.⁵⁰

Moreover, according to the analysed declarations examples of cyber attacks which may constitute a use of force (depending on the comparability factors listed above) include operations which lead to or consist of:

- injury or death to persons;⁵¹
- damage or destruction of objects;⁵²
- serious financial or economic impact;⁵³
- penetrating military systems in order to compromise defence capabilities;⁵⁴
- financing or training individuals to carry out cyber attacks against a State;⁵⁵
- interference with the operation of a nuclear reactor, resulting in widespread loss of life;⁵⁶
- disabling of air traffic control systems which results in the downing of a plane;⁵⁷
- opening a dam above a populated area causing destruction;⁵⁸
- targeting of essential medical services.⁵⁹

Conclusions and Recommendations on the Use of Force

The preceding analysis shows that there is unanimous support for the application of prohibition of the use or threat of force to cyber operations. Moreover, there is widespread support for the “scale and effects” test as a test to determine what constitutes “force” in cyberspace. It is thus recommended that:

- 1) States endorse and apply the “scale and effects” test to determine which cyber operations constitute the use of force;
- 2) States present their views on the factors which may indicate the comparability of the scale and effects of a cyber operation to a use of kinetic force;
- 3) States should present and discuss examples which in their view may constitute a use of force by cyber means.

48 *Germany: Riedel Speech.*

49 *Ibid.*

50 *Ibid.*

51 *Australia: Cyber Engagement Strategy, p. 90; Estonia: Kaljulaid Speech.*

52 *Ibid.*

53 *Netherlands: Letter to Parliament, p. 4.*

54 *France: Operations in Cyberspace, p. 7.*

55 *Ibid.*

56 *USA: Koh Speech, p. 4.*

57 *USA: Koh Speech, p. 4; UK: Wright Speech (referring to armed attacks, which always constitute a use of force).*

58 *USA: Koh Speech, p. 4.*

59 *UK: Wright Speech (referring to armed attacks, which always constitute a use of force).*

Due Diligence in Cyberspace

With the exception of the United Kingdom and the United States, **most of the analysed States** have underlined that the exclusive jurisdiction over cyber infrastructure located on the territory of a State creates rights, but also certain obligations. In particular, it is stressed that “[t]o the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states.”⁶⁰ This view reflects long-standing jurisprudence of the International Court of Justice, which held in the *Corfu Channel* case that: “Such obligations [to notify other States of dangers to shipping in the territorial waters of a State] are based (...) on certain general and well-recognized principles, namely: (...) every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.”⁶¹ Interestingly, this rule has been formulated in the *UN GGE Report 2015* not as a binding rule of international law, but rather as a voluntary and non-binding norm: “States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs”.⁶²

A possible reason for States’ preference to include this obligation in the 2015 Report as a non-binding norm rather than a rule of international law is the scope of the obligation such a rule would create in the cyber context. In particular, it is unclear which actions a State would be obliged to undertake to prevent its territory from being used for internationally wrongful acts and how far a State would have to monitor cyber activity within its territory. In particular the United States have underlined that the principle of sovereignty over ICTs located on a State’s territory should not be used as an excuse to violate human rights and other obligations under international law.⁶³

Several States have addressed the extent of a State’s obligations under the due diligence rule:

Australia underlines that upon knowledge of malicious cyber activity emanating from its territory, a State “should take reasonable steps [to put an end to the harmful activity] consistent with international law.”⁶⁴

Estonia sees certain preventive obligations on States, namely to “make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states”.⁶⁵ These steps include the development of means to assist the injured State in the identification, attribution and investigation of malicious activities, but should depend on capacities and the availability of information.⁶⁶

60 *Australia: Cyber Engagement Strategy*, p. 91.

61 *Corfu Channel* (United Kingdom v. Albania), ICJ Rep. 1949, 4, p. 22.

62 UN Doc. A/70/174, para. 13(3).

63 *USA: Egan Speech*, p. 175.

64 *Australia: Cyber Engagement Strategy*, p. 91.

65 *Estonia: Kaljulaid Speech*.

66 *Ibid.*

France underlines the obligation of a State to comply with its due diligence requirement under a “reasonable measures” standard, but forcefully stresses that a failure or inability to stop or prevent “wrongful acts against other States perpetrated from its territory by non-state actors (...) cannot constitute an exception to the prohibition of the use of force.”⁶⁷

The Netherlands also endorse a reasonableness standard, arguing that “a state must take measures which, in the given circumstances, may be expected of a state acting in a reasonable manner.”⁶⁸ The Dutch government adds that an injured State’s right to request cooperation under the due diligence principle depends on the circumstances of the case but does not depend on whether the cyber operation produces physical damage. Upon receipt of a request for assistance the requested State may be obliged to shut down servers used in a malicious cyber operation against the injured State.⁶⁹

Conclusions and Recommendations on Due Diligence

The preceding analysis shows that there is widespread support for the existence of a duty of due diligence in cyberspace. A plurality of States endorses a reasonableness standard for the actions required of a State to discharge its due diligence obligation. It is thus recommended that:

- 1) States endorse the due diligence obligation as a binding rule of international law, rather than a voluntary non-binding norm of responsible State behaviour;
- 2) States present their views on whether the scope of the due diligence obligation differs depending on whether a cyber operation
 - a) originates from the territory of a State;
 - b) uses ICT infrastructure located in a State (e.g. command and control servers), but does not originate from there; or
 - c) is transmitted through the ICT infrastructure located in a State;
- 3) States present their views on the content of the obligation of due diligence, in particular with respect to:
 - a) the applicable standard;
 - b) the existence of any preparatory steps necessary to discharge the due diligence obligation (i.e. development of means to prevent, stop, attribute and investigate any malicious use of ICTs against third States);
 - c) obligations of notification of and assistance to the injured State;
 - d) the steps required to be taken in order to stop a malicious use of ICTs upon notification by the injured State;
 - e) any possible threshold of injury, upon which the obligation to assist and stop would be triggered.

67 *France: Operations in Cyberspace*, p. 10 (thereby rejecting the applicability of the so-called “unwilling or unable” test, which asserts that a State may use force in self-defence against non-state actors operating from the territory of another State without its consent, if that State is unwilling or unable to prevent its territory from being used by non-state actors to conduct attacks; on the “unwilling or unable” test, see e.g. Olivier Corten. (2016). “The Unwilling or Unable Test: Has it Been, and Could it be, Accepted?”, *Leiden Journal of International Law*, 29 (3), pp. 777-799).

68 *Netherlands: Letter to Parliament*, p. 4.

69 *Ibid.*

State Responsibility

Attribution – General Overview

Under general international law, States bear responsibility for conduct which constitutes an internationally wrongful act. An act is wrongful when it cumulatively fulfils two conditions: the act or omission in question must violate an international obligation of a State and this act or omission must be attributable to that State.⁷⁰ The international community has agreed that the customary rules of State responsibility are also applicable to State conduct in cyberspace.⁷¹ It has to be noted, however, that while the general applicability of those rules is not contentious, many specific aspects of international responsibility, including the question of attribution of conduct, as well as countermeasures and necessity, remain problematic and the subject of many debates in academia and amongst States. This section will concentrate on the question of attribution, while countermeasures and necessity will be addressed in the section on “Response Options for States”.

The public debate around the attribution of cyber attacks employs – and often conflates – three different meanings of the term “attribution”, which need to be distinguished. As the **Dutch Minister of Foreign Affairs’** letter to Parliament sets out,⁷² there is, *first*, attribution in the technical sense, which deals with establishing the origin of a particular cyber operation, based on specific technical indicators. This is, for instance, what private cybersecurity companies do, when they “attribute” a cyber operation to a certain actor. *Secondly*, there is attribution in the political sense, which denotes the political decision of one State (or group of States) to hold another State responsible for a particular cyber operation, without necessarily attaching legal consequences to that decision.⁷³ Several cyber operations have been publicly attributed to States, for instance the WannaCry malware attack to North Korea,⁷⁴ cyber attacks against the World Anti-Doping Agency to Russia⁷⁵ or most recently the cyber attacks of October 2019 against Georgia to Russia.⁷⁶ *Lastly*, there is attribution in the legal sense, which means the attribution of a specific act or omission, conducted by an identified actor, to a State based on that actor’s connection to that State, for the purposes of inducing international responsibility.

70 Article 2, International Law Commission, *Articles on State Responsibility for Internationally Wrongful Acts*.

71 *UN GGE Report 2015*, UN Doc. A/70/174, para. 28(f), later adopted by the UN General Assembly on 23 December 2015 by Resolution 70/237, UN Doc. A/Res/70/237.

72 *Netherlands: Letter to Parliament*, p. 6.

73 Cf. *Netherlands: Letter to Parliament*, p. 6.

74 UK Foreign & Commonwealth Office. (2017). “[Foreign Office Minister condemns North Korean actor for WannaCry attacks](#)”, Press release of 19 December 2017 [12.01.2020]; The White House. (2017). “[Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea](#)”, 19 December 2017 [12.01.2020].

75 UK National Cyber Security Centre. (2018). “[Reckless campaign of cyber attacks by Russian military intelligence service exposed](#)”, Press release of 3 October 2018 [12.01.2020].

76 UK Foreign & Commonwealth Office. (2020). “[UK condemns Russia’s GRU over Georgia cyber-attacks](#)”, Press release of 20 February 2020 [25.02.2020]; US Department of State. (2020). “[The United States Condemns Russian Cyber Attack Against the Country of Georgia](#)”, Press statement of 20 February 2020 [25.02.2020].

The standards of attribution in the legal sense are not contentious between the analysed States. **Most States** explicitly or implicitly endorse the bases for attribution as found in the International Law Commission (ILC)'s Articles on State Responsibility.⁷⁷ As such, the most appropriate bases for attribution of cyber operations to a State are:

- conduct by an organ of a State (Art. 4 ARSIWA);
- conduct by persons or entities exercising elements of governmental authority (Art. 5 ARSIWA);
- conduct by a person or group of persons acting on the instructions of, or under the direction or control of a State (Art. 8 ARSIWA);
- conduct acknowledged or adopted by a State as its own⁷⁸ (Art. 11 ARSIWA).⁷⁹

While the legal standard of attribution in international law is clear, the main challenges for attributing cyber operations are connected with the technical aspects of cyberspace – its anonymity, interconnectedness, transboundary character and the use of proxies – which make obtaining reliable evidence to identify the perpetrators of a cyber operation difficult. This raises three questions: *first*, what is the standard of evidence that States should use for the purposes of attribution, *second*, which factors or indicators should States take into account when making that determination and *third*, is there a duty to provide evidence when publicly attributing a cyber operation to a State?

Attribution – Standard of Proof

The burden and standard of proof for attribution of cyber operations have been addressed by several of the analysed States. **The United States** stress that “[t]he law of state responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution”.⁸⁰ **The Netherlands** adds that “[i]n the government’s view, the burden of proof will indeed vary in accordance with the situation, depending on the seriousness of the act considered to be in breach of international law and the intended countermeasures”.⁸¹ This position reflects the International Court of Justice’s varying standards of proof, which depend on the gravity of the breach and varies between a “fully conclusive” evidence standard for “charges of exceptional gravity”, leaving “no room for reasonable doubt”⁸² to “proof at a high level of certainty appropriate to the seriousness of the allegation”⁸³ for charges of lesser gravity.⁸⁴ Additionally, **some States** argue that for the purposes of attribution, absolute certainty is not required; rather they are required by international law only to “act reasonably under the circumstances when they gather

77 *France: Operations in Cyberspace*, p. 10; *Australia: 2019 Supplement*; *Netherlands: Letter to Parliament*, p. 6.

78 Potentially applicable, for instance, in the case of official statements acknowledging operations by so-called “patriotic hackers”.

79 See, in general, International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts*, UN Doc A/56/83 [ARSIWA].

80 *USA: Egan Speech*, p. 177.

81 *Netherlands: Letter to Parliament*, p. 7.

82 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Serbia and Montenegro)*, Judgment of 26 Feb. 2007, ICJ Rep. 2007, 129, para. 208-209.

83 *Ibid.* para. 210.

84 For a thorough scholarly assessment of the question of evidence before the ICJ see Juan Jose Quintana. (2015). *Litigation at the International Court of Justice*, Brill Nijhoff: pp. 382–480.

information and draw conclusions based on that information”,⁸⁵ with the victim State being “confident in its attribution of [a cyber operation] to a hostile state before it takes action in response”.⁸⁶ This view finds support in the *Tallinn Manual 2.0*, where the International Group of Experts agreed that States must act reasonably with regard to the *ex ante* uncertainty as to the attribution of cyber operations and consider the relevant available information “in light of the attendant circumstances and the importance of the right involved”.⁸⁷

In the opinion of the author, this standard of “reasonableness” is problematic and requires further clarification. In particular, it needs to be clarified whether “reasonableness” refers to a *duty of care* that supposedly rests upon a State making an attribution or whether it refers to the *standard of evidence* a State has to rely upon when determining a certain fact, for instance the identity of the attacker. For instance, the **United States’** position that a State is obliged to “act reasonably under the circumstances when they gather information and draw conclusions based on that information”⁸⁸ seems to point to a *duty of care* when making the attribution. However, in international law such duties of reasonable care exist in relation to *primary rules* of international law, especially obligations of prevention such as the duty to prevent transboundary harm,⁸⁹ and not to *secondary rules* of international law relating to State responsibility. In the context of *primary rules*, “reasonableness” sets the standard by which it is to be assessed whether a State fulfilled a certain international obligation, e.g. the obligation to prevent transboundary harm, and therefore does not bear international responsibility for any harmful incident which may have occurred despite the action taken by the State. This standard cannot be easily transposed to *secondary rules* of attribution.

To better illustrate the point, imagine the following situation: State A suffers a cyber attack. Based on available evidence, it is reasonably confident that the cyber attack can be attributed to State B and decides to answer in kind to induce State B to stop. The wrongfulness of State A’s conduct is precluded only if the conduct in question constitutes a countermeasure against a previous wrongful act by State B.⁹⁰ Now imagine that it later turns out that State A’s initial assessment was wrong: State C was the culprit, not State B. In other words, there was no previous wrongful act by State B. Would the fact that State A had acted “reasonably under the circumstances” nevertheless somehow preclude the wrongfulness of its retaliatory cyber attack against State B? If “reasonableness” were a *duty of care*, State A might argue that – acting “reasonably under the circumstances” – it has discharged its *duty of care* and would therefore not bear international responsibility for violating State B’s rights. State B would therefore bear the consequences of State A’s erroneous attribution, without the right to claim restitution or compensation.

85 USA: *Egan Speech*, p. 177; see also *Estonia: Kaljulaid Speech*: “At the end of the day what is required from the attributing state, is not absolute certainty but what is reasonable”.

86 UK: *Wright Speech*.

87 *Tallinn Manual 2.0*, pp. 81–82.

88 USA: *Egan Speech*, p. 177; see also *Estonia: Kaljulaid Speech*: “At the end of the day what is required from the attributing state, is not absolute certainty but what is reasonable”; however, the US also clarify that “As with all countermeasures, this puts the responding State in the position of potentially being held responsible for violating international law if it turns out that there wasn’t actually an internationally wrongful act that triggered the right to take countermeasures, or if the responding State made an inaccurate attribution determination”.

89 ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries*, Yearbook of the International Law Commission, 2001, vol. II, Part Two, p. 148ff., Article 3 para 11.

90 Article 22, ARSIWA.

In the present author's opinion such a consequence would be incompatible with the law of State responsibility, as State responsibility is objective and does not depend on fault or wrongful intent.⁹¹ In other words, it does not matter whether from an *ex ante* perspective State A might have reasonably thought that State B was responsible for the cyber attack – it bears the consequences of a wrongful decision, even if the error was not known or foreseeable at the moment of decision making. In this regard State responsibility substantially differs from international criminal law, which recognizes mistakes of fact and law as grounds for excluding (criminal) responsibility⁹² due to the absence of the mental element of a crime.⁹³ Moreover, “lack of intent” or “reasonable care” do not figure as grounds for precluding the wrongfulness of a breach of international law. Thus, a State remains internationally responsible for a wrongful act even if it took *reasonable care* to prevent misattributions. “Reasonableness” should therefore be understood to refer to a *standard of evidence*, i.e. the standard of assessing evidence for the purposes of attribution, as well as the type of evidence a State should rely on when making an attribution, taking into account the particular technical circumstances of cyberspace.

Attribution – Indicators

The question then remains what types of evidence can be relied upon by a State to attribute a cyber operation to another State. Here, the concept of reasonableness could indeed be useful to determine the applicable standard of evidence, taking into account “the seriousness of the act considered to be in breach of international law and the intended countermeasures”.⁹⁴ The **Dutch** government holds that evidence can include “both information obtained through regular channels and intelligence”.⁹⁵ Similarly, **Australia** “relies on the assessments of its law enforcement and intelligence agencies, and consultations with its international partners”.⁹⁶ According to **Estonia**, factors to assess the origin of malicious cyber operations may include “technical information, political context, established behavioural patterns and other relevant indicators”.⁹⁷ Similarly, **France** postulates the use of technical indicators such as “identification of the attack and transit infrastructure for the cyberoperation and its location, identification of the adversary methods of operation (AMO), the overall chronology of the perpetrator's activities, the scale and gravity of the incident and the compromised perimeter, or the effects sought by the attacker”.⁹⁸

91 ARSIWA, Article 49, commentary para. 3; James Crawford. (2006). “State Responsibility”, *Max Planck Encyclopaedia of Public International Law*, Oxford University Press: para 12.

92 Cf. Art. 32(1) Rome Statute.

93 Cf. Albin Eser. (2002). “Mental Elements—Mistake of Fact and Mistake of Law”, in: Antonio Cassese, Paola Gaeta and John RWD Jones (eds), *The Rome Statute of the International Criminal Court*, Oxford University Press: p. 394.

94 *Netherlands: Letter to Parliament*, p. 7.

95 *Netherlands: Letter to Parliament*, p. 6.

96 *Australia: 2019 Supplement*.

97 *Estonia: Kaljulaid Speech*.

98 *France: Operations in Cyberspace*, p. 10.

Attribution – Duty to Provide Evidence

France,⁹⁹ the Netherlands,¹⁰⁰ the United Kingdom,¹⁰¹ and the United States¹⁰² hold that international law does not require States to provide the evidence on which an attribution has been made. States agree, however, that there may be policy reasons to disclose (some of) the underlying information, such as to help to legitimise the validity of such attribution.

Moreover, the United Kingdom and in particular France stress that there is no duty under international law to – individually or collectively – publicly attribute a cyber operation. The decision to publicly attribute remains a sovereign and political decision of a State; the absence of a public attribution does not bar a State which has been the target of a cyber operation from applying consequences in accordance with international law.¹⁰³

Recommendations on Attribution

- 1) States should endorse the ILC Articles on State Responsibility with respect to attribution of cyber conduct;
- 2) States should present their views on the standard of evidence they regard as necessary and/or sufficient to establish the origin of a cyber operation and attribute it to a State;
- 3) States should present their views on the indicators which may be used to attribute a cyber operation to a State. Such indicators might include:
 - technical indicators (infrastructure used, methods of operation, scale and gravity of the incident, intended effects)
 - political indicators (political context, for instance whether a dispute with another State exists, whether tensions have flared up etc.)
 - behavioural patterns (chronology of activities, methods of operation).

99 France: *Operations in Cyberspace*, p. 11.

100 Netherlands: *Letter to Parliament*, p. 6.

101 UK: *Wright Speech*.

102 USA: *Egan Speech*, p. 177.

103 France: *Operations in Cyberspace*, p. 11.

Response Options for States

To conform with the law of State responsibility, measures taken by States in response to cyber operations must either not amount to internationally wrongful acts or, if they violate a rule of international law such as the principle of non-intervention, must be justifiable with reference to one of the circumstances precluding wrongfulness. The analysed States recognize as legitimate response options retorsions, countermeasures, acts taken on the grounds of necessity and actions taken in self-defence.

Retorsion

Retorsions are reactions which may be considered unfriendly, but which do not interfere with the target State's rights under international law.¹⁰⁴ While only **Australia**,¹⁰⁵ the **Netherlands**¹⁰⁶ and the **United States**¹⁰⁷ specifically refer to retorsions as response options to cyber attacks, it is safe to assume that the recourse to actions which do not violate international obligations is largely unproblematic. Acts of retorsion may include declaring diplomats *persona non grata* or the imposition of sanctions.

Countermeasures

A majority of States (all except Germany, which did not address this issue) agrees that a State which fell victim to an internationally unlawful cyber attack may respond by resort to countermeasures, i.e. measures which otherwise would be unlawful, but whose unlawfulness is precluded, if they are undertaken with the aim of inducing the responsible State to cease the attack.¹⁰⁸ **All States** furthermore endorse the main conditions for the imposition of countermeasures:

- countermeasures must be directed only at the responsible State;
- countermeasures must be taken with the aim to induce the responsible State to stop a violation of international law;
- countermeasures must be temporary, necessary and proportionate;
- countermeasures must not amount to a threat or use of force and may not violate fundamental human rights.

Additionally, **France**,¹⁰⁹ the **United Kingdom**¹¹⁰ and the **United States**¹¹¹ consider that countermeasures taken in response to a cyber operation are not limited to measures in kind; rather, a State may also resort to non-cyber-based countermeasures.

104 Thomas Giegerich. (2011). "Retorsion", *Max Planck Encyclopaedia of Public International Law*, Oxford University Press: para 1.

105 *Australia: 2019 Supplement*.

106 *Netherlands: Letter to Parliament*, p. 7.

107 *USA: Egan Speech*, p. 177.

108 See, e.g., *USA: Egan Speech*, p. 178.

109 *France: Operations in Cyberspace*, p. 8.

110 *UK: Wright Speech*.

111 *USA: Egan Speech*, p. 178.

A further element of the customary law of countermeasures, laid down in Article 52(1) ARSIWA, is the requirement to call upon the responsible State to fulfil its obligations and to notify it of any decision to take countermeasures. Article 52(2) ARSIWA allows for an exception to the notification requirement in case of urgent countermeasures which are necessary to preserve a State's rights. In this vein, the **majority** of the analysed States¹¹² holds the view that in the cyber context States are under certain circumstances permitted to depart from this obligation to give prior notification. This may be due to the covert nature of cyber intrusions and the necessity of covertness and secrecy of (cyber) countermeasures¹¹³ or the urgency of the action.¹¹⁴ Given that such a derogation from the obligation of prior notification would constitute an exception from a customary rule of international law, it should be further clarified what the precise conditions for this derogation are and whether States may derogate only with respect to cyber-based countermeasures or also non-cyber-based countermeasures.

Lastly, **Estonia** postulates that not only States which are victims of a cyber attack, but also States “which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation”.¹¹⁵ This view has been contradicted by **France**, which argues that “[u]nder international law, [...] counter-measures must be taken by France in its capacity as victim. Collective counter-measures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's rights.”¹¹⁶ The ILC Articles on State Responsibility do not give clear guidance on this matter. Article 54 ARSIWA holds that “This chapter [on countermeasures] does not prejudice the right of any [non-injured] State [...] to invoke the responsibility of another State, to take lawful measures against that State”. It may be argued that there is sufficient State practice and *opinio iuris* to establish a customary rule permitting collective countermeasures by non-injured States, but – crucially – only in defence of collective obligations of community interest.¹¹⁷ In the opinion of the present author, the majority of reported cyber attacks may affect individual rights of States, e.g., the right to respect for territorial sovereignty or the obligation not to interfere in the internal affairs of a State, but they do not breach any existing collective obligations.¹¹⁸ Therefore, the Estonian position is to be understood as a proposal for the progressive development of international law, rather than a statement on its current content.

112 *France: Operations in Cyberspace*, p. 8; *Netherlands: Letter to Parliament*, p. 7; *UK: Wright Speech*; *USA: Egan Speech*, p. 178.

113 *UK: Wright Speech*; *France: Operations in Cyberspace*, p. 8.

114 *Netherlands: Letter to Parliament*, p. 7.

115 *Estonia: Kaljulaid Speech*.

116 *France: Operations in Cyberspace*, p. 7.

117 Cf. Martin Dawidowicz. (2017). *Third-Party Countermeasures in International Law*, Cambridge University Press; Elena Katselli Proukaki. (2010). *The Problem of Enforcement in International Law*, Routledge.

118 There may be, however, an emerging obligation to protect the “Public Core of the Internet”; for more on this topic and on collective countermeasures generally see: Przemysław Roguski. (forthcoming). “*Collective Countermeasures in Cyberspace: Lex Lata, Progressive Development or a Bad Idea?*”; in: *12th International Conference on Cyber Conflict: 20/20 Vision – The Next Decade*. Proceedings of CyCon 2020.

Recommendations on Countermeasures

- 1) States should endorse the customary rules on countermeasures as laid down in the ILC Articles on State Responsibility;
- 2) States should present their views on whether countermeasures in response to cyber operations should only be cyber-based or whether they may include non-cyber-based measures;
- 3) States should present their views on whether they consider the obligation to give prior notification to be derogable in the cyber context and if yes, under which circumstances;
- 4) States should present their views on the permissibility of collective countermeasures and in particular:
 - a) Whether collective countermeasures are permitted under current international law;
 - b) If not, whether international law should be progressively developed to allow collective countermeasures and under which conditions.

State of Necessity

Under the international law of State responsibility, States may invoke the state of necessity to protect their essential interests against a grave and imminent peril. This is a rule of customary international law, recognized by the International Court of Justice¹¹⁹ and codified by the International Law Commission in Article 25 ARSIWA. This “plea of necessity” as a measure precluding the wrongfulness of a response action to an offensive cyber operation has not received the same attention of States as countermeasures. Only **three States** have so far addressed the applicability of the plea of necessity (as opposed to necessity in the context of self-defence or international humanitarian law) to cyber operations: **France**,¹²⁰ the **Netherlands**¹²¹ and the **United States**,¹²² with only the Netherlands doing it in greater detail.

The **Dutch** position is particularly noteworthy, as it contains examples when the constitutive elements of a plea of necessity may be fulfilled in the cyber context. According to the Dutch government, an “essential interest” – while open to interpretation in practice – may “certainly” include the operation of services such as the electricity grid, water supply and the banking system.¹²³ The government interprets the criterion of a “grave and imminent peril”¹²⁴ to mean that there must be a threat of “very serious consequences” for the essential interest at stake and these consequences must be imminent and objectively verifiable.¹²⁵ According to the Dutch view the serious consequences do not have to be physical; situations where “virtually the entire internet is rendered inaccessible” or there are severe shocks to the financial markets may be sufficiently serious. Importantly, the Dutch government stresses that necessity may be invoked even when the “precise origin of the damage” or the attribution of international responsibility to a particular State are not clear.¹²⁶

119 *Gabčíkovo-Nagymaros Project* (Hungary v Slovakia), [1997] ICJ Rep 7, para. 49 et seq.

120 *France: Operations in Cyberspace*, p. 8.

121 *Netherlands: Letter to Parliament*, pp. 7-8.

122 *USA: Egan Speech*, p. 178.

123 *Netherlands: Letter to Parliament*, p. 8.

124 Article 25(1)(a) ARSIWA.

125 It has to be noted, however, that the ICJ clarified in *Gabčíkovo* para 54, that a threat is imminent, even if it is far off in time, provided that the realization of the peril is no less certain and inevitable.

126 *Netherlands: Letter to Parliament*, p. 8.

Recommendations on the State of Necessity

- 1) States should endorse the customary rules on the state of necessity as laid down in Article 25 ILC Articles on State Responsibility;
- 2) States should present their views on how they understand the concept of “essential interests” in the cyber context;
- 3) States should present their views on what constitutes a “grave and imminent peril” to those essential interests.

Self-defence

All analysed States acknowledge the right of a State to individual or collective self-defence against cyber operations amounting to an armed attack under Article 51 UN Charter. As with the use of force, most States accept that a cyber operation may constitute an armed attack if its scale and effects are comparable to kinetic or physical armed attacks, thereby endorsing the International Court of Justice’s “scale and effects” test in *Nicaragua*.¹²⁷ France uses a slightly different “scale and severity” test to determine the existence of an armed attack.¹²⁸ Furthermore, although only France¹²⁹ the Netherlands¹³⁰ and the United States¹³¹ specifically say that the use of force in self-defence has to meet the conditions of necessity and proportionality, it is safe to assume that all States share this view, given that it reflects customary international law.¹³² It needs to be added that the United States takes the view that the right to self-defence exists against *any* unlawful use of force, thereby rejecting the existence of a threshold of armed attack distinct from the threshold of the use of force.¹³³ France and the Netherlands, on the other hand, take the opposite view, relying on the International Court of Justice’s *Nicaragua* decision.¹³⁴

127 *Nicaragua*, para. 195.

128 *France: Operations in Cyberspace*, p. 8.

129 *Ibid.* p. 9.

130 *Netherlands: Letter to Parliament*, p. 9.

131 *USA: Koh Speech*, p. 7.

132 *Nicaragua*, para. 176.

133 *Ibid.*

134 *France: Operations in Cyberspace*, p. 8; *Netherlands: Letter to Parliament*, p. 8 (both citing *Nicaragua*, paras 191 and 195, respectively).

With respect to the necessary scale and effects of a cyber operation, the **Dutch** government stresses that “[a]t present there is no international consensus on qualifying a cyber attack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non-material consequences.”¹³⁵ According to **France**, an armed attack may be presumed “if it caused substantial loss of life or considerable physical or economic damage”.¹³⁶ Examples include attacks against critical infrastructure with significant consequences which may paralyse “whole swathes of the country’s activity, trigger technological or ecological disasters and claim numerous victims”.¹³⁷ In **Germany’s** view, factors to be taken into account include “the seriousness of the attack, the immediacy of its effects, depth of penetration of the cyber infrastructure and its military character”.¹³⁸ Additionally, **France** endorses the “accumulation of events” theory,¹³⁹ whereby cyber attacks which in isolation do not reach the threshold of an armed attack may still be considered as such “if the accumulation of their effects reaches a sufficient threshold of gravity, or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or from different entities acting in concert.”¹⁴⁰

Germany and **France** address the question of the right to self-defence against non-State actors perpetrating armed attacks by cyber means and reach opposite conclusions. While Germany accepts that self-defence measures may also target non-State actors to which the cyber operation has been attributed,¹⁴¹ France does not recognise the extension of the right to self-defence to acts perpetrated by non-State actors without attribution to a State.¹⁴² An exception can be made for non-State actors which function as “quasi-States”, such as ISIS. France acknowledges, however, that general practice may shift towards accepting the right to self-defence against non-State actors.

Lastly, **Australia** and **France** address the question of pre-emptive self-defence in the context of cyberspace. According to Australia, “[a] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts.”¹⁴³ France “allows itself to use pre-emptive self-defence in response to a cyber attack that ‘has not yet been triggered but is about to be, in an imminent and certain manner, provided that the potential impact of such an attack is sufficiently serious’”.¹⁴⁴

135 *Ibid.* p. 9.

136 *France: Operations in Cyberspace*, p. 8.

137 *Ibid.*

138 *Germany: Riedel Speech*.

139 For a scholarly description of the accumulation of events theory see e.g. Christine Grey. (2018). *International Law and the Use of Force*, Oxford University Press: p. 164ff.; David Kretzmer. (2013). “The Inherent Right to Self-Defense and Proportionality in *Jus ad Bellum*”, *European Journal of International Law*, 24 (1): pp. 235-282; J. Francisco Lobo. (2018). “One Piece at a Time: The “Accumulation of Events” Doctrine and the “Bloody Nose” Debate on North Korea”, *Lawfare*, 16 March 2018 [25.02.2020].

140 *France: Operations in Cyberspace*, p. 9.

141 Deutscher Bundestag. (2015). “Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE”, BT-Drs. 18/6989, p. 11 (hereinafter *Germany: BT-Drs*).

142 *France: Operations in Cyberspace*, pp. 8-9.

143 *Australia: 2019 Supplement*.

144 *France: Operations in Cyberspace*, p. 9 (citing SGDSN, *Strategic Review of Cyberdefence*, 2018, p. 84).

In the opinion of the author, this view presents significant practical challenges with regard to determining the imminence and certainty of an armed attack by cyber means. How is this to be determined? Given the potentially grave consequences of pre-emptive self-defence against cyber attacks and the challenges regarding to attribution and malware analysis, States should address this point in greater detail. In line with that, States should also address the standard of proof necessary for an act of self-defence against cyber attacks. As the **Netherlands** notes, “States may (...) use force in self-defence only if the origin of the attack and the identity of those responsible are sufficiently certain”, with the proof being adequate and convincing.¹⁴⁵

Conclusions and Recommendations on Self-defence

All States accept the right to individual or collective self-defence against cyber operations amounting to an armed attack. The existence of an armed attack shall be determined by comparing the “scale and effects” of the cyber operation to armed attacks using physical force. Any use of force in self-defence must conform to the requirements set out in Article 51 UN Charter.

It is further recommended that:

- 1) States should present their views on the factors which may indicate the comparability of the scale and effects of a cyber operation to a kinetic armed attack;
- 2) States should present their views on whether they endorse the “accumulation of events” theory as one of the ways to determine the existence of an armed attack by cyber means;
- 3) States should address the question whether self-defence against non-State actors which have committed armed attacks by cyber means is permissible under international law;
- 4) States should address the question whether pre-emptive or anticipatory self-defence against cyber operations constituting an armed attack is permissible under international law and if yes, how is the imminence of an armed attack by cyber means to be determined.

¹⁴⁵ *Netherlands: Letter to Parliament*, p. 9.

Conclusion

The preceding analysis shows that there exists widespread agreement among the seven analysed States on the major issues pertaining to the application of international law to cyber operations – such as the existence and content of the obligation not to use force in cyberspace or the general applicability of the rules on State responsibility to conduct in cyberspace. There remain, however, differences of opinion (or lack of formulated positions) on the application and interpretation of specific rules, for instance with respect to the existence of an obligation to respect the sovereignty of another State in cyberspace or the existence and extent of an obligation of due diligence in cyberspace. To increase the stability of international relations, it is necessary that not only the general applicability of international law in cyberspace is affirmed, but that there exists a widespread understanding and agreement as to the applicability and interpretation of specific rules of conduct in the context of cyberspace. States can (and should) contribute to achieving this result by presenting their views on the application and interpretation of international law in cyberspace. It is the hope of the author and the Hague Program for Cyber Norms that the present policy brief may contribute to the work of diplomats, analysts and scholars in this regard.

Annex: Excerpts from Statements of States on How International Law Applies to Cyber Operations

This Annex is part of the 2020 Policy brief *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views* by Przemysław Roguski. The Annex contains relevant excerpts from speeches, statements and other official documents from the governments of Australia, Estonia, France, Germany, the Netherlands, the United Kingdom and the United States, presenting the analysed States' views on how international law applies in cyberspace, which formed the source material for the comparative analysis. The excerpts are grouped thematically, reflecting the structure of the 2020 Policy brief.

Source materials used and referenced in this Annex:

Australia

Commonwealth of Australia, Department of Foreign Affairs and Trade. (2017). [Australia's Cyber Engagement Strategy, Annex A: Australia's position on how international law applies to state conduct in cyberspace](#). [*Australia: Cyber Engagement Strategy*].

Commonwealth of Australia, Department of Foreign Affairs and Trade. (2019). [Australia's Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace](#). [*Australia: 2019 Supplement*].

Estonia

Kersti Kaljulaid. (2019). "[President of the Republic at the opening of CyCon 2019](#)". Speech of Estonian President Kersti Kaljulaid in Tallinn on 29 May 2019. [*Estonia: Kaljulaid Speech*].

France

French Ministry of the Armies. (2019). [International Law Applied to Operations in Cyberspace](#). [*France: Operations in Cyberspace*].

Germany

Norbert Riedel. (2015). "[Cyber Security as a Dimension of Security Policy](#)". Speech of Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London on 18 May 2015. [*Germany: Riedel Speech*].

Deutscher Bundestag. (2015). [Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drs. 18/6989](#). [*Germany: BT-Drs.*].

The Netherlands

Ministry of Foreign Affairs. (2019). [Letter to the parliament on the international legal order in cyberspace](#). 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. [*Netherlands: Letter to Parliament*].

United Kingdom

Jeremy Wright. (2018). "[Cyber and International Law in the 21st Century](#)". Speech by Attorney General Jeremy Wright QC MP on 23 May 2018. [UK: *Wright Speech*].

UK Ministry of Defence. (2016). [Cyber Primer](#), 2nd ed. [UK: *Cyber Primer*].

United States

Harald Hongju Koh. (2012). "[International Law in Cyberspace](#)". Remarks by Harald Hongju Koh, Legal Adviser to the US Department of State, on 18 September 2012, reprinted in [Harvard Int'l LJ Online](#), 54, December 2012, pp. 1-12. [US: *Koh Speech*].

Brian J. Egan. (2016). "[Remarks on International Law and Stability in Cyberspace](#)". Remarks by Brian J. Egan, Legal Adviser to the U.S. Department of State, on 10 November 2016, reprinted in *Berkeley Journal of Int'l Law*, 35 (1), pp. 169-180. [US: *Egan Speech*].

Sovereignty

France

“Any unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty.”¹⁴⁶

“Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.”¹⁴⁷

Germany

“Even in cases where one cannot speak of a use of force, the use of cyber capabilities might constitute a violation of sovereignty, if the attack can be attributed to a state, which then in turn could lead to consequences within the confines of public international law.”¹⁴⁸

Netherlands

“The principle of sovereignty, i.e. that states are equal and independent and hold the highest authority within their own borders, is one of the fundamental principles of international law. More specific rules of international law, such as the prohibition of the use of force, the principle of non-intervention and the right of self-defence stem from this principle.”¹⁴⁹

“According to some countries and legal scholars, the sovereignty principle does not constitute an independently binding rule of international law that is separate from the other rules derived from it. The Netherlands does not share this view. It believes that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act. This view is supported, for example, by the case law of the International Court of Justice, which ruled in *Nicaragua v. United States of America* that the United States had acted in breach of its obligation under customary international law not to violate the sovereignty of another state.”

“States have an obligation to respect the sovereignty of other states and to refrain from activities that constitute a violation of other countries’ sovereignty. Equally, countries may not conduct cyber operations that violate the sovereignty of another country. It should be noted in this regard that the precise boundaries of what is and is not permissible have yet to fully crystallise. This is due to the firmly territorial and physical connotations of the traditional concept of sovereignty. The principle has traditionally been aimed at protecting a state’s authority *over property and persons within its own national borders*. In cyberspace, the concepts of territoriality and physical tangibility are often less clear.”

146 *France: Operations in Cyberspace*, p. 6.

147 *Ibid.* p. 7.

148 *Germany: Riedel Speech*.

149 *Netherlands: Letter to Parliament*, p. 1.

“The act of exercising investigative powers in a cross-border context is traditionally deemed a violation of a country’s sovereignty unless the country in question has explicitly granted permission (by means of a treaty or other instrument). Opinion is divided as to what qualifies as exercising investigative powers in a cross-border context and when it is permissible without a legal basis founded in a treaty.”¹⁵⁰

United Kingdom

“Some have sought to argue for the existence of a cyber specific rule of a ‘violation of territorial sovereignty’ in relation to interference in the computer networks of another state without its consent.

Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government’s position is therefore that there is no such rule as a matter of current international law.”¹⁵¹

United States

“States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered.”¹⁵²

“As an initial matter, remote cyber operations involving computers or other networked devices located on another State’s territory do not constitute a per se violation of international law. In other words, there is no absolute prohibition on such operations as a matter of international law. This is perhaps most clear where such activities in another State’s territory have no effects or *de minimis* effects.

(...)

Although certain activities – including cyber operations – may violate another State’s domestic law, that is a separate question from whether such activities violate international law. The United States is deeply respectful of other States’ sovereign authority to prescribe laws governing activities in their territory. Disrespecting another State’s domestic laws can have serious legal and foreign policy consequences. As a legal matter, such an action could result in the criminal prosecution and punishment of a State’s agents in the United States or abroad, for example, for offenses such as espionage or for violations of foreign analogs to provisions such as the U.S. Computer Fraud and Abuse Act. From a foreign policy perspective, one can look to the consequences that flow from disclosures related to such programs. But such domestic law and foreign policy issues do not resolve the independent question of whether the activity violates international law.

In certain circumstances, one State’s non-consensual cyber operation in another State’s territory could violate international law, even if it falls below the threshold of a use of force. This is a challenging area of the law that raises difficult questions. The very design of the Internet may

150 Netherlands: Letter to Parliament, p. 2.

151 UK: Wright Speech.

152 USA: Koh Speech, p. 6.

lead to some encroachment on other sovereign jurisdictions. Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States.”¹⁵³

Non-intervention

Australia

“Harmful conduct in cyberspace that does not constitute a use of force may still constitute a breach of the duty not to intervene in the internal or external affairs of another state. This obligation is encapsulated in Article 2(7) of the Charter and in customary international law. A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely. Such matters include a state’s economic, political, and social systems, and foreign policy. Accordingly, as former UK Attorney-General Jeremy Wright outlined in 2018, the use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of Parliament, or in the stability of States’ financial systems would constitute a violation of the principle of non-intervention.”¹⁵⁴

France

“Many States are acquiring the capacity to prepare and conduct operations in cyberspace. When carried out to the detriment of the rights of other States, such operations may breach international law. Depending on the extent of their intrusion or their effects, they may violate the principles of sovereignty, non-intervention or even the prohibition of the threat or use of force.”¹⁵⁵

“Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France’s political, economic, social and cultural system, may constitute a violation of the principle of non-intervention.

A cyberattack which penetrates State digital systems, affects the military or economic power, security or survival capacity of the Nation, or constitutes interference in France’s internal or external affairs, will entail defensive cyber warfare operations that may include neutralisation of the effect.”¹⁵⁶

Germany

“In cyberspace, too, the activities of government agencies must be measured against the applicable law. In terms of peacetime international law, these are the prohibition of intervention, the prohibition of use of force as well as the exceptions existing under international law.”¹⁵⁷

153 USA: Egan Speech, p. 174.

154 Australia: 2019 Supplement.

155 France: Operations in Cyberspace, p. 6.

156 Ibid. p. 7.

157 Germany: BT-Drs, p. 9 (own translation).

Netherlands

“The development of advanced digital technologies has given states more opportunities to exert influence outside their own borders and to interfere in the affairs of other states. Attempts to influence election outcomes via social media are an example of this phenomenon. International law sets boundaries on this kind of activity by means of the non-intervention principle, which is derived from the principle of sovereignty.

The non-intervention principle, like the sovereignty principle from which it stems, applies only between states. Intervention is defined as interference in the internal or external affairs of another state with a view to employing coercion against that state. Such affairs concern matters over which, in accordance with the principle of sovereignty, states themselves have exclusive authority. National elections are an example of internal affairs. The recognition of states and membership of international organisations are examples of external affairs.

The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law. In essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state. Although there is no clear definition of the element of coercion, it should be noted that the use of force will always meet the definition of coercion. Use of force against another state is always a form of intervention.”¹⁵⁸

United Kingdom

“In certain circumstances, cyber operations which do not meet the threshold of the use of force but are undertaken by one state against the territory of another state without that state’s consent will be considered a breach of international law.

The international law prohibition on intervention in the internal affairs of other states is of particular importance in modern times when technology has an increasing role to play in every facet of our lives, including political campaigns and the conduct of elections. As set out by the International Court of Justice in its judgment in the Nicaragua case, the purpose of this principle is to ensure that all states remain free from external, coercive intervention in the matters of government which are at the heart of a state’s sovereignty, such as the freedom to choose its own political, social, economic and cultural system.

The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space. But the practical application of the principle in this context would be the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system. Such acts must surely be a breach of the prohibition on intervention in the domestic affairs of states.”¹⁵⁹

“The customary international law principle of non-intervention prohibits states from intervening or interfering in the affairs of another state. The principle prohibits conduct that is coercive in character against affairs that a state should be permitted to decide freely, including the choice of political, economic, social and cultural systems and the formulation of foreign policy. A cyber operation which does not constitute a use of force or armed attack may nevertheless contravene the principle of non-intervention.”¹⁶⁰

158 *Netherlands: Letter to Parliament*, p. 3.

159 *UK: Wright Speech*.

160 *UK: Cyber Primer*, p. 12.

United States

“In certain circumstances, one State’s non-consensual cyber operation in another State’s territory could violate international law, even if it falls below the threshold of a use of force. This is a challenging area of the law that raises difficult questions. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States.

Relatedly, consider the challenges we face in clarifying the international law prohibition on unlawful intervention. As articulated by the International Court of Justice (ICJ) in its judgment on the merits in the Nicaragua Case, this rule of customary international law forbids States from engaging in coercive action that bears on a matter that each State is entitled, by the principle of State sovereignty, to decide freely, such as the choice of a political, economic, social, and cultural system. This is generally viewed as a relatively narrow rule of customary international law, but States’ cyber activities could run afoul of this prohibition. For example, a cyber operation by a State that interferes with another country’s ability to hold an election or that manipulates another country’s election results would be a clear violation of the rule of non-intervention. For increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States’ activities in cyberspace.”¹⁶¹

Use of Force and Armed Attack

Australia

“In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity’s scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive (‘scale’) damage or destruction (‘effects’) to life, or injury or death to persons, or result in damage to the victim state’s objects, critical infrastructure and/or functioning.”¹⁶²

“Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber operations that constitute an armed attack and in respect of acts of self-defence that are carried out by cyber means. Thus if a cyber operation – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged.”¹⁶³

“The rapidity of cyber attacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been raised by Australia in explaining its position on the concept of imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances. (...)”¹⁶⁴

161 USA: Egan Speech, pp. 174-175.

162 Australia: Cyber Engagement Strategy, p. 90.

163 Australia: 2019 Supplement.

164 Australia: Cyber Engagement Strategy, p. 90.

Estonia

“First and foremost, states must refrain from the threat of or use of force against the territorial integrity and political independence of other states. However, we already know that cyber operations, which cause injury or death to persons or damage or destruction of objects, could amount to use of force or armed attack under the UN Charter.”¹⁶⁵

France

“Any unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty. If it is accompanied by effects that constitute a use of force within the meaning of Article 2, para. 4 of the United Nations Charter, France may take counter-measures or bring the matter before the United Nations Security Council (UNSC). It is not ruled out that a cyberattack may reach the threshold of an armed attack to which France may respond in self-defence under Article 51 of the United Nations Charter. Definition of the threshold of violation is a political decision taken on a case-by-case basis in light of the criteria established by international law.”¹⁶⁶

1.1.2. Some cyberoperations may violate the prohibition of the threat or use of force

The most serious violations of sovereignty, especially those that infringe France’s territorial integrity or political independence, may violate the prohibition of the threat or use of force, which applies to any use of force, regardless of the weapons employed. In digital space, crossing the threshold of the use of force depends not on the digital means employed but on the effects of the cyberoperation.

A cyberoperation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those that result from the use of conventional weapons.

However, France does not rule out the possibility that a cyberoperation without physical effects may also be characterised as a use of force. In the absence of physical damage, a cyberoperation may be deemed a use of force against the yardstick of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target. This is of course not an exhaustive list. For example, penetrating military systems in order to compromise French defence capabilities, or financing or even training individuals to carry out cyberattacks against France, could also be deemed uses of force.

However, not every use of force is an armed attack within the meaning of Article 51 of the United Nations Charter, especially if its effects are limited or reversible or do not attain a certain level of gravity.”¹⁶⁷

1.2. A cyberattack that causes damage of a significant scale or severity may constitute an armed attack giving entitlement to the use of self-defence

In accordance with the case law of the International Court of Justice (ICJ), France distinguishes the gravest forms of the use of force, which constitute an armed attack to which the victim State may respond by individual or collective self-defence, from other less grave forms. Cyberattacks may constitute a grave form of the use of force to which France could respond by self-defence.

¹⁶⁵ Estonia: Kaljulaid Speech.

¹⁶⁶ France: Operations in Cyberspace, p. 6.

¹⁶⁷ Ibid. p. 7.

“1.2.1. Categorisation of a cyberattack as an armed attack

France reaffirms that a cyberattack may constitute an armed attack within the meaning of Article 51 of the United Nations Charter, if it is of a scale and severity comparable to those resulting from the use of physical force. In the light of these criteria, the question of whether a cyberattack constitutes armed aggression will be examined on a case-by-case basis having regard to the specific circumstances.

A cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to paralyse whole swathes of the country’s activity, trigger technological or ecological disasters and claim numerous victims. In such an event, the effects of the operation would be similar to those that would result from the use of conventional weapons.

To be categorised as an armed attack, a cyberattack must also have been perpetrated, directly or indirectly, by a State. Leaving aside acts perpetrated by persons belonging to State organs or exercising elements of governmental authority, a State is responsible for acts perpetrated by non-state actors only if they act *de facto* on its instructions or orders or under its control in accordance with the rules on State responsibility for internationally wrongful acts and ICJ case law. To date, no State has categorised a cyberattack against it as an armed attack. In accordance with ICJ case law, France does not recognise the extension of the right to self-defence to acts perpetrated by non-state actors whose actions are not attributable, directly or indirectly, to a State.”¹⁶⁸

Germany

“In Germany’s opinion, [the question whether hostile cyber-action is an armed attack”] depends on its scale and effects: If a state finds itself the target of a cyber-operation with effects comparable to an armed attack, it may exercise its right to self-defence. Factors to be taken into account include, *inter alia*, the seriousness of the attack, the immediacy of its effects, depth of penetration of the cyber infrastructure and its military character.

Even in cases where one cannot speak of a use of force, the use of cyber capabilities might constitute a violation of sovereignty, if the attack can be attributed to a state, which then in turn could lead to consequences within the confines of public international law.”¹⁶⁹

The Netherlands

“The government believes that cyber operations can fall within the scope of the prohibition of the use of force, particularly when the effects of the operation are comparable to those of a conventional act of violence covered by the prohibition. In other words, the effects of the operation determine whether the prohibition applies, not the manner in which those effects are achieved. (...) A cyber operation would therefore in any case be qualified as a use of force if its scale and effects reached the same level as those of the use of force in non-cyber operations.

International law does not provide a clear definition of ‘use of force’. The government endorses the generally accepted position that each case must be examined individually to establish whether the ‘scale and effects’ are such that an operation may be deemed a violation of the prohibition of use of force. (...) In the view of the government, at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force.

168 *Ibid.* p. 8.

169 *Germany: Riedel Speech.*

It is necessary, when assessing the scale and effects of a cyber operation, to examine both qualitative and quantitative factors. *The Tallinn Manual 2.0* refers to a number of factors that could play a role in this regard, including how serious and far-reaching the cyber operation's consequences are, whether the operation is military in nature and whether it is carried out by a state. These are not binding legal criteria. They are factors that could provide an indication that a cyber operation may be deemed a use of force, and the government endorses this approach. It should be noted in this regard that a cyber operation that falls below the threshold of use of force may nonetheless be qualified as a prohibited intervention or a violation of sovereignty.”¹⁷⁰

United Kingdom

“The next relevant provision of the UN Charter is in Article 2(4) which prohibits the threat or use of force against the territorial independence or political integrity of any state. Any activity above this threshold would only be lawful under the usual exceptions – when taken in response to an armed attack in self-defence or as a Chapter VII action authorised by the Security Council. In addition, the UK remains of the view that it is permitted under international law, in exceptional circumstances, to use force on the grounds of humanitarian intervention to avert an overwhelming humanitarian catastrophe.

Thirdly, the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter.

If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means.”¹⁷¹

“Article 2(4) of the United Nations Charter (which reflects customary international law) prohibits the threat or use of force. A cyber operation may constitute a use of force if it causes the same or similar effects as a kinetic attack.

Armed attack is not defined in international law, but it is generally accepted that it must be an act of armed force of sufficient gravity, having regard to its scale and effects. A cyber operation may constitute an armed attack if its method, gravity and intensity of force is such that its effects are equivalent to those achieved by a kinetic attack which would reach the level of an armed attack.”¹⁷²

170 *Netherlands: Letter to Parliament*, pp. 3-4.

171 *UK: Wright Speech*.

172 *UK: Cyber Primer*, pp. 12-13.

Due Diligence in Cyberspace

Australia

“To the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states. In this context, we note it may not be reasonable to expect (or even possible for) a state to prevent all malicious use of ICT infrastructure located within its territory. However, in Australia’s view, if a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law.”

Estonia

“Thirdly, states must keep on strengthening their own resilience to cyber threats and disruptions, both individually and collectively. Therefore, states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states. They should strive to develop means to offer support when requested by the injured state in order to identify, attribute or investigate malicious cyber operations. This expectation depends on national capacity as well as availability, and accessibility of information. As I mentioned here last year, we have to also consider the capacities of different states to be able to control such operations that exploit their infrastructure or systems. Therefore, meeting this expectation should encompass taking all feasible measures, rather than achieving concrete results.

And this also means that further effort must go to cyber capacity building and development cooperation to increase states’ capacity to prevent and respond to cyber threats.”¹⁷³

France

“France exercises its sovereignty over the information systems located on its territory. In compliance with the due diligence requirement, it ensures that its territory is not used for internationally wrongful acts using ICT. This is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors.”¹⁷⁴

“The fact that a State fails to comply with its due diligence obligation can justify the taking of political and diplomatic measures that may include counter-measures or a referral to the UNSC. The fact that a State does not take all reasonable measures to stop wrongful acts against other States perpetrated from its territory by non-state actors, or is incapable of preventing them, cannot constitute an exception to the prohibition of the use of force.”¹⁷⁵

173 *Estonia: Kaljulaid Speech*.

174 *France: Operations in Cyberspace*, p. 6.

175 *France: Operations in Cyberspace*, p. 10.

Germany

“There is consensus that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of activities related to information and communication technology, and to their jurisdiction over the required infrastructure within their territory.

Such sovereign rights carry duties as well. We believe that States must provide an adequate level of protection for IT infrastructure on their territory, with a view of safeguarding the overall functionality and stability of the Internet.”¹⁷⁶

Netherlands

“It should be noted that not all countries agree that the due diligence principle constitutes an obligation in its own right under international law. The Netherlands, however, does regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act.

In the context of cyberspace, the due diligence principle requires that states take action in respect of cyber activities:

- carried out by persons in their territory or where use is made of items or networks that are in their territory or which they otherwise control;
- that violate a right of another state; and
- whose existence they are, or should be, aware of.

To this end a state must take measures which, in the given circumstances, may be expected of a state acting in a reasonable manner. It is not relevant whether the cyber activity in question is carried out by a state or non-state actor, or where this actor is located. If, for example, a cyberattack is carried out against the Netherlands using servers in another country, the Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers, regardless of whether or not it has been established that a state is responsible for the cyberattack.

It is generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers sufficiently serious adverse consequences. The precise threshold depends on the specific circumstances of the case. It is clear, however, that such adverse consequences do not necessarily have to include physical damage.”¹⁷⁷

Attribution

Australia

“It is a longstanding rule of international law that, if a state acts in violation of an international obligation, and that violation is attributable to the state, that state will be responsible for the violation.

The customary international law on state responsibility, much of which is reflected in the International Law Commission’s Articles on the Responsibility of States for Internationally Wrongful Acts, apply to state behaviour in cyberspace.”¹⁷⁸

Estonia

“[S]tates have the right to attribute cyber operations both individually and collectively according to international law. Our ability and readiness to effectively cooperate among allies and partners in exchanging information and attributing malicious cyber activities has improved. The opportunities

176 *Germany: Riedel Speech.*

177 *Netherlands: Letter to Parliament*, pp. 3-4.

178 *Australia: Cyber Engagement Strategy*, p. 91.

for malicious actors to walk away from their harmful actions with plausible deniability are clearly shrinking. Last year demonstrated that states are able to attribute harmful cyber operations both individually or in a coordinated manner. It is not something unachievable and endlessly complex. At the end of the day what is required from the attributing state, is not absolute certainty but what is reasonable. When assessing malicious cyber operations we can consider technical information, political context, established behavioural patterns and other relevant indicators.

More than simply attributing, we must take a stance that harmful cyber operations cannot be carried out without consequences. One good example would be EU's Cyber Diplomacy Toolbox, which foresees a framework for joint EU diplomatic response to malicious cyber activities. Two weeks ago, EU Member States agreed on a horizontal framework which will allow to impose restrictive measures, or sanctions, against malicious cyber operations in similar manner as it is possible for terrorist acts or use of chemical weapons. Several allies have already taken diplomatic steps or set in place economic restrictive measures against adversarial states, or individuals responsible for harmful cyber operations."¹⁷⁹

France

"When a cyberattack is detected, France takes the necessary steps to categorise it, which may include neutralising its effects. Identification of the instigator is based mainly, though not solely, on technical information gathered during investigations of the cyberattack, especially identification of the attack and transit infrastructure for the cyberoperation and its location, identification of the adversary methods of operation (AMO), the overall chronology of the perpetrator's activities, the scale and gravity of the incident and the compromised perimeter, or the effects sought by the attacker. This information can help to determine whether or not a link exists between the instigators and a State.

A cyberattack is deemed to have been instigated by a State if it has been perpetrated by a State organ, a person or entity exercising elements of governmental authority, or a person or group of persons acting on the instructions of, or under the direction or control of that State.

The identification of a State as being responsible for a cyberattack that is an internationally unlawful act does not in any way oblige the victim State to make a public attribution. Such attribution is a discretionary choice made, *inter alia*, according to the nature and origin of the operation, the specific circumstances and the international context. It is a sovereign decision insofar as France reserves the right to attribute publicly, or not, a cyberattack against it and to bring that information to the attention of its population, other States or the international community. This policy does not rule out close coordination with France's allies and partner States, including international or regional organisations, in particular the European Union (EU) and the North Atlantic Treaty Organisation (NATO). However, while the decision may go as far as collective attribution of a cyberattack, it lies solely with France. In addition, international law does not require States to provide the evidence on which the public attribution of a cyberattack is based, though such information helps to legitimise the validity of such attribution.

In all events, a decision not to publicly attribute a cyberattack is not a final barrier to the application of international law, and in particular to assertion of the right of response available to States."¹⁸⁰

179 *Estonia: Kaljulaid Speech.*

180 *France: Operations in Cyberspace*, pp. 10-11.

Germany

“Das völkerrechtliche Unterscheidungsgebot erfordert aber bei der Nutzung technischer Einrichtungen und Aktivitäten im Cyber-Raum nicht, die Zurechenbarkeit zu einem bestimmten Staat offenzulegen.”¹⁸¹

„However, the principle of distinction under international law does not require, when using technical facilities and [conducting] activities in cyberspace, to disclose the attribution to a particular State.” (own translation)

Netherlands

“For a state to be held responsible under international law for a cyber operation and, by extension, for a target state to be able to take a countermeasure in response, it must be possible to attribute the operation to the state in question. Any attribution of cyber operations is always based on a government decision. Special attention is paid to the degree to which the government has information of its own at its disposal or to which it is able to reach an independent conclusion concerning information it has obtained.

In the context of cyberspace, three forms of attribution can be distinguished:

- Technical attribution – a factual and technical investigation into the possible perpetrators of a cyber operation and the degree of certainty with which their identity can be established.
- Political attribution – a policy consideration whereby the decision is made to attribute (publicly or otherwise) a specific cyber operation to an actor without necessarily attaching legal consequences to the decision (such as taking countermeasures). The attribution need not necessarily relate to a state; it may also concern a private actor.
- Legal attribution – a decision whereby the victim state attributes an act or omission to a specific state with the aim of holding that state legally responsible for the violation of an obligation pursuant to international law.

In the case of legal attribution a distinction must be made between operations carried out by or on behalf of a state and operations carried out by non-state actors. An act by a government body in its official capacity (for example the National Cyber Security Centre) is always attributable to the state. An act by a non-state actor is in principle not attributable to a state. However, the situation changes if a state has effective control over the act or accepts it as its own act after the fact. In such a case, then on-state actor (or ‘proxy’) carries out the operation on the instructions of, or under the direction or control of that state. The threshold for establishing effective control is high. A financial contribution to the activities of a non-state actor, for example, is not sufficient.

In order to attribute a cyber operation it is not required that a state disclose the underlying evidence. Evidence in the legal sense becomes relevant only if legal proceedings are instituted. A state that takes countermeasures or relies on its inherent right of self-defence (see below) in response to a cyber operation may eventually have to render account for its actions, for example if the matter is brought before the International Court of Justice. In such a situation, it must be possible to provide evidence justifying the countermeasure or the exercise of the right of self-defence. This can include both information obtained through regular channels and intelligence.

Under international law there is no fixed standard concerning the burden of proof a state must meet for (legal) attribution, and thus far the International Court of Justice has accepted different standards of proof. The CAVV and the AIV rightly observe as follows in this regard: *‘International law does not have hard rules on the level of proof required but practice and case law require sufficient certainty on the origin of the attack and the identity of the author of the attack before action can be taken.’*

181 Germany: BT-Drs, p. 11.

In the government's view, the burden of proof will indeed vary in accordance with the situation, depending on the seriousness of the act considered to be in breach of international law and the intended countermeasures."¹⁸²

United Kingdom

"The international law rules on the attribution of conduct to a state are clear, set out in the International Law Commissions Articles on State Responsibility, and require a state to bear responsibility in international law for its internationally wrongful acts, and also for the acts of individuals acting under its instruction, direction or control.

These principles must be adapted and applied to a densely technical world of electronic signatures, hard to trace networks and the dark web. They must be applied to situations in which the actions of states are masked, often deliberately, by the involvement of non-state actors. And international law is clear - states cannot escape accountability under the law simply by the involvement of such proxy actors acting under their direction and control.

But the challenge, as ever, is not simply about the law. As with other forms of hostile activity, there are technical, political and diplomatic considerations in publicly attributing hostile cyber activity to a state, in addition to whether the legal test is met.

There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based, or to publicly attribute hostile cyber activity that it has suffered in all circumstances.

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

For example, the WannaCry ransomware attack affected 150 countries, including 48 National Health Service Trusts in the United Kingdom. It was one of the most significant attacks to hit the UK in terms of scale and disruption. In December 2017, together with partners from the US, Australia, Canada, New Zealand, Denmark and Japan, we attributed the attack to North Korean actors. Additionally, our attribution, together with eleven other countries, of the destructive NotPetya cyber-attack against Ukraine to the Russian government, specifically the Russian Military in February this year illustrated that we can do this successfully. If more states become involved in the work of attribution then we can be more certain of the assessment. We will continue to work closely with allies to deter, mitigate and attribute malicious cyber activity. It is important that our adversaries know their actions will be held up for scrutiny as an additional incentive to become more responsible members of the international community."¹⁸³

United States

"States are legally responsible for activities undertaken through "proxy actors," who act on the State's instructions or under its direction or control. The ability to mask one's identity and geography in cyberspace and the resulting difficulties of timely, high-confidence attribution can create significant challenges for States in identifying, evaluating, and accurately responding to threats. But putting attribution problems aside for a moment, established international law does address the question of proxy actors. States are legally responsible for activities undertaken through putatively private actors, who act on the State's instructions or under its direction or control. If a State exercises a

¹⁸² Netherlands: Letter to Parliament, pp. 6-7.

¹⁸³ UK: Wright Speech.

sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it. These rules are designed to ensure that States cannot hide behind putatively private actors to engage in conduct that is internationally wrongful. (...)

As I mentioned earlier, cyberspace significantly increases an actor's ability to engage in attacks with "plausible deniability," by acting through proxies. I noted that legal tools exist to ensure that States are held accountable for those acts. What I want to highlight here is that many of these challenges – in particular, those concerning attribution – are as much questions of a technical and policy nature rather than exclusively or even predominantly questions of law. Cyberspace remains a new and dynamic operating environment, and we cannot expect that all answers to the new and confounding questions we face will be legal ones.

These questions about effects, dual use, and attribution are difficult legal and policy questions that existed long before the development of cyber tools, and that will continue to be a topic of discussion among our allies and partners as cyber tools develop. Of course, there remain many other difficult and important questions about the application of international law to activities in cyberspace – for example, about the implications of sovereignty and neutrality law, enforcement mechanisms, and the obligations of States concerning "hacktivists" operating from within their territory. While these are not questions that I can address in this brief speech, they are critically important questions on which international lawyers will focus intensely in the years to come.

And just as cyberspace presents challenging new issues for lawyers, it presents challenging new technical and policy issues. Not all of the issues I've mentioned are susceptible to clear legal answers derived from existing precedents – in many cases, quite the contrary. Answering these tough questions within the framework of existing law, consistent with our values and accounting for the legitimate needs of national security, will require a constant dialogue between lawyers, operators, and policymakers. All that we as lawyers can do is to apply in the cyber context the same rigorous approach to these hard questions that arise in the future, as we apply every day to what might be considered more traditional forms of conflict."¹⁸⁴

"States and commentators often express concerns about the challenge of attribution in a technical sense—that is, the challenge of obtaining facts, whether through technical indicators or all-source intelligence, that would inform a State's determinations about a particular cyber incident. Others have raised issues related to political decisions about attribution – that is, considerations that might be relevant to a State's decision to go public and identify another State as the actor responsible for a particular cyber incident and to condemn that act as unacceptable. These technical and policy discussions about attribution, however, should be distinguished from the legal questions about attribution. In my present remarks, I will focus on the issue of attribution in the legal sense.

From a legal perspective, the customary international law of state responsibility supplies the standards for attributing acts, including cyber acts, to States. For example, cyber operations conducted by organs of a State or by persons or entities empowered by domestic law to exercise governmental authority are attributable to that State, if such organs, persons, or entities are acting in that capacity.

Additionally, cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own.

¹⁸⁴ USA: Koh Speech, pp. 6-8.

Thus, as a legal matter, States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When there is information—whether obtained through technical means or all-source intelligence – that permits a cyber act engaged in by a non-State actor to be attributed legally to a State under one of the standards set forth in the law of state responsibility, the victim State has all of the rights and remedies against the responsible State allowed under international law.

The law of state responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution. In this context, a State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. Absolute certainty is not – and cannot be – required. Instead, international law generally requires that States act reasonably under the circumstances when they gather information and draw conclusions based on that information.

I also want to note that, despite the suggestion by some States to the contrary, there is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action. There may, of course, be political pressure to do so, and States may choose to reveal such evidence to convince other States to join them in condemnation, for example. But that is a policy choice—it is not compelled by international law.”¹⁸⁵

Countermeasures

Australia

“If a state is a victim of malicious cyber activity which is attributable to a perpetrator state, the victim state may be able to take countermeasures against the perpetrator state, under certain circumstances. However, countermeasures that amount to a use of force are not permissible. Any use of countermeasures involving cyberspace must be proportionate. It is acknowledged that this raises challenges in identifying and assessing direct and indirect effects of malicious cyber activity, in order to gauge a proportionate response. The purpose of countermeasures is to compel the other party to desist in the ongoing unlawful conduct.”¹⁸⁶

Estonia

“Cyber should no longer look like an easy choice of weapons and therefore we must be ready to use deterrence tools. First and foremost, states must refrain from the threat of or use of force against the territorial integrity and political independence of other states. However, we already know that cyber operations, which cause injury or death to persons or damage or destruction of objects, could amount to use of force or armed attack under the UN Charter. We here in Estonia are very much dependent on a stable and secure cyberspace. Such harmful effects could be caused by a cyber operation, which for example, targets digital infrastructure or services necessary for the functioning of society. And let’s not forget – growing digitalization of our societies and services can also lower the threshold for harmful effects. In order to prevent such effects, states maintain all rights, in accordance with international law, to respond to harmful cyber operations either individually or in a collective manner.

Among other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected

185 USA: Egan Speech, p. 177.

186 Australia: *Cyber Engagement Strategy*, p. 90.

by the malicious cyber operation. The countermeasures applied should follow the principle of proportionality and other principles established within the international customary law. International security and the rules-based international order have long benefitted from collective efforts to stop the violations. We have seen this practice in the form of collective self-defence against armed attacks. For malicious cyber operations, we are starting to see this in collective diplomatic measures I mentioned before. The threats to the security of states increasingly involve unlawful cyber operations. It is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no lawful recourse to use of force exists. Allies matter also in cyberspace.”¹⁸⁷

France

“A decision to respond is a political one, taken in compliance with international law. Such a response may include the use of force, depending on the gravity of the cyberattack. Any unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty. If it is accompanied by effects that constitute a use of force within the meaning of Article 2, para. 4 of the United Nations Charter, France may take counter-measures or bring the matter before the United Nations Security Council (UNSC). (...)

States targeted by such cyberattacks are entitled to respond to them within the framework of the options offered by international law. In response to a cyberattack, France may consider diplomatic responses to certain incidents, counter-measures, or even coercive action by the armed forces if an attack constitutes armed aggression.”¹⁸⁸

“In general, France can respond to cyberattacks by taking counter-measures. In response to a cyberattack that infringes international law (including use of force), France may take counter-measures designed to (i) protect its interests and ensure they are respected and (ii) induce the State responsible to comply with its obligations.

Under international law, such counter-measures must be taken by France in its capacity as victim. Collective counter-measures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State’s rights.”¹⁸⁹

“Counter-measures must also be taken in compliance with international law, in particular the prohibition of the threat or use of force. Consequently, they form part of a peaceful response, their sole purpose being to end the initial violation, including in reaction to a cyberoperation that constitutes a use of armed force within the meaning of Article 2, para . 4 of the United Nations Charter. The response to a cyberoperation may involve digital means or not, provided that it is commensurate with the injury suffered, taking into account the gravity of the initial violation and the rights in question.

Lastly, the use of counter-measures requires the State responsible for the cyberattack to comply with its obligations. The victim State may, in certain circumstances, derogate from the obligation to inform the State responsible for the cyberoperation beforehand, where there is a need to protect its rights. The possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability.”¹⁹⁰

187 *Estonia: Kaljulaid Speech.*

188 *France: Operations in Cyberspace*, p. 6.

189 *Ibid.* p. 7.

190 *Ibid.* p. 8.

Netherlands

“If a state is the victim of a violation by another state of an obligation under international law (i.e. an internationally wrongful act), it may under certain circumstances take countermeasures in response. Countermeasures are acts (or omissions) that would normally constitute a violation of an obligation under international law but which are permitted because they are a response to a previous violation by another state. In cyberspace, for example, a cyber operation could be launched to shut down networks or systems that another state is using for a cyberattack. A countermeasure is different to the practice of retorsion in that it would normally be contrary to international law. For this reason, countermeasures are subject to strict conditions, including the requirement that the injured state invoke the other state’s responsibility. This involves the injured state establishing a violation of an obligation under international law that applies between the injured state and the responsible state, and requires that the cyber operation can be attributed to the responsible state. In addition, the injured state must in principle notify the other state of its intention to take countermeasures. However, if immediate action is required in order to enforce the rights of the injured state and prevent further damage, such notification may be dispensed with. Furthermore, countermeasures must be temporary and proportionate, they may not violate any fundamental human rights, and they may not amount to the threat or use of force.”¹⁹¹

United Kingdom

“Consistent with the de-escalatory nature of international law, there are clear restrictions on the actions that a victim state can take under the doctrine of countermeasures. A countermeasure can only be taken in response to a prior internationally wrongful act committed by a state, and must only be directed towards that state. This means that the victim state must be confident in its attribution of that act to a hostile state before it takes action in response. In cyberspace of course, attribution presents particular challenges, to which I will come in a few moments. Countermeasures cannot involve the use of force, and they must be both necessary and proportionate to the purpose of inducing the hostile state to comply with its obligations under international law.

These restrictions under the doctrine of countermeasures are generally accepted across the international law community. The one area where the UK departs from the excellent work of the International Law Commission on this issue is where the UK is responding to covert cyber intrusion with countermeasures.

In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it. The covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.

In addition, it is also worth stating that, as a matter of law, there is no requirement in the doctrine of countermeasures for a response to be symmetrical to the underlying unlawful act. What matters is necessity and proportionality, which means that the UK could respond to a cyber intrusion through non-cyber means, and vice versa.”¹⁹²

191 *Netherlands: Letter to Parliament*, p. 7.

192 *UK: Wright Speech*.

“An internationally wrongful act committed by a state entitles the injured state to take proportionate countermeasures. Countermeasures are actions:

- in light of a refusal to remedy the wrongful act;
- directed against the other state to induce compliance with its obligations; and
- which are proportionate.”¹⁹³

United States

“The customary international law doctrine of countermeasures permits a State that is the victim of an internationally wrongful act of another State to take otherwise unlawful measures against the responsible State in order to cause that State to comply with its international obligations, for example, the obligation to cease its internationally wrongful act. Therefore, as a threshold matter, the availability of countermeasures to address malicious cyber activity requires a prior internationally wrongful act that is attributable to another State. As with all countermeasures, this puts the responding State in the position of potentially being held responsible for violating international law if it turns out that there wasn’t actually an internationally wrongful act that triggered the right to take countermeasures, or if the responding State made an inaccurate attribution determination. That is one reason why countermeasures should not be engaged in lightly.

Additionally, under the law of countermeasures, measures undertaken in response to an internationally wrongful act performed in or through cyberspace that is attributable to a State must be directed only at the State responsible for the wrongful act and must meet the principles of necessity and proportionality, including the requirements that a countermeasure must be designed to cause the State to comply with its international obligations—for example, the obligation to cease its internationally wrongful act—and must cease as soon as the offending State begins complying with the obligations in question.

The doctrine of countermeasures also generally requires the injured State to call upon the responsible State to comply with its international obligations before a countermeasure may be taken—in other words, the doctrine generally requires what I will call a “prior demand.” The sufficiency of a prior demand should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement, which is to give the responsible State notice of the injured State’s claim and an opportunity to respond.

I also should note that countermeasures taken in response to internationally wrongful cyber activities attributable to a State generally may take the form of cyber-based countermeasures or non-cyber-based countermeasures. That is a decision typically within the discretion of the responding State and will depend on the circumstances.”¹⁹⁴

Self-defence

Australia

“Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber operations that constitute an armed attack and in respect of acts of self-defence that are carried out by cyber means. Thus if a cyber operation – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is

193 UK: *Cyber Primer*, p. 12.

194 USA: *Egan Speech*, pp. 178-179.

engaged. The rapidity of cyber attacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been raised by Australia in explaining its position on the concept of imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances. (...)

‘[A] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts.

This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy.

Consider, for example, a threatened armed attack in the form of an offensive cyber operation (and, of course, when I say ‘armed attack’, I mean that term in the strict sense of Article 51 of the Charter). The cyber operation could cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second. Is it seriously to be suggested that a state has no right to take action before that split-second?’

Attorney-General, Senator the Hon. George Brandis QC,
University of Queensland, 11 April 2017”¹⁹⁵

France

“Under Article 51 of the United Nations Charter, a State that suffers an armed attack is entitled to use individual or collective self-defence. Self-defence in response to an armed attack carried out in cyberspace may involve digital or conventional means in compliance with the principles of necessity and proportionality. On a decision by the President of the Republic to commit the French armed forces, the Armed Forces Ministry may carry out cyberoperations for military purposes in cyberspace.

Cyberattacks which do not reach the threshold of an armed attack when taken in isolation could be categorised as such if the accumulation of their effects reaches a sufficient threshold of gravity, or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or from different entities acting in concert.

In exceptional circumstances, France allows itself to use pre-emptive self-defence in response to a cyberattack that “has not yet been triggered but is about to be, in an imminent and certain manner, provided that the potential impact of such an attack is sufficiently serious”. However, it does not recognise the legality of the use of force on the grounds of preventive self-defence.

States which, in the conduct of a cyberoperation or in their response to a cyberattack, decide to use non-state actors, such as companies providing offensive cyber services or groups of hackers, are responsible for those actors’ actions. In view of the risk of systemic instability arising from the private-sector use of offensive capabilities, France, following on from the Paris Call, is in favour of regulating them strictly and prohibiting such non-state actors from carrying out offensive activities in cyberspace for themselves or on behalf of other non-state actors.

Lastly, any response on the grounds of self-defence remains provisional and subordinate. It must be promptly reported to the UNSC³⁷ and suspended as soon as the Security Council takes the matter in hand, replacing unilateral action with collective measures or, failing that, as soon as it has achieved its purpose, namely to repel or end the armed attack. Other measures, such as counter-measures or referral to the UNSC, may be preferred if they are deemed more appropriate.”¹⁹⁶

195 *Australia: 2019 Supplement*.

196 *France: Operations in Cyberspace*, p. 9.

Germany

“In order to cross the threshold of armed attack, the cyber attack must be equivalent in scope and effect to the use of conventional weapons and acts of war. The extent to which an activity fulfils these conditions can only be assessed on a case-by-case basis.”¹⁹⁷

“A State that has become the target of a cyber operation equivalent in scope and effect to an armed attack (...) is entitled to exercise the right to individual or collective self-defence, including cyber operations against the State or non-state actor to which the armed attack can be attributed. The extent to which an activity fulfils these conditions is, in turn, subject to a case-by-case assessment.”¹⁹⁸

Netherlands

“A state targeted by a cyber operation that can be qualified as an armed attack may invoke its inherent right of self-defence and use force to defend itself. This right is laid down in article 51 of the UN Charter. This therefore amounts to a justification for the use of force that would normally be prohibited under article 2(4) of the UN Charter. For this reason strict conditions are attached to the exercise of the right of self-defence.

An armed attack is not the same as the use of force within the meaning of article 2(4) of the UN Charter (see above). In the *Nicaragua* case, the International Court of Justice defined an armed attack as the most serious form of the use of force. This implies that not every use of force constitutes an armed attack.

To determine whether an operation constitutes an armed attack, the scale and effects of the operation must be considered. International law is ambiguous on the precise scale and effects an operation must have in order to qualify as an armed attack. It is clear, however, that an armed attack does not necessarily have to be carried out by kinetic means. This view is in line with the *Nuclear Weapons Advisory Opinion* of the International Court of Justice, in which the Court concluded that the means by which an attack is carried out is not the decisive factor in determining whether it constitutes an armed attack. The government therefore endorses the finding of the CAVV and the AIV that ‘*a cyber attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons (...)*’. There is therefore no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons.

At present there is no international consensus on qualifying a cyberattack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non-material consequences.

The government endorses the position of the International Court of Justice, which has observed that an armed attack must have a cross-border character. It should be noted that not all border incidents involving weapons constitute armed attacks within the meaning of article 51 of the UN Charter. This depends on the scale and effects of the incident in question.

The burden of proof for justifiable self-defence against an armed attack is a heavy one. The government shares the conclusion of the CAVV and the AIV that ‘*No form of self-defence whatever may be exercised without adequate proof of the origin or source of the attack and without convincing proof that a particular state or states or organised group is responsible for*

¹⁹⁷ Germany: *BT-Drs*, p. 10.

¹⁹⁸ *Ibid.* p. 11.

conducting or controlling the attack.’ States may therefore use force in self-defence only if the origin of the attack and the identity of those responsible are sufficiently certain. This applies to both state and non-state actors.

When exercising their right of self-defence, states must also meet the conditions of necessity and proportionality. In this regard the government shares the view of the CAVV and the AIV that invoking the right of self-defence is justifiable only ‘provided the intention is to end the attack, the measures do not exceed that objective and there are no viable alternatives. The proportionality requirement rules out measures that harbour the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future.’”¹⁹⁹

United Kingdom

“The next relevant provision of the UN Charter is in Article 2(4) which prohibits the threat or use of force against the territorial independence or political integrity of any state. Any activity above this threshold would only be lawful under the usual exceptions – when taken in response to an armed attack in self-defence or as a Chapter VII action authorised by the Security Council. In addition, the UK remains of the view that it is permitted under international law, in exceptional circumstances, to use force on the grounds of humanitarian intervention to avert an overwhelming humanitarian catastrophe.

Thirdly, the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter.

If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means.”²⁰⁰

“The inherent right of individual and collective self-defence is customary international law and is also recognised by Article 51 of the United Nations Charter. An armed attack or imminent armed attack triggers the right of self-defence or anticipatory self-defence. Any response under self-defence must be necessary and proportionate; it must be necessary to use force to deal with the threat. Military action should only be used as a last resort and the force used must be proportionate to the threat and limited to what is necessary to deal with the threat. There may be practical challenges in the application of self-defence to cyber, for example:

- in attributing a cyber attack;
- the speed with which an attack can be conducted, which greatly reduces the ability to respond to an imminent attack;
- the use of spoofing and deception by an actor that implicates another; and
- the difficulty of determining the original intent of the perpetrator, even if actions are provable and actors identifiable.”²⁰¹

¹⁹⁹ Netherlands: Letter to Parliament, pp. 8-9

²⁰⁰ UK: Wright Speech.

²⁰¹ UK: Cyber Primer, p. 13.

United States

“A State’s national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof. As the United States affirmed in its 2011 International Strategy for Cyberspace, ‘when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.’”²⁰²

“To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an “armed attack” that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response – such responses must still be necessary and of course proportionate. We recognize, on the other hand, that some other countries and commentators have drawn a distinction between the “use of force” and an “armed attack,” and view “armed attack” – triggering the right to self-defense – as a subset of uses of force, which passes a higher threshold of gravity. My point here is not to rehash old debates, but to illustrate that States have long had to sort through complicated jus ad bellum questions. In this respect, the existence of complicated cyber questions relating to jus ad bellum is not in itself a new development; it is just applying old questions to the latest developments in technology.”²⁰³

“In certain circumstances, a State may take action that would otherwise violate international law in response to malicious cyber activity. One example is the use of force in self-defense in response to an actual or imminent armed attack. Another example is that, in exceptional circumstances, a State may be able to avail itself of the plea of necessity, which, subject to certain conditions, might preclude the wrongfulness of an act if the act is the only way for the State to safeguard an essential interest against a grave and imminent peril.”²⁰⁴

202 USA: Koh Speech, p. 4.

203 USA: Koh Speech, p. 7.

204 USA: Egan Speech, p. 178.

Author

Przemysław Roguski is a Lecturer in Law at the Jagiellonian University in Kraków (Poland) and an expert on cybersecurity and international law at the Kościuszko Institute. His research focuses on the law of peacetime cyber operations and different aspects of international law relating to cybersecurity, ICT and internet governance. Previously, Przemysław has worked in private practice and as lecturer for the German Academic Exchange Service (DAAD). He holds law degrees from the University of Mainz (Germany), Trinity College Dublin (Ireland) and a PhD in international law from Jagiellonian University.

Acknowledgements


The author would like to thank Dennis Broeders, François Delerue and Kubo Mačák for their thorough reviews and valuable comments to an earlier version of this comparative analysis. As always, all errors or omissions remain my own.

All of the activities and publications of The Hague Program for Cyber Norms are supported by a grant of the Dutch Ministry of Foreign Affairs.

Contact information

E-mail: info@thehaguecybernorms.nl

Website: <https://www.thehaguecybernorms.nl>

 [@HagueCyberNorms](https://twitter.com/HagueCyberNorms)

Address

The Hague Program for Cyber Norms
Faculty of Governance and Global Affairs
Leiden University
Hague Campus
Turfmarkt 99
2511 DP The Hague

Colofon

Published March 2020.

No part of this publication may be reproduced without prior permission.

© The Hague Program for Cyber Norms/Leiden University.

Graphic design: www.pauloram.nl



THE HAGUE
PROGRAM
for Cyber Norms



Universiteit
Leiden