CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Tracing *opinio juris* in National Cyber Security Strategy Documents

Ann Väljataga

NATO CCD COE, Law researcher

Tallinn 2018

About the author

Ann Väljataga is a law researcher at the NATO CCD COE. The author would like to express her gratitude to Samuele De Tomas Colatin for valuable research assistance.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 21 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual 2.0*, the most comprehensive guide on how International Law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise Locked Shields. Every spring the Centre hosts in Tallinn the International Conference on Cyber Conflict, CyCon, a unique event joining key experts and decision-makers of the global cyber defence community. As of January 2018 CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations - to this date Austria, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Table of Contents

1. First sprouts of cyber *opinio juris* and why national cyber security strategies are a good place for spotting them

Strong *opinio juris* has been thought to be able to compensate for underdeveloped or incoherent state practice in the formation of public international law.[1] If so, then international cyber law is in particular need of manifestations of *opinio juris* of any kind, for practice is either contradictory or classified to the point of being undetectable. Traces of *opinio juris* can be found in national policy documents, guidelines, reports and manuals prepared by international organisations, and sometimes in the statements of senior politicians. Although it might be misleading to be still talking about cyber law as something overly novel or unprecedented, it is still definitely in a state of formation – a state in which any expressed *opinio juris* can only reflect an aspiration and therefore be indicative rather than descriptive. As opposed to their practices, states are slightly more externally communicative about declaring what they are aspiring to carry out and what they oppose, and sometimes even stating in black and white what they think they are legally bound to do. At this very formative stage, however, cyber *opinio juris* should also be sought in statements which bear legal significance but do not explicitly spell out commitment to a specific customary law. Besides that, *opinio juris* should also be sought where it departs from actual practice.

In the light of the latter, it should be clarified when a legally relevant statement can be considered strong enough to constitute evidence of *opinio juris.* First of all, since international law is ultimately made by states and states only, such declarations must be clearly attributable to states. Secondly, they must be expressed in a manner and forum that indicates a long-term focus and belief in an existing or desired norm, and thus announcements made merely for the purpose of short-lived media sensation, whitewashing or promoting a particular temporary political aim would not suffice. National cyber security strategies, on the contrary, while not being designed to contain legally binding (customary) norms, do communicate a state´s general position as to the rules and principles in cyber state practice and scholarly opinion, viewed as grey zones. Furthermore, a strategy is created to serve long-term objectives, and contains only declarations and aims that a state evaluates to be realistic and achievable. For this reason, the strategies are often overly general and extremely cautious in their formulations, which is why it is of no use to look for black-and-white statements and clear answers to the cyber law conundrum. However, while not constituting *opinio juris* itself, behind their misty phrasing the strategies do reveal evidence of prevalent state legal opinion.

Cyber *opinio juris* is a rare phenomenon since, for understandable reasons, states often shy away from strong verbal commitments and their consequences. As mentioned, traces of emerging *opinio* can also be found in the declarations of senior state officials. Through these channels, cyber *opinio juris* started to develop at just about the same time as NCSS-s were first adopted, starting from the general statement by Harold Koh that the US had made a firm commitment to applying existing IHL to situations of armed conflict involving cyber activities[2]. However strong, the statement was not followed by an elaboration.[3] In 2014, as a response to the Sony attack, President Barack Obama took a further step, signalling the

[1] See eg: Lepard, Brian D. *Customary international law: a new theory with practical applications*. Cambridge University Press, 2010, pp 111-112.
[2] Hongju Koh, Harold. "International law in cyberspace.", Yale law School Faculty Scholarship Series, 2012, available at: http://digitalcommons.law.yale.edu/fss_papers/4854
[3] Schmitt, Michael N., and Sean Watts. "The decline of international humanitarian Law Opinio Juris and the law of cyber warfare." *Tex. Int'l LJ* 50 (2015): 217.

possibility of response that could include a coercive element and publicly attributing the attacks to North Korea[4].

We can also find *opinio* from an entirely different canon in statements made by Russian Foreign Minister Andrei Krutskikh in response to the failure of the UN GGE in 2017. He argued that a permissive system of countermeasures and self-defence should not come before reliable technical and legal means of attribution, and consequently did not affirm the applicability of IHL in the cyber domain.[5] Although for the most part inspired and motivated by political goals, the latter protest gives clear evidence of *opinio juris* presented by Russia. Another instance of manifesting cyber *opinio juris* through policy documents (and subsequent public commentary) comes from the aftermath of the 2016 Democratic National Committee hacks, when the US Department of Defense argued that, while sovereignty underpins public international law as we know it, it is an abstract principle from which no binding rules stem.[6] Again, this rule serves a strategic purpose: not recognising obligations deriving from sovereignty allows states to conduct and respond to cyber operations against other states without breaching international law. At the same time, not recognising sovereignty will lead to weakening any protection that international law might offer against cyber attacks that do not amount to prohibited intervention, use of force or an armed attack.

Another area where traces of *opinio juris* would help the international community clear the mist would be more precise definitions of use of force and armed attack in cyberspace. Again, *opinio juris* is taking first steps in this area, although the steps sometimes go in opposite directions. The UK Attorney General has, however, shed some light on what would constitute an armed attack according to the UK´s approach, stating that an attack "against one of UK´s (ed.) nuclear reactors, resulting in widespread loss of life or a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects"[7] would qualify. Fortunately, the silence on cyber *opinio juris* is slowly being replaced by legally meaningful declarations on standalone occasions. A comprehensive analysis of the NCSS of key players would be a welcome addition to this tendency.

National cyber security strategies might serve as valuable sources for identifying *opinio juris* since, just like laws, they are meant to be overarching, time-resilient and not occasion- or technology-specific. Also, most often the procedure of drafting and adopting an NCSS is a joint endeavour of state officials responsible for international relations, economic affairs, defence, critical infrastructures and national security.[8] Therefore, the genesis of an NCSS involves more deliberation, consolidation and compromise than the issuance of a thematic policy paper or a public statement. As such, as far as non-legislative documents go, the procedure of drafting an NCSS is the most reminiscent of actual legislative drafting.

More clearly outlined legal thought can be found in strategies that have been issued over the last three years (so-called second or third generation strategies). Understandably, however, national cyber security strategies avoid legal language at all costs, to avoid consequences following from such declarations. The following analysis, therefore, is first and foremost a hypothetical prediction of the kind

---

[4] Sanger, David E., Schmidt, Michael S. and Perlroth , N. "Obama Vows a Response to Cyberattack on Sony", New York Times, 19 December 2014, available at: https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0

[5] ТАСС, "Эксперты: кибербезопасность РФ зависит от консолидации информационного сообщества", http://tass.ru/politika/4406609 (in Russian)

[6] Schmitt, M. "In Defense of Sovereignty in Cyberspace", JustSecurity, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/; Corn, Gary P., and Robert Taylor. "Sovereignty in the Age of Cyber." *AJIL Unbound* 111 (2017): 207-212.

[7] Attorney General's Office and The Rt Hon Jeremy Wright MP, "Cyber and International Law in the 21st Century", Speech on 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[8] Klimburg, Alexander, ed. *National cyber security framework manual*. NATO Cooperative Cyber Defence Centre of Excellence, 2012, p 59.

of normative framework that states which have expressed certain viewpoints in their strategies might prefer to see themselves as legally bound to. The grey zones of international cyber law that have been most heatedly debated by scholars and persistently exploited by some actors include questions regarding state responsibility and due diligence, the exact threshold of use of force or armed attack, self-defence and (collective) countermeasures. In 2017, however, the discussion was set back by some years, and questions such as whether international (humanitarian) law applies in cyber space, or whether sovereignty is merely a principle or a binding customary rule, have arisen.[9] National cyber security strategies of cyber competent nations are carefully drafted to reflect how the state would depict a normative ideal. And yet, understandably, they do not contain language that would allow direct legal connotations. The following analysis asks:

a) how is sovereignty approached?

b) what does due diligence entail? What is the standard of reasonableness in cyber strategies?

c) when and how should states react to cyber attacks? What are the thresholds of use of force and armed attack?

d) what are the sufficient grounds for state responsibility (the attribution problem)?

This study examines the recent cyber strategic documents of the United States, the United Kingdom, the Netherlands, China, France, Russia and Australia. Selection is based on the level of cyber power and significance that a particular state has, as well as the balance of competing worldviews and, in some cases, the clarity of legal thought in strategic documents. The scope is not, however, strictly limited to the list above; where relevant, illustrative examples are introduced from strategies of other states.

[9] Väljataga, A., „Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly,Incyder“, 1 September 2017, https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html

2. Revisiting (cyber) sovereignty and due diligence

The US and, more recently, the UK have expressed a view according to which alleged infringements of sovereignty are not infringements at all, since sovereignty is but an abstract principle and not a rule.[10] On the other end of the spectrum, Russia and China are ardently convinced of the binding nature of sovereignty. In June 2016, they signed the Joint Statement on Cooperation in Information Space Development, the first article of which states that both countries shall "jointly advocate respect to and oppose infringements on every country's sovereignty in information space". In particular, China, in its international cyber strategy – reportedly the world´s biggest state sponsor of cyber attacks[11] – has made sovereignty the very cornerstone of its international cyber policy, leaving no doubt as to whether it is a rule or an abstraction. China states in its national cyber security strategy:[12]

> "No infringement of sovereignty in cyberspace will be tolerated, the rights of all countries to independently choose their development path, network management method and Internet public policy, as well as to equally participate in international cyberspace governance will be respected."

Disregarding the joint declaration, the Russian Information Security Strategy[13] and the draft cyber strategy[14] remain surprisingly silent on cyber sovereignty. On the contrary, one finds praise for openness, interconnectivity and interoperability. Instead of maintaining a focus on cyber sovereignty, Russia gives priority to the concept technological sovereignty. Technological sovereignty should not be confused with cyber sovereignty, for it describes economic independence from global tech giants and emphasises the use of Russian hardware and software.[15]

We find support for sovereignty as a rule approach also in the strategies of NATO Allies. In its 2018 Cyberdefense Strategic Review, France recognises the term 'digital sovereignty', which is described as "the ability of France to retain in space the autonomous ability of appreciation, decision and action, as well as to preserve the most traditional elements of its sovereignty in the face of the new threats that exploit the increasing digitisation of society".[16]

---

[10] US, see *supra* note 3 ; UK, see *supra* note 4.
[11] Crowdstrike, „Observations From the Front Lines of Threat Hunting", October 2018, https://www.crowdstrike.com/resources/reports/observations-from-the-front-lines-of-threat-hunting/
[12] China, International Strategy of Cooperation on Cyberspace, 3 January 2017, unofficial translation available at: http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm
[13] Russian Federation, Doctrine of Information Security of the Russian Federation, 5 December 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 , paras 12 and 16.
[14] Ibid.
[15] Ibid
[16] France, Cyberdefense Strategic Review, 2018 as cited in: François Delerue, Aude Géry, „France's Cyberdefense Strategic Review and International Law, Lawfare", 23 March 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law

Furthermore, the review states that:

> "The principle of sovereignty applies to cyberspace. In this respect, France reaffirms its sovereignty over information and communication technologies (ICT) infrastructure [systèmes d'information], persons and cyber activities located within its territory, subject to its international legal obligations."[17]

Legally, such a claim of sovereignty would bring about the acceptance of obligations associated with it that can be summarised under the common denominator of due diligence. Therefore, the French review seems to acknowledge cyber due diligence, and implies that France is justified in exercising, and indeed obliged to assert, a reasonable level of control over the various actors in its cyber infrastructure.

Attribution through due diligence can, in a best case scenario, be a solution to the sense of impunity common among the more cyber-aggressive states. On the other hand, when applied opportunistically or recklessly, evoking state responsibility through due diligence could become a disruptor of international law, and a loose trigger for unnecessary escalation.[18] The scholarly jury on the matter is still out, and state practice is still yet to take shape. After its relatively strong statement on cyber due diligence, France proceeds to explain that "it must in particular work to reach an agreement at the international level on the obligations faced by a State whose infrastructure would be used for malicious purposes".[19]

The French review stands out by briefly raising the topic of attribution through due diligence; the majority of equivalent documents refrain from straightforward recognition of due diligence obligations, and circumvent connecting it to the problematics of attribution. That being said, traces of the recognition of due diligence obligations can, for instance, also be detected in Turkey's otherwise rather laconic national cyber security strategy, which declares one of Turkey's priorities to be the "fulfilment of all legal and social responsibilities by individuals, institutions, society and the state in providing cyber security".[20]

Due diligence implies that the more a State's cyber policy and legal opinion are built upon a strong concept of binding external sovereignty, the more it should recognise the obligations and international responsibilities arising from it. Due diligence is not a safeguard or responsibility embraced only by European cyber powers. Recognition of a similar level of responsibility can be found in the Chinese approach to sovereignty, which states that:

> "Upholding sovereignty in cyberspace not only reflects governments' responsibility and right to administer cyberspace in accordance with law, but also enables countries to build platforms for sound interactions among governments, businesses and social groups. This will foster a healthy environment for the advancement of information technology and international exchange and cooperation".[21]

---

[17] See also: François Delerue, Aude Géry, "France's Cyberdefense Strategic Review and International Law, Lawfare", 23 March 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law

[18] Jensen, Eric Talbot, and Sean Watts. "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer." *Tex. L. Rev.*95 (2016): 1555.

[19] France, Strategic review as referred to in: François Delerue, Aude Géry, "France's Cyberdefense Strategic Review and International Law", Lawfare, 23 March 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law

[20] Turkey, Cybersecurity strategy, 2016, http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf .

[21] China, National Cyber Security Strategy, 26 December 2016, unofficial translation available at: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

While representing polar opposites in the 'sovereignty as a principle vs sovereignty as a rule' debate, the US and China seem to view due diligence obligations in a surprisingly similar manner. The US Department of State International Strategy for Cybersecurity from March 2016 non-exhaustively lists its obligations and primary aims with regard to fostering its cyber security through threat detection and capacity building.[22]

When we look beyond both direct and veiled expressions of *opinio juris*, national cyber security strategies may have another role in clarifying the actual substance and scope of due diligence obligations. Whether applied in cyberspace or in any other domain, due diligence obligations are, at the end of the day, context dependent.[23] The degree of due diligence depends on the circumstances and issues at hand, taking into consideration the state's level of development.

This is exactly where national cyber security strategies might help shed some light on just which capabilities it would be reasonable to expect from a given state. Just as in the case of fostering international counter-terrorism, a state´s capacity-building obligations are regulated by the due diligence standard. The obligation would therefore indicate a duty to pursue and acquire through reasonably available opportunities the means and degree of control necessary to comply with international cyber security obligations.[24] Capacity building therefore depends on the resources a particular state has at its disposal. The 2016 US International Strategy for Cybersecurity lists among its priorities promoting the widespread adoption of cyber security best practices and frameworks, including national strategies, computer security incident response teams (CSIRTs), public-private partnerships and public awareness campaigns[25]. This is an example of the highest standard of perceived due diligence.

Furthermore, acknowledging interconnectivity, more developed states extend their objectives to include the provision of capacity building to other nations, in order to decrease the vulnerability of the global network of information systems. While this cannot be seen through the principle of due diligence, it emphases the importance of each nation being able to play its part in global cyber security. The US strategy spells out the underlying motivation, and the relationship between due diligence and international capacity building, when it states that[26]:

> "[A]ssistance, pursued in partnership with the Department of Homeland Security and others, is critical to achieving the Administration's cyber security goals at the bilateral, regional, and global levels. These goals include creating a global culture of cybersecurity due diligence, reducing intrusions and disruptions affecting U.S. networks, ensuring the resiliency of information infrastructure, and improving the security of the high-tech supply chain."

---

[22] U.S. International Strategy for Cyberspace, March 2016, https://www.state.gov/documents/organization/255732.pdf.
[23] International Court of Justice, Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), 26 Feb. 2007.
[24] For an analogy to counter-terrorism assistance see eg: Becker, Tal. *Terrorism and the state: rethinking the rules of state responsibility*. Bloomsbury Publishing, 2006, pp 142-144.
[25] Supra note 21, p 4.
[26] Ibid, p 21, see also: Australia, 2017 Foreign Policy White Paper, Chapter V, p 7, available at: https://www.fpwhitepaper.gov.au/foreign-policy-white-paper/chapter-five-keeping-australia-and-australians-safe-secure-and-free/open

Moreover, the Dutch International Cyber Strategy shifts its focus to the shared burden that comes with inherent interconnectivity, stating that:

> "Capacity building serves to further both short- and long-term objectives that are important to the Netherlands. The aim is to raise the level of knowledge and expertise in non-EU countries to the highest possible level in order to strengthen the currently weak links in the worldwide infrastructure of the internet."[27]

If one is to draw a rather speculative conclusion, it would be that, based on their national cyber security strategies, states:

- admit that sovereignty applies in cyberspace
- admit that it can be threatened and needs to be protected (though they are not on the same page as to whether sovereignty as a rule can be violated)
- agree that cyber due diligence follows from cyber sovereignty
- agree that cyber due diligence involves a certain level of capacity building
- have not agreed on whether and how cyber due diligence can form the basis for state responsibility

[27] The Netherlands, International Cyber Strategy, p 7; see also eg. Australia, Cyber Engagement Strategy, p 71, available at: https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_4_international_security_and_cyberspace.html

3. Foreign interference – breach of sovereignty, prohibited intervention, or a co-arising symptom of information freedom?

After the above cited French review[28], from an international law perspective one of the most bold, thorough and transparent strategic documents are Australia´s International Cyber Engagement Strategy and foreign policy white paper on open, free and secure cyberspace (hereinafter White Paper), which is extraordinarily outspoken in matters of state legal opinion. In the latter Australia announces its intention to exercise strict sovereign control to protect the cohesion of its society, the integrity of its institutions and the security of its borders and national infrastructure.[29] Besides this clear statement of internal sovereignty, Australia, in both the White Paper and in its International Cyber Engagement Strategy, prioritises its external sovereignty. In the introduction to the white paper Australia envisions cyberspace as "a realm where our ability to prosecute our interests freely is not constrained by the exercise of coercive power".[30]

The term coercive power has not been further substantiated. It can, however, be interpreted as pointing towards prohibited intervention, in the meaning of the ICJ judgement in *Nicaragua v United States of America*, whereby an intervention is only prohibited:

> "...bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."

Both strategies go on to reiterate the need to tackle unwanted "foreign influence" in domestic affairs, classifying it as one of Australia´s most important national interests.[31] In the context of recent hybrid and information operations, this statement instantly calls to mind election meddling. Although legally speaking it is difficult to classify election hacks through information operations as unlawful interventions since the coercive causality is usually missing or covert, Australian strategies seem to place these operations clearly in the category of breaches of sovereignty, if not as prohibited interventions. Unfortunately, though, neither of the Australian documents proceeds to elaborate the causal link between the intervention and the change a state is forced to take. *Opinio juris* on when coercion becomes evident is therefore still scarce, at least in strategy documents. Taking into account the increasing occurrence of interference through dis- and misinformation campaigns, combined with the fact that at least two major cyber powers have argued at the highest political level that prohibited

[28] Supra note 15.
[29] Australia, 2017 Foreign Policy White Paper, Chapter V: Open, Free and Secure Syberspace, available at: https://www.fpwhitepaper.gov.au/foreign-policy-white-paper/chapter-five-keeping-australia-and-australians-safe-secure-and-free/open
[30] Ibid, p 3.
[31] Ibid, p 6.

intervention, not breach of sovereignty, marks the threshold at which an internationally wrongful act can be detected, emergence of such *opinio* appears inevitable.

The 2018 US strategy makes mention of states that use sovereignty as a shield (see the Chinese notion of sovereignty above). It describes their adversaries' practices as follows:

> "They hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world."[32]

When talking about its own cyber-political postures and aims, the most recent US strategy indeed manages to avoid sovereignty-speech across the whole document. Nor does it offer a legal interpretation of election hacks.

The UK, in a similar way to the US, has expressed that sovereignty is a fundamental principle from which no binding rules arise. Its 2017 cybersecurity strategy noted that:

> "Cyberspace is only one sphere in which we must defend our interests and sovereignty. Just as our actions in the physical sphere are relevant to our cyber security and deterrence, so our actions and posture in cyberspace must contribute to our wider national security."

This raises the abstract, and perhaps improperly scholastic, question of whether something that cannot be violated has to be defended at all? When we look at some other core principles of law, such as "separation of powers" or "human dignity", it seems that the need to defend stems directly from the respective principle's vulnerability to violation.

External sovereignty is therefore recognised in most of the national cybersecurity strategies studied above. So far, no strategy has however expressis verbis supported the viewpoint that foreign intervention, such as election meddling, would constitute prohibited intervention and, consequently, grant the victim state the right to use proportionate countermeasures. Nor can any insight into whether another legally controversial form of intervention – cyber espionage - is considered internationally wrongful, or a mere necessary evil.

[32] National Cyber Strategy of the United States of America, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, p 34.

4. Thresholds: When to respond?

By denying the violability of sovereignty, the UK stripped itself of a means of protection. At the same time, its 2016 Cyber Primer places the threshold of use of force relatively low, asserting that, for instance, a sustained attack against the UK banking system, which could cause severe financial damage to the state, leading to a worsening economic security situation for the population, would qualify.[33] The UK´s policy documents do not further elaborate about what would mark the leap from use of force to an armed attack, and thus evoke the right to self-defence. Jeremy Wright specified that operations that would constitute an armed attack would consequently give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter. As examples, he referred to an attack on 'one of our nuclear reactors, resulting in widespread loss of life', and 'a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects'.[34] Already in 2011, in its Cyber Warfare Report, the Netherlands implied that a cyber-attack can be considered an "armed attack" if it leads to a serious disruption with long-lasting consequences. For instance, if a cyber-attack targets the entire financial system, or prevents the government from carrying out essential tasks such as policing or taxation, it would qualify as an armed attack and would therefore trigger a state's right to defend itself.

Australia follows the lead of the *Tallinn Manual 2.0* and declares that it will apply the scale and effects test as introduced by the ICJ in *Nicaragua*. The Engagement Strategy explains that, in order to classify a malicious cyber operation as an armed attack, the intended or reasonably expected direct and indirect consequences of the cyber-attack should be considered, 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. Australia also voices concern over the fact that "international peace, security and stability could be equally threatened by the cumulative effect of repeated low-level malicious online behaviour". It proceeds to treat repeated under-the-threshold actions as clear-cut instances of armed attack, provided that the cumulative scale and effects are equivalent. In a similar vein, the French review emphasises that an armed attack is defined by its scale and effects, implicitly taking up the two cumulative criteria defined in *Nicaragua*.[35] It further states that a cyber-attack could be characterised as an armed attack "because of substantial human casualties" or "considerable physical damage to objects".

We find hypothetical notions of the possibility of a cyber-attack rising to the level of an armed attack in numerous strategies and high-level political statements, from both sides of the cyber ideological divide.[36] However, more specific contextualisation, such as the examples above, remain rare. This leads to the conclusion that there is no factual consensus on whether kinetic consequences are necessary for a malicious cyber operation to qualify, either as a use of force or as an armed attack.

---

[33] United Kingdom Ministry of Defence, Cyber Primer 2nd Edition, 2016, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf

[34] United Kingdom, AG Jeremy Wright, Speech on Cyber and International Law, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[35] France, Cyberdefense Strategic Review, supra note 14.

[36]: See eg NATO Cyber Defense Pledge, Warsaw, 2016; Tallinn Manual, Rule 11, p 47; See eg Japan 2018, http://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf ; The Netherlands, The Netherlands, National Cyber Security Agenda,2018, pp 23-24, https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html ; ТАСС, "Эксперты: кибербезопасность РФ зависит от консолидации информационного сообщества", 11 July 2017, available at: http://tass.ru/politika/4406609; Belgium, Cyber Security Strategy for Defence, 2014, p 7, https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf .

5. Responses: How to respond?

Relying on the premise that use of force and its gravest form – armed attack – is possible in the cyber domain, it seems obvious to assume that serious instances of malicious cyber operations should trigger the right to turn to retorsions, countermeasures or self-defence. A majority of the studied strategies leave no room for doubt in this regard. However, it was precisely this that became the main stumbling block in the 2017 GGE. As mentioned above, the Netherlands indicated a threshold of armed attack, and this statement was followed by the Netherlands noting that such attacks would trigger the right to self-defence. In its 2018 military cyber strategy, the Netherlands is open about integrating offensive cyber capabilities into its missions, and contributing to NATO operations.

Examples of direct references to the capacity and intention of developing countermeasures are also found in the strategy of the Czech Republic. Among other objectives, the state´s key aims include increasing national capacities for active cyber defence, cyber-attack countermeasures and the training of experts specialised in questions of active counter-measures in cyber security, cyber defence and in offensive approaches to cyber security in general.[37] The UK has openly expressed an ambition to become the world leader in offensive cyber capabilities.[38] The Australian Cyber Engagement Strategy states that its array of responses "could include, but is not restricted to, offensive cyber capabilities that disrupt, deny or degrade the computers or computer networks of adversaries". It goes on to reiterate that the response would, in any case, be in line with the principle of proportionality, Australia´s conviction being that international law does indeed apply in cyberspace. Other response measures that states have raised include using technologies to induce attacks to collect information on attackers, conducting measures against botnets,[39] and upstream disruptions to block malicious traffic.[40]

Japan is embracing the concept of active defence: see, for instance, the Ise-Shima Summit of 2017, at which the G7 leaders affirmed that cyber activities could amount to use of force or an armed attack within the meaning of international law. Moreover, as G7 foreign ministers affirmed at Lucca, a state that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures against the state responsible for the wrongful act, among other lawful responses. Relying on the above, Japan declares that it will utilise political, economic, technological, legal, diplomatic, and all other viable and effective means and capabilities, depending on the threat, and take resolute responses against cyber threats that undermine national security, including those that are possibly state-sponsored.[41]

The French review articulates a clear confidence in the applicability of international law to cyber operations. This also applies to countermeasures, self-defence and international humanitarian law. These fundamentals are worth reiterating, especially after the ideological divergence that proved fatal to the 2017 UN GGE. One way in which the review stands out is in its prescription of active defence measures (that technically are in fact bordering on offence) by making it clear that, in the case of an attack, France intends to respond by taking necessary and proportionate technical measures to neutralise the effects of the attack. When read in line with its national legislation, this would include carrying out the technical operations necessary to characterise the attack and to neutralise its effects by accessing the ICT systems at their origin.[42] The British cybersecurity strategy abandons the defence-centric narrative altogether, and declares one of its aims to be having the means to respond to cyber-

[37] Czech Republic, National Cyber Security Strategy, p 18.
[38] UK, National Cyber Security Strategy 2016 - 2021, p 51.
[39] Japan, National Cyber Security Strategy, p 23.
[40] Australia, Cyber Engagement Startegy, supra note 27, p 36.
[41] Japan, supra note 38, p 43.
[42] François Delerue, Aude Géry, France's Cyberdefense Strategic Review and International Law, Lawfare, 23 March 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law

attacks in the same way as it responds to any other attack, using whichever capability is most appropriate, including an offensive cyber capability. The strategy also provides detail on what is meant by sovereign offensive capabilities:

> "Offensive cyber capabilities involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction. Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere."[43]

The French review also offers uncommon lucidity with regard to how the particularities of the cyber domain might influence the essence of countermeasures and self-defence. It argues strongly for the possibility of pre-emptive self-defence, as well as of anticipatory and/or collective response as set forth in the EU cyber diplomacy toolbox. Furthermore, the US is hinting at the possibility of collective response without explicit reference to countermeasures or retorsions. The US National Cyber Strategy states that the US will work with partners when appropriate to impose consequences against malicious cyber actors in response to their activities against the US and its interests.

While taking collective countermeasures is formally prohibited under positive international law, all the studied strategies acknowledge that the majority of cyber operations take place under the threshold of an armed attack, and accordingly the emphasis has shifted from self-defence to countermeasures. The latter, when read in conjunction with the general approval of collective response, could signify that *opinio juris* as palpable in national strategies is currently bent towards overriding the prohibition on collective countermeasures.

[43] Ibid.

6. Clearing the mist around attribution

Opinio juris has also acquired much clearer contours with regard to what is otherwise known as the final frontier of international cyber law – attribution. While there were previous instances, the breakthrough towards more forthcoming attribution was made in 2014, when the Sony hack was publicly attributed to North Korea. In March 2017, the US Department of Justice indicted two Russian individuals for "computer hacking, economic espionage and other criminal offenses in connection with a conspiracy, beginning in January 2014, to access Yahoo's network and the contents of webmail accounts". Germany has also seen a number of cyber-attacks since 2015, including the attack on the German parliament in 2015, the spear-phishing attacks on political parties and foundations in 2016, and the worldwide "NotPetya" virus in 2017. Germany has attributed these attacks to actors associated with Russia.

On 4 October 2018, the British National Cyber Security Centre published a news release that contained perhaps the most clear-cut attribution that we have witnessed to date. The Foreign Office candidly blamed Russia for four major cyber-attacks: BadRabbit ransomware, the WADA data leak, the DNC email leak and unauthorised access to Islam Channel emails and to its internal network. All these incidents were attributed with high confidence to Russian foreign intelligence services. The news release noted, among other things, that these attacks constituted a flagrant violation of international law, which marks a rare precedent of forthright legal attribution[44]. The prevailing tendency reflected in both state practice and *opinio* is to admit that attribution is difficult, and to set a goal to work towards overcoming these hindrances through intelligence cooperation and by boosting digital forensics.[45]

As discussed in the section on sovereignty, the French strategic review contains the option of evoking state responsibility by crossing the so-called attribution gap, through claiming a breach of the due diligence obligation. This remains a notable exception. In parallel with evolving state practice, *opinio juris* regarding attribution is also becoming clearer in national cyber security strategies. In its 2018 National Defence Cyber Strategy, the Dutch Ministry of Defence expresses support for a threefold model of attributing cyber incidents. It states that:

> "The increasing cyber threat requires a strong, international response based on international agreements. The status quo is still insufficient. The cabinet wants to (publicly) confront perpetrators of cyber-attacks with their behaviour more often. This requires detection, and then political, and possibly legal, attribution."[46]

Reflecting the current reality of state practice, this strategy sets down technical and political attribution as the prerequisites of legal attribution. If the first two are sufficiently clear, only then can legal responsibility be called for. The majority of the instances of public attribution have so far remained at the technical and political level. As is evident, the Dutch strategy is rather hesitant in addressing legal attribution, and refrains from elaborations which, when interpreted into the terminology of public international law, would disclose *opinio juris* with regard to what is considered to count as "effective control", or whether the effective control test is suitable for attributing cyber operations at all. The strategy argues that:

---

[44] UK, National Cyber Security Centre, News Release, "Reckless campaign of cyber-attacks by Russian military intelligence service exposed", 4 October 2018, available at: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed
[45] See eg: UK 2016, supra note 38, p ; The Netherlands, National Cyber Security Agenda, supra note 36.
[46] The Netherlands, National Defence Cyber Strategy, December 2018, p 7, available at: https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018

> "A state actor who is (publicly) held accountable for his actions will make a different assessment than an attacker who can operate in complete anonymity. The Netherlands thereby contributes to combating impunity in the digital domain."

Attribution is therefore seen more as a naming-and-shaming tool of deterrence, rather than the basis of state responsibility in a public international law sense. Likewise, the US avoids legal language in its otherwise open approach to attribution, stating that it will

> "…routinely work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or its partners."[47]

Phrased differently, the above might imply that the US supports the use of (collective) countermeasures on the presumption that an operation can be reasonably attributed to a malicious actor, state-sponsored or not. Further elaboration of what is needed for such attribution is, however, missing. The individual national security strategies say disappointingly little about the legal side of attribution, and when read together may only reveal that legal attribution of cyber incidents is a matter too fragile and momentous about which to speak prematurely.

[47] Supra note 29, p 34.

7. Conclusions

Cyber *opinio juris* is in a formative stage. It is not as rare as it used to be, but it is sometimes contradictory and almost always extremely vague and discreet. By the end of 2018 almost 90 states had adopted a national cyber security strategy. Typically, the process that foreshadows the publication of a national cyber security strategy is not so different from actual legislative drafting: different interest groups are called together, the greatest common denominator is found, numerous compromises are made and in the end only such content is published that has won the approval of the parties involved. Any legally relevant statement made in the pages of a national cyber security strategy, therefore, is a result of careful deliberation and is rarely, if ever, haphazard. Particularly considering that the declarations are meant as realistic goals to be communicated to the international community and pursued in a predetermined period. As such, national cyber security strategies may contain strong evidence of the norms to which a state sees itself as legally bound.

As a result of this comparative reading of strategy documents from Australia, China, France, the UK, the US, the Netherlands and a few other states, some traces of state legal opinion on grey zone issues have been found.

Firstly, sovereignty is always recognised, and more often than not in a way that indicates it being seen as a rule that can be subject to violations. Thereafter, the strategies tend to take the next logical step by recognising the obligations and responsibilities deriving from sovereignty. The relationship between due diligence and state responsibility is, however, rarely examined in close detail. While all unequivocally chastise foreign interference by cyber means, no strategy contains significant traces of whether interferences such as election meddling can be considered an internationally wrongful act, and if so, then how severe an act they are. Interestingly, there is considerable disagreement even among otherwise likeminded nations on the criteria for detecting a cyber use of force or armed attack.

Somewhat unexpectedly, kinetic consequences or the lack thereof are not seen as the ultimate litmus test. Drawing from an almost universal understanding that countermeasures, as opposed to self-defence, are what is needed in tackling (state-sponsored) cyber-attacks on a daily basis, the states representing a more Western liberal cyber policy are suggesting of the possibility for opening the door to collective and anticipatory countermeasures.

Finally, alongside evolving state practice and *opinio juris* expressed through other channels, national cyber security strategies are also opening up and offering legal thinking on attribution. The most notable examples of the tendency are the French Strategic Review of Cyber Defence (2018) and the Dutch National Defence Cyber Strategy (2018).