CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Trends in international law for cyberspace

May 2019

About this paper

This paper is a collaborative view of the NATO CCDCOE Law Branch experts, demarcating the latest trends in international law and envisioning their evolution over the next few years. It is an independent product of the CCDCOE and does not represent the official policy or position of NATO or any of its Sponsoring Nations.

We do not assert this to be a complete catalogue of trends, neither is the list presented in any particular order. Also, while we have made every effort to describe globally relevant legal developments, we acknowledge that the list stems from a Euro-Atlantic geopolitical perspective, and that the division between political developments and trends in law is not always clear-cut.

1. Maturing consensus that international law applies in cyberspace, but continued debate on how it applies

a. It is now generally held that international law[1] applies to cyberspace: this has been confirmed *inter alia* by UN GGE 2013 and 2015 consensus reports;[2] in statements of regional organisations (NATO,[3] EU,[4] OAS SCO, etc.); by (joint) statements of States;[5] and by States in the *Tallinn Manual 2.0* (TM 2.0) State consultation process. However, such a conclusion does not warrant overconfidence, as States like Russia and China have been walking back their commitment even to the broad notion of the applicability of existing international law in cyberspace.

b. The legal debate has shifted to *how* international law applies in cyberspace. This process is neither predetermined nor singular; it evolves through State practice and political statements (individually and collectively via international organisations and fora), and by scholarly legal discussion. Furthermore, it involves a number of different issues of varied specificity.

c. Acceptance of particular legal rules to cyberspace varies. Certain rules are generally accepted, such as prohibition of intervention (Rules 66–67 of TM 2.0) and the right to self-defence (Rules 71–75 of TM 2.0). Others, in particular the exercise of (territorial) sovereignty (Rules 1–5 of TM 2.0)[6] and due diligence (Rules 6–7 of TM 2.0) in cyberspace, have received mixed reactions on their scope and content, even from countries which do not question the relevance of existing international law to cyberspace.[7]

d. States are likewise divided on whether existing treaty and customary law is adequate (as maintained by the West) or whether new treaty instruments are needed; the SCO[8] States are the most prominent proponents of the latter.[9]

e. The conceptual difference in approaches 'cybersecurity vs. information security' also persists, as does the practice of applying national sovereignty over 'information space' (China and Russia as prime examples).

CCDCOE resources

- Michael N. Schmitt (Ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017)
- Wolff Heintschel von Heinegg, International Law and International Information Security: A Response to Krutskikh and Streltsov Tallinn Paper No. 9 (2015)
- Katharina Ziolkowski (Ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (2013)

2. State responses to malicious cyber activities

a. **States demonstrate greater preparedness to attribute State-sponsored malicious cyber activities to originators**;[10] this applies to both capability and political willingness. Along with evolving practice, legal standards for attribution are becoming clearer, with attribution understood as a political decision supported by established (by technical and intelligence means) facts in aggregate, in contrast to judicial evidentiary standards. While there is no legal requirement to publish evidence to support attribution, States are doing so, with growing levels of detail.[11] See also Rules 15–17 of TM 2.0.

b. **Seeking legal options to impose costs on malicious State actors.** Given that State-sponsored cyber operations typically remain below the threshold of armed attack, States are seeking to hold malicious cyber-actors to account by denouncing their actions and imposing costs on them. Responses to malicious cyber activity have so far been limited to retorsions, i.e. legally non-controversial measures (sanctions,[12] indictments,[13] and publicity[14]). Although in principle legally available, there are yet no (communicated) uses of countermeasures[15] within the meaning of the term under the law of State responsibility (Rules 20–25 of TM 2.0).

c. **Evolving coordination of responses to cyber operations**, reflecting the perception that malicious cyber activities are a violation of rules-based international order.[16] The availability of collective responses depends on their nature. While collective retorsions and collective defence are permissible, countermeasures are the right of the injured State and the plea of necessity is available to a State when there is grave and imminent peril to its essential interests. The issue of the availability of collective countermeasures is controversial and will likely remain so, given the interest by States in multinational responses. Coordination of legitimate responses is legally uncontroversial, however, and coordinated use of responses by regional allies (EU,[17] NATO) is emerging.

d. **Choice of means of response to a cyber armed attack.** With regard to *jus ad bellum* it has been widely recognised that a cyber operation of a certain gravity and consequence may constitute an armed attack triggering the right to self-defence. In such a situation, States are free to choose appropriate means to respond, within the limits of international law, and they are not limited to cyber means only.

CCDCOE resources

- Responsive Cyber Defence studies (2015 & 2016) (available for NATO and NATO CCDCOE member nations)
- Matthijs Veenendaal, Kadri Kaska, Pascal Brangetto, 'Is NATO Ready to Cross the Rubicon on Cyber Defence? Cyber Policy Brief' (2016)
- Jeffrey Carr 'Responsible Attribution: A Prerequisite for Accountability' Tallinn Paper No. 6 (2014)

3. Promoting norms of responsible behaviour in cyberspace

a. **There is now a host of initiatives to promote non-binding international norms of responsible conduct,** driven by States, international and regional organisations, and the private sector, with a view to maintaining security and stability in cyberspace. With their varied scope, purpose and origin, the content of proposals fluctuates, ranging from elementary and nonspecific to fragmented and contradictory. All parties seek norms for cyberspace but they have very different ideas as to the desired end state and the means to get there. However, the emergence of propositions for concrete commitments (rather than mere emphasis on the importance of cybersecurity) is evident. We do not yet know whether these initiatives will have a practical impact and, if so, what it will be.

b. **Limited progress in existing international formats.** Following the failure of the UN Group of Governmental Experts (GGE) to produce a consensus report in 2017, the UN General Assembly adopted two new resolutions: one, sponsored by EU countries, US, Canada, Australia, Japan *et al.* and creating a new GGE;[18] the second, sponsored by Russia, China, and Central Asian and African countries, creating an open-ended working group (OEWG)[19] to 'further develop the rules, norms and principles of responsible behaviour of States', introduce changes if necessary, and study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations'.[20]

The OSCE Permanent Council adopted a second set of CBMs[21] in 2016, with limited impact.

c. **State endorsement of voluntary 'norms, rules and principles of responsible State behaviour'**, while stressing their non-binding nature.[22] Additional State-driven formats have arisen, such as the Paris Call for Trust and Security in Cyberspace (2018).[23]

d. **Sharp increase in multistakeholder, bottom-up activism** in proposing international cyber norms. The technology industry in particular is taking a more active stance in reaching out to States (Microsoft proposed the Digital Geneva Convention[24]), but also committing themselves to 'act responsibly, to protect and empower […] users and customers, and thereby to improve the security, stability, and resilience of cyberspace'.[25] Initiatives such as the Cybersecurity Tech Accord[26] and the Charter of Trust for a Secure Digital World[27] have gained wider industry support.

CCDCOE resources

- Anna-Maria Osula and Henry Rõigas (Eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives* (2016)
- Tomáš Minárik, 'OSCE Expands Its List of Confidence-Building Measures for Cyberspace: Common Ground on Critical Infrastructure Protection'. INCYDER (2016)
- Michael N. Schmitt & Liis Vihul The Nature of International Law Cyber Norms Tallinn Paper No. 5 (2014)

4. Use of cyber activities in military operations

a. **Legal questions around the operationalisation of cyber activities.** Cyber activities have become a regular part of military operations, requiring practical operational answers regarding the lawful conduct of specific activities. This is true for armed conflict and for peacetime military operations (e.g. peacekeeping). It raises legal issues about conducting cyber intelligence operations, the limits of State sovereignty, the threshold of armed attack triggering the right of self-defence, and how to apply the rules of international humanitarian law. This also includes the issues of defining legal mandates for cyber commands, definition of cyber operations doctrine, and adjusting and developing the rules of engagement (ROEs) regarding cyber activities.

b. **Offensive cyber operations** are a politically sensitive and often controversial issue; however, under international law the same rules and principles apply to defensive and offensive capabilities and operations. NATO has chosen to address this with the political decision on integration of sovereign cyber effects into NATO operations, which has also raised a range of legal issues.

c. **Acceptance of international humanitarian law (IHL).** The *Tallinn Manuals 1.0* and *2.0* restatements of existing international law norms on international humanitarian law (IHL) have been quite well accepted by States. There remains a group of States, however, who maintain the position that applying IHL to cyber operations would implicitly militarise cyberspace.

CCDCOE resources

- Tallinn Manual 2.0 (2017)
- ROE studies (2016 & 2017) (available for NATO and NATO CCDCOE member nations)
- INCYDER: NATO articles (2014-2018)

5. Law enforcement & national security

a. **Harmonisation of criminal substantive law.** The Council of Europe (CoE) Convention on Cybercrime[28] now has 62 States parties; a further 10 States have signed it or been invited to accede. The practice of States applying a 'margin of appreciation' when transposing treaty norms into national legislation is decreasing but still present.

b. **Procedural law and digital evidence**: expansion of extraterritorial jurisdiction. Increasing 'digitalisation' of crime pushes the need to access digital evidence for criminal investigations across borders, including in the cloud. Legal developments in Europe[29] and the USA[30] indicate expanding extraterritorial jurisdiction over data. The proposed 2nd Additional Protocol to the CoE Convention on Cybercrime[31] seeks to find a balance between legitimate law enforcement interests, individual privacy rights and foreign sovereignty.

These developments contrast with emerging regional and national legislation protecting privacy, which can challenge the investigation of cyber crimes, and with national legislation mandating data localisation in their countries for the purposes of domestic criminal proceedings, essential service security, critical infrastructure protection, or national security.[32]

c. **Mass surveillance**. After two landmark judgments of the European Court of Justice[33] ruled general data retention unlawful, EU Member States are looking for options that would meet the legal requirements ('specific and limited' retention)[34] set out by the court.[35] In contrast, the latest rulings of the ECtHR on mass surveillance seem to be more open to bulk interception.[36]

d. **Encryption backdoors.** The increasing prevalence of encryption technologies contains a dilemma: it strengthens cybersecurity but poses a challenge to law enforcement authorities to investigate serious

crime. Some countries (the 'Five Eyes';[37] France and Germany[38]) have supported legislation to compel technology and communications companies to decrypt customers' data,[39] while others (the Netherlands, Estonia)[40] have voiced support for strong encryption. There are calls for EU level regulation on the issue of encryption backdoors,[41] while workable technical options are yet lacking.[42]

e. **Cyber espionage.** Peacetime cyber espionage by States does not *per se* violate international law, but the manner and method might (Rule 32 of TM 2.0). National law restrictions or bilateral arrangements may apply (e.g. the US-China agreement to restrain economic espionage[43]). The G20 has issued a political statement asserting that no country should conduct or support ICT-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors.[44] The statement lacks legal force, however, and its immediate political effect does not go beyond the G20 countries.[45]

CCDCOE resources

- Anna-Maria Osula, 'The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives', MUJLT Vol 11, No 1 (2017)
- Tomáš Minárik 'Council of Europe Ponders a New Treaty on Cloud Evidence', INCYDER (2017)
- Anna-Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data', MUJLT Vol 9, No 1 (2015)
- Anna-Maria Osula, 'Accessing Extraterritorially Located Data: Options for States' (2015)
- Ann Väljataga, 'ECtHR: When not backed by strong safeguards, mass surveillance violates privacy', INCYDER (2018)

6. Industry regulation

a. **The growing volume of regulation on industry and service providers** marks a shift of focus from an end-user (retail) approach to cybersecurity and placing emphasis on design security and resilience on the provider (wholesale) side. In Europe, there have been several recent developments to illustrate this: regulation introduced for essential services and digital service providers (the EU NIS directive of 2016);[46] personal data protection requirements for data processors (GDPR);[47] and creating a legal framework for cybersecurity certification of products, services and processes distributed in the EU (Cybersecurity Act).[48]

b. **Approaches to product security and supply regulation vary**: with Europe tending towards legislation (Cybersecurity Act), the US prefers voluntary industry standards (US National Cyber Strategy of 2018).[49] However, on both continents, cybersecurity concerns have induced a practice of restricting industry providers from autocratic states free access to the market.[50]

c. **A retreat from former liberal approaches to content regulation** is also present in Western societies, as indicated by regulation introduced in issues such as net neutrality,[51] content provision[52] and the EU Copyright Directive proposal.[53] The ECHR judgment in the *Delfi* case solidifies platform providers' responsibility over content, as opposed to the previously prevailing 'mere conduit' approach.[54] As a result of hybrid campaigns against democratic elections, also States that have traditionally emphasised the regulation and protection of code as opposed to content have begun to pay heightened attention to maintaining control over their information space.

CCDCOE resources

- Ann Väljataga, 'A balancing act: The EU proposes a new framework for cybersecurity certification', INCYDER (2018)
- Kadri Kaska, Henrik Beckvard, Tomáš Minárik, 'Huawei, 5G, and China as a Security Threat' (2019)

7. Projected developments in a 5-year perspective

a. **We expect further clarity regarding how international law applies** to be driven primarily by State practice, as a new global treaty is nowhere in sight. However, the evolution of State practice into a binding customary norm is a process long beyond the 5-year horizon of this paper, and consensus over *how* international law applies is a far greater challenge than acceptance for the applicability of international law in principle (remembering that even the latter is contested by states like China and Russia).

Since a global treaty is unlikely, there is potential for multilateral and regional instruments between States to emerge, meaning that the significance of international organisations in the emergence and development of international law is likely to increase.

b. **There will be continued polarisation over the scope and focus of State control over cyberspace**, i.e. cybersecurity vs. information security.

Russia, China *et al*. continue to consider 'information space' as a matter of exercising control over content and use, whereas Western democracies focus on technical security and the free exercise of fundamental rights online in the same way as offline. The challenge posed by a growing number of State and State-sponsored information operations and concerns over election security will not change the conceptual understandings.

c. **We expect an evolution in State responses to malicious cyber activity.** The current restraint is likely to change as States are seeking more effective deterrence against malicious cyber activities; e.g. the US Department of Defense Cyber Strategy[55] concept of 'defending forward' to disrupt or halt malicious cyber activity at its source is potentially a step in that direction, although any operations communicated so far can be characterised as espionage.[56]

d. **Discussions at both national and international levels will continue on how sovereignty applies in cyberspace** (as a principle or a norm). The UK has instigated a lively debate among legal advisers in various roles by officially stating its lack of persuasion 'that we can currently extrapolate from that general principle [of State sovereignty] a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.'[57] The UK Government's position is therefore that there is no such rule as a matter of current international law.

e. **A more active regulatory approach will inevitably result in a degree of legal 'Westphalianisation' or fragmentation of the internet**, with varied legal requirements and degrees of State control applied in different regions. However, this does not mean a binary choice between a Californian- vs a Russian/Chinese-style model, but various combinations along specific topics that emerge and evolve organically. The multilateral **model of internet governance** has not been widely accepted, despite much effort from authoritarian regimes, and discussions on how to maintain and further improve the multistakeholder model are shifting to inclusiveness, balance, accountability, and fair process.[58]

f. **The GDPR in particular will affect privacy regulation and industry conduct globally**, with as yet uncertain effects on incident response and combating crime. Alongside privacy requirements, the emerging trend of regulating security and resilience by design is likely to gain more momentum, extending from industry to the (global) service and platform provider level.

g. **The evolution and growing foothold of diverse digital technologies** – cloud computing, the Internet of Things, artificial intelligence (including machine learning) and the expected introduction of quantum computing – pose a dilemma for States and regulators: drive innovation, partner and shape the environment, or react to industry advances? These technological developments will likewise affect military operations. For regulation to be relevant and avoid having adverse socioeconomic and national security impact, the legal discussions need to become more nuanced regarding the nature of and processes involved in evolving technologies. This in turn requires better technological literacy on behalf of the legislator.

References

1 International law arises from international treaties and international custom (customary international law) and is supplemented by State practice and *opinio juris*. The so-called soft law, or political norms, are not binding on States, but they have political relevance and States subscribing to them will generally respect them.

2 '[I]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment' (UN GGE 2013 report A/68/98); 'The Group emphasized the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by States. […] The Group also noted the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction.' (UN GGE 2015 report, A/70/174)

3 'Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace' (NATO Wales Summit Declaration 2014; position reaffirmed in 2016 Warsaw and 2018 Brussels Summit declarations.).

4 'The EU strongly promotes the position that international law, and in particular the UN Charter, applies in cyberspace.' (EU Cybersecurity Strategy 2017).

5 Joint statement made by the PermRep of Canada to the UN on behalf of Australia, Chile, Estonia, Japan, the Netherlands, New Zealand, the Republic of Korea, the United Kingdom, and Canada on Information and Telecommunications in the Context of International Security (2018).

6 Memorandum from JM O'Connor, General Counsel of the Department of Defense, 'International Law Framework for Employing Cyber Capabilities in Military Operations' (19 January 2017), as cited by S Watts & T Richard, 'Baseline Territorial Sovereignty and Cyberspace' (2018) 22 Lewis & Clark L. Rev. 771, 829.

Gary P. Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207, 208.

Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018).

7 '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.' UK Attorney General Jeremy Wright, 'Cyber and International Law in the 21st Century' (May 2018).

8 The Shanghai Cooperation Organisation, founded 2001, is a political, economic and military organisation with China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan as members.

9 The Shanghai Cooperation Organisation 'Yekaterinburg Agreement' on cooperation in the field of international information security (2009).

10 Examples: June 2017 NotPetya and October 2017 BadRabbit malware campaigns attributed to the Russian Federation by the UK, Australia, and New Zealand (February and October 2018); spring 2018 spearphishing campaign against OPCW employees and systems jointly attributed by the Netherlands and UK to the Russian Federation (October 2018); May 2017 WannaCry attributed to North Korea by the UK and US (December 2017); US attribution of 2016 presidential election interference to the Russian Federation (January 2017).

See also https://www.wired.com/story/white-house-russia-notpetya-attribution/.

11 Dutch MOD statement of 4 Oct 2018: the minister's remarks; Dutch MOD presentation.

12 Russel Brandom, US announces new sanctions against Russian trolls and hackers, The Verge, 15 Mar 2018.

13 US Department of Justice press release regarding the indictment of Russian GRU officers (Oct 2018).

14 For example, the Netherlands foiled a cyber operation by the Russian military intelligence (GRU) against the Organisation for the Prohibition of Chemical Weapons (OPCW) in 2018 and publicly exposed the details of the operation in October 2018.

15 Article 22 of Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001). Countermeasures are (otherwise unlawful) actions taken by a State in response to a breach by another State to induce the latter to comply with its obligations.

16 Joint statement by the UK and Dutch prime ministers on 4 October 2018.

17 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 7 June 2017, 9916/17.

18 'Advancing responsible State behaviour in cyberspace in the context of international security', A/C.1/73/L.37.

19 'Developments in the field of information and telecommunications in the context of international security', A/C.1/73/L.27/Rev.1.

20 Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', Council on Foreign Relations (November 2018).

21 OSCE 2016 set of CBMs, Decision No 1202.

22 Joint Statement by Australia, Canada, Chile, Estonia, Japan, the Netherlands, New Zealand, the Republic of Korea and the UK on Information and Telecommunications in the Context of International Security (2018); 'As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts; it also encourages the development and implementation of regional confidence building measures, both in the Organisation for Security and Co-operation in Europe and other regions.' (EU Cybersecurity Strategy 2017); ASEAN-US Leaders Statement on Cybersecurity Cooperation (2018).

23 Paris Call of 12 November 2018 for Trust and Security in Cyberspace.

24 Microsoft proposal for a Digital Geneva Convention.

25 See the Cybersecurity Tech Accord.

26 Cybersecurity Tech Accord, with 79 industry signatories as of January 2019.

27 Charter of Trust for a Secure Digital World, with 12 industry signatories as of January 2019.

28 Council of Europe Convention of Cybercrime website.

29 European Commission regulatory package proposal on E-evidence (April 2018).

30 US CLOUD Act (part of the Consolidated Appropriations Act, 2018, H.R. 1625).

31 Council of Europe website concerning the drafting process of the draft Second Additional Protocol.

32 ESOMAR summary and analysis of the New Russian Data Localisation Law (2015).

33 Joined Cases C203/15 and C698/15 *Tele2 Sverige AB and Watson*; Joined Cases C-293/12 and C-594/12 Digital Rights Ireland; European Digital Rights, 'EU Member States fight to retain data retention in place despite CJEU rulings' (May 2018).

34 Paras 108-111 of the CJEU Tele2 judgment.

35 European Court of Human Rights factsheet on Court judgments in mass surveillance cases raised to the Court.

36 European Court of Human Rights judgment in the Big Brother Watch vs UK case (September 2018).

37 Australia's 'anti-encryption' law (December 2018).

38 German and French joint letter by Ministers of the Interior (February 2017).

39 Brian Barret, The Apple-FBI Battle is Over, but the New Crypto Wars have Just Begun, Wired (March 2016).

40 The Netherlands' cabinet position on encryption (2016); Estonian Information System Authority position in Estonian Annual Cyber Security Assessment 2018 (p 38-40). Both view strong encryption as fundamental to the functioning of the digital society and national digital ecosystem, not merely a security vs privacy dilemma.

41 Iain Thomson, 'Germany, France lobby hard for terror-busting encryption backdoors – Europe seems to agree', The Register (February 2017).

42 'Shining a Light on the Encryption Debate: a Canadian Field Guide'. Joint Research Publication, The Citizen Lab and the Canadian Internet Policy & Public Interest Clinic, May 2018.

43 Mikk Raud, China and Cyber: Attitudes, Strategies, Organisation. NATO CCDCOE, 2016.

44 G20 Leaders' Communiqué (November 2015 Antalya Summit).

45 Daniel Paltiel, 'G20 Communiqué Agrees on Language to Not Conduct Cyber Economic Espionage', CSIS (2015)

46 Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

47 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

48 Commission proposal for the "Cybersecurity Act"; European Commission press release regarding agreement reached among the EU Parliament, Council and Commission (December 2018).

49 National Cyber Strategy of the United States of America (2018).

50 For example, the USA banned the use of Kaspersky products in government agencies in 2017. Between 2018-2019, a number of countries (USA, Japan, Australia, Czechia) have restricted Chinese technologies (Huawei and ZTE in particular) from government procurements and 5G communications networks, citing threats to national security.

51 BBC News, 'US officially repeals net neutrality rules' (June 2018).

52 Human Rights Watch critique of the German Social Media Law (February 2018).

53 Proposal for a Directive on copyright in the Digital Single Market (COM/2016/0593 final); amendments adopted by the European Parliament.

54 *Delfi AS v. Estonia* (2015) ECtHR 64669/09.

55 Summary of the US DoD Cyber Strategy (2018).

56 Eric Jensen, 'Countering Russian Election Hacks'. JustSecurity (November 2018).

57 UK Attorney General Jeremy Wright, 'Cyber and International Law in the 21st Century' (May 2018).

58 Jeremy Malcolm, 'Is Multi-Stakeholder Internet Governance Dying?' Electronic Frontier Foundation (2017).

For further information see the resources on the CCDCOE homepage Research section:

The Strategy and Governance resource comprises a regularly updated comprehensive collection of national cyber security strategies and relevant legal acts, as well as reports outlining the national cybersecurity governance structures of selected countries.

INCYDER is a research tool offering easy access to the most relevant legal and policy documents related to cyber security adopted by international organisations. It also features articles authored by NATO CCDCOE researchers analysing the impact of these documents and keeps up-to-date organisations' profiles in cyber security.

The International Cyber Law: Interactive Toolkit is a forthcoming dynamic web-based resource for legal professionals who work with matters at the intersection of international law and cyber operations. At its heart, the Toolkit consists of 13 (and counting) hypothetical scenarios, each of which contains a description of cyber incidents inspired by real-world examples accompanied by detailed legal analysis. The Toolkit may also be explored by looking for legal concepts you are interested in or by reading about individual real-world examples that had inspired the scenarios. The individual scenarios and the Toolkit as such have been reviewed by a team of over 20 peer reviewers.

The project is supported through the UK ESRC IAA Project Co-Creation scheme. Partner institutions include the University of Exeter, United Kingdom, NATO CCDCOE in Tallinn, Estonia, and the Czech National Cyber and Information Security Agency (NCISA) in Brno, Czechia. The project team is composed of Dr Kubo Mačák (Exeter University), Tomáš Minárik (CCDCOE) and Taťána Jančárková (NCISA). The Toolkit will be launched at CyCon 2019 and it is expected to be continuously updated and expanded.