EasyChair Preprint

№ 5111

Cybersecurity Due Diligence

Joanna Kulesza

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

March 9, 2021

Cybersecurity due diligence

Joanna Kulesza, University of Lodz

IRIS 2021 submission

On Dec. 16th, 2020 the European Commission's Vice-President Josep Borrell presented the European Cybersecurity Strategy.[1] The 2020 pandemic has exemplified how important network resilience and international cooperation are for Europe and the world. The European approach to cybersecurity, as designated by the 2016 EU Directive on security of network and information systems (NIS Directive) relies on risk assessment and due care. It was the crucial document that included network operators and DNS providers into the category of European critical infrastructure operators and service providers. This significantly added EU's reliance on business participation in ensuring a safe online environment for business and pleasure. The EU Cybersecurity Strategy follows up on this policy line, making cybersecurity one more area of international law and policy that relies on a good-business practice based standard of due diligence, required from critical infrastructures operators. This paper seeks to put this latest development of cybersecurity in the context of contemporary international law, drawing analogies with the law of state responsibility and international liability, as developed by international environmental law, law of treaties or diplomatic relations.

Introduction

In Borell's own words, the 2020 Cybersecurity Strategy aims to meet four fundamental goals:

1) EU aims to advance the UN Programme of Action targeting responsible state behaviour in cyberspace;

2) EU "strengthens our ability to prevent, deter and respond to malicious behaviour in cyberspace";

3) It will "work to ensure cyber defence cooperation", as well as

4) increase work with third countries, regional and international organisations, civil society and the private sector.

All of these goals are direct results of the application of international law in cyberspace and follow up on extensive international law scholarship and practice. International law scholarship can therefore allow for a speedy implementation of these aspirational goals in Europe and beyond making it the poster child for cybersecurity resilience. This goal might be of particular importance in time of global struggles over online trust and security, including but not limited to the discussion around 5G and supply chain security. Once European sets an example for how cybersecurity is done across boarders " we will provide more practical support to our partners, where necessary, to increase their cyber resilience" as Borell puts it.[2]

His 2020 statement follows up on the operational framework introduced in the 2016 EU Directive on security of network and information systems (NIS Directive). The NIS Directive

[1] Cybersecurity Strategy: Remarks by the High Representative/Vice-President Josep Borrell at the joint press conference with Vice-President Margaritis Schinas and Commissioner Thierry Breton, Brussels, 16/12/2020 - 14:54, UNIQUE ID: 201216_9 https://eeas.europa.eu/headquarters/headquarters-homepage/90700/cybersecurity-strategy-remarks-high-representativevice-president-josep-borrell-joint-press_en

[2] Idem.

covers “digital Infrastructures”, including Internet Exchange Points (IXPs), the domain name system (DNS) service providers and Top Level Domain (TLD) name registries as well as an open category of “online marketplace” services, “online search engines” and “cloud computing service”, as the well-established category of critical infrastructures. To indicate what challenges lie ahead of states implementing the 2020 Cybersecurity Strategy in the coming years, a brief reference to “critical infrastructure” (CI) must be made. While particular listings of networks and services granted the highest level of protection differ among states and are kept in strict confidence to hinder potential attackers, a rough consensus on what infrastructure needs to be protected first when state security and stability is at stake can easily be traced. Civil defense theories indicate that “critical infrastructure” covers also mass transportation, water and alike. The European Commission refers to critical infrastructure as “an asset or system which is essential for the maintenance of vital societal functions”.[i] It goes into much detail on how to identify critical infrastructure and puts numerous obligations onto its operators, including but not limited to a risk analysis identifying potential threats to those most vulnerable assets.[ii] Also in the US critical infrastructure has been defined by the US Homeland Security Office as “the assets, systems, and networks,” physical or digital, whose “incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”[iii] While no legally binding order applies, protection of critical infrastructure follows the 2013 Presidential Policy Directive 21 (PPD-21) on “Critical Infrastructure Security and Resilience” indicating 16 distinct sectors.[iv] On the international level the OECD’s approach to CI focuses on the threats rather than the targets, with a definition of “critical risks” that covers “threats and hazards” resulting in “the most strategically significant risk,” yet originating from “sudden onset events” such as “earthquakes, industrial accidents, terrorist attacks, pandemics, illicit trade or organized crime.[v] With its broad perception of CI the OECD follows a “‘whole-of-society approach”, requesting state bodies, but also businesses and individuals to engage in all activities targeted at mitigating possible risks. This approach is best fitted to the globalised international economy of the 21st century and a perfect reflection of the online environment discussed further herein – the transnational network of interrelated services is vulnerable to attack at its weakest point, hence they all must be protected with equal diligence. OECD recommends “creating models for public-private partnerships” allowing for exchange of information vital for national security. It emphasizes the role of private actors as those in disposition of most information and often a better infrastructure.[vi] OECD indicates “critical infrastructure networks” as including “energy, transportation, telecommunications and information systems,”[vii] and encourages private parties to ensure a high enough level of preparedness through risk-analysis and sector-specific security standards.[viii] And while non-binding, the OECD Recommendation serves as a superb answer to the contemporary security challenges, by putting the obligations of states and private bodies on equal footing.

State duties and private parties obligations

It is clear that while international law is binding to states, it cannot be enforced directly against private parties. With that the question on how the international community as a whole can effectively enforce international law obligations onto private companies operating within the jurisdiction of states reluctant to introduce appropriate national laws, remains open. But CI protection in general and cyberthreats prevention in particular are just a few new elements in the universal catalogue of known threats to international peace and security that has been developing over centuries. Before cybersecurity, it was nuclear power, oil production and transportation and outer space exploration that triggered a shift in the way the global community looked at international liability and state responsibility. The challenges those areas of activity brought about resulted in a state duty to protect others for transboundary harm – one originated

within state territory or jurisdiction yet affecting foreign territory or subjects. It was exactly this challenge that kept the UN International Law Commission occupied for over 60 years trying to answer the questions of state responsibility and international liability for transboundary harm. This was done primarily by detailing duties of states in implementing standards for private bodies in preventing significant harm to "neighbouring" countries, i.e. all those potentially affected by risk-generating activities performed within state territory, under state jurisdiction or control.[ix] A crucial element of this puzzle has been the issue of due diligence – a flexible international standard, indicating what actions states need to perform to ensure private sector compliance and prevent significant transboundary harm. The ILC work indicates that when performing any obligation of conduct – one that requires them to perform in a certain way as opposed to achieving a particular result – states need to act with due diligence. This flexible standard covers nine elements:

1. Good faith on behalf of the state in meeting its international obligations, including those obligations of conduct that introduce the duty to prevent significant transboundary harm.

2. Due diligence is the result of the well-recognized principle of good neighborliness, which necessitates for states to refrain from causing harm or damage within the territory or in the legally protected interests of others or in common territories.

3. Performance of any due diligence obligation is assessed territorially, i.e. with regard to a given territory and potentially harmful actions initiated or conducted therein.

4. The duty to perform with due diligence is a derivative of the principle of sustainable development. As such it requires a risk assessment for any new procedure or legislation that may bring with it a risk of significant transboundary harm.

5. As confirmed in numerous international law treaties, the due diligence principle is a state obligation to undertake "all necessary measures" expected of a "good government" in a given situation. A state is to perform according to this standard when meeting its international obligation, but the individual measures as well as tools for assessing them are always case-specific. Due diligence always implies however the need for administrative or other formal procedures aimed for authorizing risk-generating activities undertaken within state territory, jurisdiction or control. These procedures need to be enforced in a way that a "good government" would have done. This theoretical model of "good government" reflects a long legal tradition, dating back to Roman law with the theoretical model of a "good family man" and has been present in civil law until this day. When trying to identify how a "good government" would have acted in a given case the court is to consider the performance of state bodies in own affairs, state's economic condition and the performance of countries in the region or in a particular economic sector, among other case-specific factors. Courts would often rely on the assessment of experts in a given field when attempting to identify what actions should have been taken by the government to prevent a given harmful occurrence, as discussed below.

6. Assessing the due diligence standard relies on technical expertise and reference to the state of art in a given area of practice. With that in mind, individual efforts are usually set against its financial and technological capabilities of the acting state. Taken precautions must reflect the current state of technical knowledge in a given area, yet nothing that is clearly outside the financial or organizational capability of the state or

ones in its region can be considered as required. The efforts taken by the acting state are set against similar measures taken by other states in the region in given circumstances. Also the size of potential damage is to be considered – the more severe the pending harm the more intensive state efforts are expected.

7. Due diligence covers also the duty to exchange information with others: states, private parties and international organizations. Information on potential risks and measures taken to mitigate them is to be shared, with exception for information considered crucial to state security or its economic interests. This thin line between information necessary for others to effectively protect themselves from pending grave damage and those considered crucial to state economy is always done by the risk generating state and remains among the most disputable issues in contemporary globalized economy. There are no universal standards allowing to draw the line between what needs to be shared for the purposes of global security and what is allowed to be kept secret even when global security is at stake.

8. States are required to refrain from discrimination when it comes the treatment of both: victims and operators, disregarding their country of origin, the role they played in the potentially harmful activity or their economic status. Any preference for e.g. national operators when compared with the standard required from foreign ones would be considered a violation of the due diligence standard.

9. Due diligence obligation is a continuous one, requiring states to upkeep their efforts in assessing and preventing international law violations resulting in potential harm to others. A single risk assessment performed before or at the start of a risky activity, a single authorization procedure or one done occasionally are not considered diligent. Potentially harmful activities need to be continuously monitored for potentially harmful incidents and operators' procedures must be updated according to the latest technological expertise and information received from other parties.

International legal scholarship and practice indicate that due diligence is not to be considered with regard to the so-called *post facto* prevention, i.e. measures taken after actual damage arises. Moreover, there is no consensus on vicarious responsibility of states or their risk liability for the actions of individuals, unless necessary stipulations are put into an international treaty binding upon the acting state.

The Borrell Declaration – Europe's statement on leading the way

The Cybersecurity Strategy follows up on on the April statement from Borrell on malicious cyber activities exploiting the coronavirus pandemic, proposing a way forward to ensure cyber security in times of coronavirus.[x] Pursuing EU's long strategy on a defensive cybersecurity policy, the High Representative refrained from statements encouraging states to take active measures against attackers. Instead, the EU:

"call[ed] upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law and the 2010, 2013 and 2015 consensus reports of the United Nations Groups of Governmental Experts (UNGGEs) in the field of Information and Telecommunications in the Context of International Security."

This declaration was important for two reasons. First and foremost, is sees an officer of the European Union in their official capacity refer to due diligence as the expected mode of conduct in national and international cybersecurity policy. Regardless of earlier controversies among diplomats, academics and state officials, the EU herewith confirmed that the international law duty of prevention is applicable to cyberattacks. Secondly, it builds upon the European experience of shared sovereignty to pave the way forward for the international community on how to best attain both: individual freedom and collective safety. Let us unpack this loaded, international law paradigm that is due diligence and see how EU's experience with applying it to cybersecurity can be useful beyond the 27 member states.

Offensive vs. defensive cybersecurity

Cyberattacks are among most controversial categories of international relations. While legal scholarship has gone to great lengths to define them,[xi] the decision on naming and shaming the perpetrator of any malicious cyberactivity rests exclusively with each state.[xii] This is the case due to, primarily, the concept of sovereignty and the consequential right to individual self-defense: each country enjoys the right to defend itself against an armed attack and whether a cyberattack can be recognized as one remains disputed among academics and practitioners.[xiii] This ambiguity leads to freedom: states hold it as their sovereign right to decide on individual basis whether they have been subjected to an armed attack and whether they are entitled to proportionately yet effectively defend themselves in a given situation. This approach, although officially supported and adopted by some states, most significantly the United States with their 2018 "Defend Forward" strategy,[xiv] raises concerns similar to those behind "preemptive" (or "preventive") self-defense.[xv] Preemptive self-defense, although recognized by the majority of international legal scholarship, still provokes discussions. The United Nations and the Charter it was built on rely upon the universal prohibition of the use of force. Article 51 UNC, allowing for self-defense in face of a direct armed attack, introduces one of the very few exceptions and as such should be read and applied restrictively. Any doubt as to the nature of an alleged attack should therefore be understood as a prohibition to respond with violence – only should an attack undoubtedly be the use of force, can self-defense be deployed. As per both: legal scholarship and state notifications, all international cyberattacks noted thus far have failed to meet the armed attack threshold, making the discussion on armed self-defense irrelevant. This however has not stopped some states from reading cyberattacks as an invitation to preventive or preemptive self-defense, rendering the restrictive concept behind the UNC largely futile.

Granted an armed counter-attack would not be valid in light of international law, what is left is defensive capability. This is the approach that the European Union has consistently adopted, be it with the Cybersecurity Strategy, the NIS Directive and the following national laws and strategies or the GDPR, which all focused on creating a comprehensive security culture around critical data and resources.

The European Culture of Cyber-resilience

The EU Security Union Strategy for 2020 to 2025 follows the European Agenda on Security (2015-2020) with the review of the Network and Information Systems Directive, the development of the a Joint Cyber Unit and the adoption of a new Cybersecurity Strategy. All of these create a comprehensive roadmap for non-European parties who would like to build upon EU's success story. The European culture of cybermedicine is built upon six pillars: 1) certification based on legally binding standards 2) investment in research, networking and capacity building 3) coherent cybersecurity policy guidance for states and non-state actors 4) building skills and awareness 5) communication and coherence among cybersecurity

communities 6) building synergies with other areas of cyber policy, including cybercrime, cyber diplomacy, defense and foreign relations.[xvi]

All these activities have led the EU to hold at its disposal a comprehensive set of tools enhancing its cyberresilience. While some EU countries have openly declared their capability and willingness to engage in active cyberdefence, this is by far not the official EU policy – quite to the contrary. The comprehensive set of policy tools named above provides the EU with a board landscape of tools readily available across all 27 states. A particularly interesting tool in this set of policy measures is that of certification: is assumes that all operators of services which have been listed as crucial to the secure operation of the European open market must ensure that the infrastructures under their control live up to a certain technical standard of care. ENISA ('European Union Agency for Network and Information Security') - the EU cybersecurity agency – offers guidance and certification services for critical infrastructure operators, particularly when it comes to cybersecurity. As previously argued such practice falls directly into the international law principle of due diligence.[xvii] International law offers this flexible, standard based norm to meet the challenges posed by rapidly developing technological landscape. Whether in environmental law, space exploration or cybersecurity, due diligence necessitates reasonable efforts by "good governments" as per "objective standards relating to a given conduct".[xviii] ENISA guidance and certification do exactly that: set an objective cybersecurity standard related to particular circumstances, respectively: cybersecurity threats. These general cybersecurity standards have been promptly and respectively amended for the new, challenging circumstanced that were brought by the pandemic, with ENISA publishing guidance also for protecting internet infrastructures and services from COVID-19 specific threats.[xix]

Next Steps

The due diligence principle requires operators of risk-generating activities to be legally obliged to meet certain cybersecurity obligations, ones followed by sanctions if not met. This is a model followed by e.g. the NIS Directive, obliging states to introduce a due diligence obligation for all critical infrastructure operators, as reflected in international best practices, measured with the universal standard of "best available technologies". This standard remains a flexible one, relying on the ever changing technological developments and technical experts assessment. Yet any operator falling short of meeting this flexible standard is likely to face civil liability according to general principles of law that require those who case others' harm, be it through their actions or omissions, to cover for the losses. This principle resulted in obligatory liability insurance for oil transportation or nuclear power production. Good business practice resulted in a comprehensive insurance scheme, developing alongside the blooming yet risk-generating business, in the form of liability funds fueled by private operators. With the scale of possible damage resulting from a compromised information system in such areas of public life as transportation or water supplying, civil liability is likely to exceed the financial capabilities of individual operators. With that in mind, introducing obligatory insurance for critical infrastructure operators, including those offering Internet-based services and creating a joint liability fund, fueled by private operators, seems a useful example to follow. Europe has already paved a way for such a model with its NIS Directive and its implementation through ENISA and national cybersecurity policies. Some states, e.g. France, have already explored that path and introduced voluntary ISP liability insurance, although it was originally introduce to curtail liability for copyright violations. The risk-assessment mechanisms and good practices of insurance companies accompanying the introduction of such services may serve as a blueprint for the international standard for cybersecurity due diligence.

A cybersecurity due diligence standard is EU's response to the fast paced changes the Internet landscape has been subjected to. Since it is impossible to effectively attribute state responsibility for online disruptions for both technical and legal reasons, due diligence offers a useful answer to the question on who should cover possible damages inflicted online. When one considers due diligence as the answer, it is no longer necessary to engage into the difficult debate on state-actors, state-sponsored attacks and private parties liability. It is no longer necessary to prove who is behind a given attack or a malfunction, where telling the two apart can at times also prove difficult. It is much easier to identify those, who should have taken all necessary measures to prevent the attack from causing significant harm. This is not to imply that all harm caused through online activates needs to be successfully prevented – as discussed in detail herein above and elsewhere, the due diligence standard implies a best efforts obligation. As in the case of e.g. a medical procedure what is required is to use all one's professional knowledge to prevent damage. Should all such knowledge and capability be deployed, the obligation is met and no liability can be enforced, even if the damage could not be successfully prevented. The extensive work of the ILC and the rich body of international law should be viewed as a valuable resource for preventing significant transboundary harm in yet another area of international relations – that of Internet governance and cybersecurity.

---

[i] European Commission, Critical Infrastructure, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm; see also: European Commission, Communication from the Commission on a European Programme for Critical Infrastructure Protection, 2006, final and documents mentioned therein, in particular the: The Commission Staff Working Document on the Review of the European Programme For Critical Infrastructure Protection (EPCIP), 2012 and the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82 (further herein: ECIs Directive). See Article 2, ECIs Directive, which describes "critical infrastructure" as an "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"

[ii] Articles 3 – 5 ECIs Directive. Effectively the European critical infrastructures include:
"1) energy installations and networks; 2) communications and information technology; 3) finance; 4) health care; 5) food; 6) water (dams, storage, treatment and networks); 7) transport (airports, ports, intermodal facilities, railway and mass transit networks and traffic control systems); 8) production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials); 9) government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)."
See: European Commission, Critical infrastructure protection,
http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm.

[iii] Office of Homeland Security, What Is Critical Infrastructure?, 2013, http://www.dhs.gov/what-critical-infrastructure.

[iv] Those critical sectors include: the chemical sector, commercial facilities, communications, "critical manufacturing", dams, defence industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems as well as water and wastewater systems. See: The White House, Office of the Press Secretary, February 12, 2013, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Those are almost identical as those defined by the ECIs Directive, see supra 10 above.

[v] The 2014 Recommendation of the Council on the Governance of Critical Risks (further herein: OECD GCR). Earlier documents include: the 2008 Recommendation on the Protection of Critical Information Infrastructures, the 1988 Recommendation of the Council concerning Chemical Accident Prevention, Preparedness and Response and the 2002 Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

[vi] OECD GCR, Para. III 5 i)

[vii] OECD GCR Para IV.2. i).
[viii] OECD GCR Para IV.3.
[ix] For a detailed discussion on these developments see: J. Kulesza, Due diligence in international law, BRILL 2016.
[x] Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic, 30 April 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/
[xi] Just to mention the comprehensive analysis by Marco Roscini, Cyber Operations and the Use of Force in International Law, UOP 2014 or François Delerue, Cyber Operations and International Law, CUP 2020.
[xii] Idem.
[xiii] Idem.
[xiv] United States Department Of Defense Cyber Strategy, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF which on p. 3 reads: "The Department must take action in cyberspace during day-to -day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests".
[xv] R. Coate, The UN and the Legal Status of Preemptive and Preventive War. In: Glad B., Dolan C.J. (eds) Striking First. Palgrave Macmillan, New York 2004.
[xvi] For a detailed review of all these policy areas, please visit: European Commission, "Shaping Europe's digital future", available at https://ec.europa.eu/digital-single-market/en/cyber-security#Legislation%20and%20certification .
[xvii] F. Delerue, J. Kulesza, P. Pawlak, The Application Of International Law In Cyberspace: Is There a European Way?, April 2019, https://eucyberdirect.eu/wp-content/uploads/2019/05/delerue_kulesza_pawlak-international-law-in-cyberspace-european-way-april-2019-eucyberdirect_.pdf
[xviii] UN Doc. A/CN.4/487 at 23, referencing the work of the Institute of International Law.
[xix] Most notably: ENISA, Cybersecurity in the healthcare sector during COVID-19 pandemic, May 11, 2020 , available at: https://www.enisa.europa.eu/topics/wfh-covid19?tab=articles .