CURRENT ISSUES IN EUROPEAN CYBERSECURITY THE NIS DIRECTIVE, DUE DILIGENCE AND INTERNATIONAL LAW

Joanna Kulesza, PhD

University of Lodz, Poland
E-Mail-Adresse: joannakulesza@gmail.com

The 2016 EU Directive on security of network and information systems (NIS Directive) is arguably the most significant attempt at increasing cybersecurity and network resiliency in Europe. It includes Internet based services and their operators into the well established category of critical infrastructure (CI). This implies an increased reliance on business participation. Numerous categories of Internet based services will need to raise the level of security they provide for their infrastructure and software. They will also be required to share information on threats and best practices in preventing and combating cyberthreats with their peers and states agencies. The NIS Directive makes therefore 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 has thus far been the case for e.g. power plant operators, water suppliers or banking services. 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

The 2016 EU Directive on security of network and information systems (NIS Directive) 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 NIS Directive 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 defence 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".[1] It goes into much detail on how to identify critical infrastructure and puts numerous obligations onto its operators, including but not

[1] 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"

limited to a risk analysis identifying potential threats to those most vulnerable assets.[2] 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."[3] 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.[4] 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.[5] 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.[6] OECD indicates "critical infrastructure networks" as including "energy, transportation, telecommunications and information systems,"[7] and encourages private parties to ensure a high enough level of preparedness through risk-analysis and sector-specific security standards.[8] 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 transporta-

2 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.

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

4 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.

5 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.

6 OECD GCR, Para. III 5 i)

7 OECD GCR Para IV.2. i).

8 OECD GCR Para IV.3.

tion 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.[9] 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

[9] For a detailed discussion on these developments see: J. Kulesza, Due diligence in international law, BRILL 2016.

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.

ISP due diligence

Among those private parties obliged to undertake particular cybersecurity measures are those providing Internet services, in particular those responsible for Internet connectivity. This broad category referred to as Internet Service Providers (ISPs) is most discussed when cybersecurity is at stake, primarily because they are the obvious actors to be held responsible for any Internet security breaches. This instinctive reaction, although often not justified – because it is the users, private or corporate, who are to blame for intrusions – has significantly changed the legal and technical situation of ISPs in the recent years, with enhanced cybersecurity and cyber resilience legislation and growing expectations targeted at their activities.

For academic purposes, providers offering Internet-related services may be identified as: access providers, caching providers, host providers, and content providers, depending on the kind of service or services they enable, where clearly one entity can play two or more roles simultaneously.[10] While detailing individual obligations of each ISP group would provide material for a separate chapter, it suffices to say that they all are under growing pressure and increasing obligations to introduce appropriate cybersecurity measures. The ongoing discussion covers three crucial points:

[10] For a discussion on the significance of such a categorisation see e.g.: Thomas Hoeren, The European Liability and Responsibility of Providers of Online-Platforms such as 'Second Life', 1 Journal of Information Law and Technology (2009), available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/hoeren. This distinction was reflected in the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce, OJ L 178, 17.7.2000), Articles 12 – 15.

(1) *The potential need for a conclusive rather than an open list of ISPs obliged to introduce particular cybersecurity measures.*

The current trend is for creating open lists of such entities, ones referring to categories of services or operated infrastructures considered critical, rather than a conclusive list of business sectors, services, or service providers. This is due to two factors: the fast changing nature of all Internet-related issues – a conclusive list risks becoming outdated by the time it is completed; and a significant resilience from the ISP community itself, not willing to be subjected to additional, costly security obligations, going beyond what the business itself finds sufficient. Those arguments are well justified: an open list of cybersecurity bound entities leaves much room for speculation on the scope and content of actually required measures and, primarily, their subjects. Practical solutions come rather from national, regional, and international business practices, rather than state legislation that is limited to setting general obligations and non-binding, inconclusive guidelines.[11]

(2) *The question of particular cybersecurity measures to be enacted by ISPs in respective business areas.*

While it remains clear that all ISPs must undertake certain network resiliency and data protection measures, with particular emphasis on users' data and privacy, there remains the challenge of identifying the manner in which information significant for cybersecurity measures ought to be exchanged. Businesses are reluctant to share information about vulnerabilities used by the attackers for conducting cyberattacks against them as well as about methods of identifying such threats or breaches. Sharing the latter might give undesired business advantage to the competition or reveal trade secrets.

(3) *The problem of operational costs brought about by enhanced cybersecurity measures, with ISPs requesting financial support from governments in order to facilitate the growing demand for new cybersecurity tools, procedures, software and hardware.*

So far governments have been reluctant in offering any financial support to ISPs, laying the material burden of cybersecurity measures on the business and, indirectly, on the users. An exemplary list of businesses endowed with particular cybersecurity obligations may be derived from e.g. current EU regulations. An interesting example of such eagerly discussed regulations is the evolution of the recent (2016) EU Directive on Network and Information Security (NIS Directive).[12] It endows "digital services providers" with particular cybersecurity obligations, including but not limited to implementing "a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced". The EU observes, that since "most network and information systems are privately operated, cooperation between the public and private sectors is essential". With that in mind the suggested "security culture" should rely not only on national laws, but also on "voluntary industry practices". As the EU declares: establishing a trustworthy level playing field is also essential to (…) ensure effective cooperation from all Member States". The EU emphasizes, that the "responsibilities in ensuring the security of network and information systems lie, to a great extent, with (…) digital service providers". They are encouraged to "promote a culture of risk management and ensure that the most serious incidents are reported". Referring directly to good business practice as an efficient tool for ensuring security, the EU

[11] For examples of good business practice see the work provided by e.g.: the European Union Agency for Network and Information Security (ENISA), Resilience of Networks and Services and Critical Information Infrastructure Protection unit, homepage available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP. Good business practice is being facilitated through non-binding cybersecurity standards offered also by the International Standardisation Organisation (ISO standards: 27001 and 27002), Information Security Forum (ISF; the regularly updated "Standard of Good Practice") or the Internet Engineering Task Force (IETF; through their Requests for Comments (RFCs) starting with the 1997 RFC 2196). The above named activities and documents are only meant to serve as examples and are not intended as a complete or a representative list.

[12] DIRECTIVE (EU) 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, OJEU L 194/1; http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

emphasizes the need for operators to "pursue their own informal cooperation mechanisms to ensure the security of network and information systems". This new broad category of "digital services providers" includes, but is not limited to: e-commerce services ("online marketplace"), search engines and cloud computing services.[13]

Significantly, the EU adopted the NIS Directive following another significant shift in its internal policy – one referring to the protection of individual privacy through personal data safeguards. This legislative dichotomy: the need to simultaneously ensure security and privacy with little help or guidance from the state, puts ISPs in a particularly difficult position. The unspecified cybersecurity preventive measures are to go hand in hand with enhanced protection of personal data, requiring e.g. a privacy audit, ensuring that all personal data at the disposal of the administrator, is secured and used solely for legally determined purposes. With the enhanced role to be played by good business practice and with companies being encouraged to exchange information on potential security threats unofficially, EU laws put ISPs to a challenging test in balancing the interests of customers, competitors and states.

Cyberterrorism and cybersecurity

The 21st century saw a new face of international terrorism. To the already ambiguous list of "asymmetric" threats to international peace and security, i.e. ones originated by private individuals such as terrorist or radical groups, possibly by states not capable of a traditional armed attack conducted with the use of national military, was amended with the notions of "cyberthreats", "cyberterrorism" and "cyberwarfare", neither of which can be clearly and reliably defined as per contemporary legal scholarship and international practice. Their general common trait is the use of the global computer network based on the Internet Protocol (TCP / IP) and protocols compatible with it as tools for conducting attacks on national security and creating new threats to international peace.[14] The direct reference to the well recognized, yet not uncontroversial, notions of terrorism and war show the scale of potential harm to domestic and international interests caused by cyberthreats.[15] Any attempt to define "cyberterrorism" as an element of legal terminology must rely on the UN antiterrorism conventions. The legal qualification of threats originated online has been subject to political and scholarly debate since late 1990s, accompanying the slow rise of other Internet governance related debates on international agendas.[16] One of the early scholarly attempts at a legal assessment of cyberthreats described cyberterrorism as the use of a digital system to commit an act punishable or prohibited by the UN anti-terrorist treaties.[17] With this UN reference, "cyberterrorism" could be defined as:

"*an intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm*".[18]

The definition centers on a particular category of information systems, as described above with a reference to "critical infrastructure". It is because of the security of such systems that states need to take particular mea-

[13] DIRECTIVE (EU) 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, OJEU L 194/1; http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[14] Sushil Jajodia, *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats* (Springer 2011); H. P. Hestermeyer, *Transboundary Harm: Internet Torts* in *Transboundary…,* Russell A. Miller, Rebecca M. Bratspies (eds.), 268 – 280.

[15] M. E. O'Connell*,* 'Cyber Security without Cyber War' (2012) 14 JCSL 189 – 190.

[16] For a detailed discussion on the legal issues of Internet governance and their evolution see: Joanna Kulesza, 'Legal issues in a networked world' in *Handbooks of Communication Science 5, Communication and Technology* L. Cantoni, J.A. Danowski (eds.), (De Gruyter Mouton 2015) 345-364.

[17] Stanford University, *Draft International Convention to Enhance Protection from Cyber Crime and Terrorism* (2000) available at: <http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf> accessed 14 March 2016 (hereinafter cited as: *Stanford cybersecurity draft*).

[18] *Stanford cybersecurity draft*, Article 1.

sures to protect international peace and prevent their damage, as critical infrastructures are forever more frequently operated online or at least equipped with an Internet connection. The latter, a relatively new technical feature, can be considered their weakest point. This particular risk of significant harm caused to states as well as international security with the use of the global network has been appearing on international diplomatic agendas. The international duty of states to prevent online generated threats is being discussed in the context of international cooperation on law enforcement and can be enforced through a combination of various means, covering "all practicable measures" to prevent threatening conduct within or outside state territories as per the universal norms of jurisdiction. This can also be done through exchange of information, coordination of administrative and other activities and introducing any other appropriate measures.[19]

Those general observations reflect the contemporary consensus and international practice on antiterrorist measures. Time has shown that the general principles of anti-terrorist treaties remain accurate and applicable to new threats, such as those originated online. This observation seems particularly significant regarding the fact that the question of international cybersecurity and threat prevention has recently transcended the academic debate and entered diplomatic forums of intergovernmental organizations.

It must be observed however that the obligation to prevent significant transboundary harm inflicted with the use of an electronic network applies to two categories of events: incidental and deliberate, with the latter often showing a terrorist character if the acting individuals operated without state authorization, followed a political motivation and aimed at causing panic or corrupting a government. The duty o prevention applies however also to the former category, implying respective obligations of all states. Effectively, regardless of the origins of a given harmful event, state responsibility depends on its actions *vis-a-vis* a particular threat. If in a given situation a state fails to undertake preventive measures or ones minimizing the harmful results, e.g. by identifying the individuals or occurrences originating the threats it is deemed undiligent and may be held internationally responsible. If however in a given situation a state has taken all measures at its disposal to prevent a given harmful event and that threat showed unavoidable, it may be freed from responsibility. What is more, the international law criteria of "aggravating circumstances" that is circumstances the occurrence of which brings a "higher level of responsibility" of a state is met when state authorities, informed of an ongoing cyberattack originated from state territory, intentionally fail to initiate appropriate procedures or proceedings.[20]

With that it seems safe to say that all states are under an obligation to prevent significant transboundary harm originated within state jurisdiction, territory or control. This obligation should be met with the application of all appropriate measures, including but not limited to introduction of judicial and administrative measures aimed at identifying and prosecuting such offences or enforcing other forms of liability. This due diligence obligation should be executed in international cooperation aimed at preventing such attacks. The latter includes the necessity to share information on potential threats and jointly identify effective prevention measures. Just as in the general observations made by the ILC, it is the individual state's level of economic and technological development that proves significant for assessing the level of diligence required in a particular case, although the lack of material resources may not serve as the sole explanations for enabling state territory for originating harmful online activities. Moreover, also in the context of cybersecurity, the duty of prevention a continuous one, requiring states to engage in ongoing collaboration. All preventive measures aimed at granting international cybersecurity need to be introduced and enforced in good faith and proportional to the particular threat. The element of proportionality, imminent to due diligence can be used to support an argument for a higher due diligence standard for the protection critical infrastructure, such as power plants, water supplies or public transportation supported by computer operated infrastructure. Moreover, it may be argued that the elements of the global network itself, such as the Internet backbone or the DNS also should be granted particular protection, higher than e.g. local or commercial networks.

---

19 *Stanford cybersecurity draft,* Article 11.

20 *García Amador's second report,* U.N. Doc. A/CN.4/106, pt. 9*,* 122.

Cybersecurity due diligence

These observations have already been recognized beyond academic debate and included in various documents. Arguably it was the Council of Europe with its 2011 Recommendation that was the first international forum to recognize the role of due diligence in international cybersecurity. [21] It has called upon states to cooperate with other stakeholders: business and civil society to identify and enforce all necessary measures "to prevent, manage and respond to significant transboundary disruptions to (…) the infrastructure of the Internet." This duty was to be enforced "within the limits of non-involvement in day-to-day technical and operational matters" as performed by private parties, such as Internet service and content providers. The reference to "all relevant stakeholders" mirrors the multistakeholder principle of international Internet law and Internet governance.[22] The Recommendation goes on to identify a minimum standard of care in cases of maintaining risks and consequences of any "disruptions", i.e. negative consequences influencing "the stable and ongoing functioning of the network", resulting from "technical failures". Council of Europe (CoE) puts particular emphasis on the interconnection between effective networks resilience and international cooperation, by directly identifying it as "intrinsically related to" the decentralized and distributed nature of this unique medium. Significantly, since all actions "in one jurisdiction may affect the ability of users to have access to information on the Internet in another", the international no-harm principle needs to be recognized as the starting point of any cybersecurity cooperation. This is also a derivative of the general obligation of states to act in compliance with international law, ensuring that "their actions do not have an adverse transboundary impact". The CoE Committee of Ministers made a direct reference to the possible harmful effect that the activities taken in one location may have on the "access to and use of the Internet" beyond state jurisdiction. States are therefore under an international obligation to

ensure that their actions within their jurisdictions do not illegitimately interfere with access to content outside their territorial boundaries or negatively impact the transboundary flow of Internet traffic,

with a failure to meet this obligation resulting in possible responsibility of an non-diligent state. One of the significant elements of the international legal order that comes into play with reference to online threats is the international human rights law, obliging states to refrain from putting illegitimate, from an international point of view, limitation on individual rights, in particular the right to privacy or freedom of expression.[23] Effectively, any "blanket surveillance", i.e. a non-case-specific invasion of privacy or any other restriction of online communications may not be introduced as preventive measure as it would go against the body of international human rights law in general and against the recommendations of the Human Rights Council in particular, including e.g. those referring to Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[24]

With that it can be easily ascertained that the due diligence obligation of preventing transboundary harm online does not reach as far as continuous surveillance of all subjects to state jurisdiction. It is rather to the contrary – such surveillance needs to be considered a breach of international human rights law and go against state positive duties of states to ensure fundamental rights to all state subjects. Also, as per the human rights standard on free speech, as in Article 19 ICCPR, any duty of preventive censorship regarding online content, placed on e.g. Internet service providers, should also be viewed as a violation of international human rights

[21] CoE, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet; September 21st, 2011, pt. 1.3. (hereinafter cited as: *CoE, Recommendation CM/Rec(2011)8…*).

[22] For a detailed definition of the multistakeholderism principle in international Internet law see: Joanna Kulesza, (2012). International Internet law. *Global Change, Peace & Security* 24(3), 351 – 364.

[23] *CoE, Recommendation CM/Rec(2011)8*…, para. 1.1.1.

[24] United Nations (1966). International Covenant on Civil and Political Rights, G.A. res. 2200A (XXI), U.N. Doc. A/6316 (1966).

law.[25] The same free speech standard, which prohibits censorship, should be viewed as prohibiting rather than encouraging any state authorization for online services, although in some cases they might be considered risk-originating activities. The encouraged cooperation focuses rather on preventing transboundary harm to Internet's stability and resilience through the development and implementation of emergency procedures for managing and responding to Internet disruptions applicable to all stakeholders, in particular bodies managing critical infrastructure. Aiming to meet this obligation states need to ensure "the development and implementation of common standards, rules and practices aimed at preserving and strengthening the stability, robustness and resilience of the Internet". This general obligation translates into particular duties of criminal law enforcement and international legal aid as well as no undue delay in notifying potential victims of any risks of significant transboundary disruptions to the functioning of the network.[26] Such notice from the originating state should comprise of four elements: 1) a prompt notification of any such risk for all potentially affected states; 2) sharing all available information relevant to responding to a given disruption; 3) prompt engagement in multilateral consultations aimed at identifying and applying mutually acceptable measures of response to threats already arisen as well as provide 4) mutual assistance "as appropriate". When attempting to indicate the activities within the duty of due diligence one should reflect "with due regard" the capabilities of individual states, with other states offering help to those affected in good faith, aiming to mitigate the already arisen harmful results. Due diligence in cases of online communications ought to reflect the multistakeholder environment and the principle of non-involvement, obliging states to refrain from interference with the "day-to-day technical and operational matters". As is the case with all due diligence obligations, states are required to introduce "reasonable: legislative, administrative or any other appropriate measures" to ensure online security and connectivity. An obligation so identified indicates the basic efforts of states with regard to securing online communications. States are therefore encouraged to engage "in dialogue and co-operation for the further development of international standards relating to responsibility and liability" for online disruption.[27]

A similar idea is reflected in the EU NIS Directive, which requires states to ensure that all critical infrastructure operators, including those operating on the digital market, are legally obliged to introduce risk management mechanisms and procedures ensuring information sharing with state authorities. The fact that no such obligation existed thus far resulted in only under 30% of small and medium enterprises in Europe ensuring any risk management policies, including risk assessment and procedures in case of a system failure. This obligation, while arguably ensuring a higher level of security, will also result in increased costs for the operation of individual service providers. Whether those costs should be borne by the enterprises alone, or whether states should subsidize new security features, remains open to discussion. Moreover, the information sharing duty, resting upon private bodies, remains unilateral – while state authorities and state-operated infrastructures remain one of the main targets of cyberattacks, states shun the duty to share threat information with private companies. This policy seems short-sighted as only through comprehensive cooperation can cyberthreats be affectively liquidated.

This most recent European regulation can be seen as evidence for the ongoing transposition of international law due diligence standard onto particular, international cybersecurity obligations, aimed at ensuring a safe transboundary flow of data and information services. As a result, the well recognized due diligence standard in international law translates onto individual duties of states in the domain of cybersecurity. Those duties include listing potentially threat-originating services, whose operators will need to meet particular security obligations under the pain of sanctions but also a good-faith involvement in international cooperation and exchange of information.

---

[25] See e.g. European Court of Justice (2011), Judgment of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) ; case number C-70/10.

[26] *CoE, Recommendation CM/Rec(2011)8*…, para. 2.1.3.

[27] *CoE, Recommendation CM/Rec(2011)8*…, para. 2.

ISP risk liability – why we need an insurance fund

International law has developed various tools to target the inherent risk of transboundary harm generated within its various fields of deployment. Those experiences can well be used to counter imminent cybersecurity threats. In international environmental law for example, any risk generating activity needs to be proceeded by a state authorization and accompanied by obligatory risk insurance acquired by the operators. Those two elements are to ensure a high level of security and necessitate caution on behalf of the operator, whose negligence could result in loss of lives or great economic losses. As the case of Ukraine in 2015 proved, cybersecurity issues can result in identical damages, with insufficient cybersecurity measures in place generating great disruptions to public life and significant monetary damages. While setting up a service offering Internet-based services usually does not require prior authorization, the significant losses that it may cause have already provoked the insurance industry to offer voluntary insurance. Yet since the networks and supply chains that have traditionally been co-notated as offering services critical to the public, such as power suppliers or public transportation are being integrated with computer-operated technologies to run them, any threat to so installed critical infrastructure is also a cybersecurity threat. Any cybersecurity breach can result in large numbers of victims and the line to be drawn between computer systems crucial to critical infrastructure security and those insignificant to its safe operation is forever more blurred, as proved by the Stuxnet incident, where an employee's infected thumb drive used on the nuclear facility's computer caused the whole system to overheat, threatening a nuclear disaster for the whole region. Yet the line we chose to draw for computer-operated or computer-supported critical infrastructure results directly in subjecting its operator to costly security obligations. Thus far the catalogue of risk-originating activities recognized in international law has been intentionally kept narrow, relying on treaties and soft law dealing with nuclear energy, outer space and maritime oil transportation. It required state authorization for any operator to engage with such activity, one granted only after scrupulous security procedures have been implemented. Since cyberthreats are likely to occur in various areas of public life, as indicated above, subjecting all computer-based services to authorization would be excessive and undesired, if not simply unenforceable. It would be recommended however to look at Internet-based services offered to support critical infrastructure operation, potentially causing significant transboundary harm, as an element of the open category of risk-generating activities, accompanied by a due diligence obligation, seems well justified.

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 vaguely set 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 principles 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 for the Internet based community. One should emphasize, that some states, including 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 seems the natural 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.[28] 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.

[28] For a detailed discussion on the issue see: Joanna Kulesza, (BRILL 2016). Due Diligence in International Law.