STATE RESPONSIBILITY IN DIGITAL SPACE

by Jovan Kurbalija[1]

This text is an adaptation of the same-titled article that appeared in the Swiss Review of International & European Law, *2016, issue 2*

Abstract

State responsibility is one of the mechanisms for legal redress in international affairs. Yet the formulation of state responsibility in the digital realm is still in a very early stage. This article addresses both a *lex lata* analysis based on existing law of state responsibility, and *lex ferenda* solutions that may be developed in order to address specificities of the Internet, such as state responsibility for the digital activities of non-state actors under their jurisdiction. The practical applicability of the laws describing state responsibility is analysed for the case study of an imaginary cyberattack by country A (DigiLand) on the electrical grid system of country B (CyberStan), which caused a blackout and major damage in CyberStan. The search for a possible solution in the digital field involves the potential application of law and the practice of state responsibility developed previously in environmental law and other specialised fields of international law. In addition, the analysis addresses the interplay between states' careful approach to international responsibilities, and the practical need to provide legal solutions for cases in the digital field.

Content

---

[1] Dr Jovan Kurbalija is the founding director of DiploFoundation and Head of the Geneva Internet Platform. He is a former diplomat with a professional and academic background in international law, diplomacy and information technology.

The growing relevance of the Internet for modern society increases the need for legal redress in digital space. The legal interests of individuals, entities and countries are threatened by cyberattacks on critical infrastructure, cybercrime, data theft, and defamation - to name a few. Due to the trans-border nature of Internet communication, legal redress often requires action beyond national borders.

In the search for justice and legal solutions, a wide range of mechanisms has started to appear. In Europe, recourse on digital cases is often sought with the Court of Justice of the European Union, as was the case with the right to be forgotten and the Safe Harbour framework. [2] Internet companies take on a quasi-juridical role by ruling on cases raised by their users. For example, in the implementation of the Court of Justice of European Union ruling on the right to be forgotten, Google had to evaluate 1,486,964 requests for the removal of Internet addresses in the period of 29 May 2014 – 10 May 2016.[3] Legal cases related to Internet domains are handled through an innovative type of arbitration, in the form of the Uniform Dispute Resolution Procedure (UDRP).[4]

States are looking for an effective legal response to challenges posed by digital developments. The Internet influences how states deliver their core functions of ensuring peace and stability, as well as economic and social wellbeing, and protecting human rights. States' responsibilities towards citizens and their international responsibilities towards other states are increasingly affected by the Internet.

Thus, it is not surprising that the words 'responsible' and 'responsibility' are among the most used terms - 13 times – in the 2015 report on global cybersecurity of the United Nations Group of Government Experts.[5] A policy principle of reasonable behaviour of states in digital space has been frequently mentioned in international instruments.[6]

This article discusses how the law of state responsibility can ensure the implementation of the policy principle of the responsibility of states in digital space. The article addresses both a *lex lata* analysis based on existing law of state responsibility, as outlined in the International Law Commission Draft Articles on Responsibility of States for Internationally Wrongful Acts (hereinafter referred to as the *Draft Articles*), and *lex ferenda* solutions that may be developed in order to address specificities of the Internet, such as state responsibility for digital activities of non-state actors under their jurisdiction.

---

[2] See Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12, decided 13 May 2014; ECLI:EU:C:2014:317) concerning the right to be forgotten;Maximillian Schrems v. Data Protection Commissioner (C-362/14, decided 6 October 2015; ECLI:EU:C:2015:650) concerning the invalidation of the Safe Harbour framework.

[3] Google, «European privacy requests for search removals,» Google Transparency Report, 10 May 2016, <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en> (all internet sources were last accessed in May 2016).

[4] For a comprehensive survey of Internet governance, jurisdiction and legal developments, consult Jovan Kurbalija, An introduction to Internet Governance, 6th ed. Geneva, 2014.

[5] United Nations, General Assembly, Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General A/70/172 (22 July 2015).

[6] Council of Europe's 2011 resolution stressed various aspects of state responsibility in digital space, including « …their shared and mutual responsibilities to take reasonable measures to protect and promote the universality, integrity and openness of the Internet…» Council of Europe Recommendation CM/REC(2011)8, Recommendation of the Committee of Ministers to member states on the protection of the universality, integrity, and openness of the Internet (21 September 2011).

The first section discusses the impact of the Internet on international law and the main concepts and terminology related to state responsibility in the digital field. This section also examines how the digital field could benefit from the development of law and practice of state responsibility in environmental and other specialised fields.

The second section examines the applicability of state responsibility rules to the Internet in an imaginary cyberattack by country A (DigiLand) on the electric grid system of country B (CyberStan), which caused a blackout and major damage in CyberStan.

I. Main concepts and terminology on state responsibility

Before addressing the application of state responsibility to the digital sphere, it is important to situate this analysis within the broader discussion on both state responsibility and the interplay between the Internet and international law.

A. Applicability of international law to digital sphere

The core social functions of the law remain as relevant in the Internet era as it was a thousand years ago, when our far predecessors started using rules in order to organise human society. Law is about regulating rights and responsibilities among individuals and the entities they form, be it companies, organisations or states. Throughout the long evolution of human society, technology has also been evolving, yet the basis of the law remains the same.

In the Internet era, the intense trans-border digital interaction poses the main challenge in applying existing legal rules. There is a consensus that existing international law applies to the Internet.[7] This principle is stipulated by the 2013 Report of the UN Government Group of Experts (GGE)[8] and was reiterated subsequently in other policy decisions. In the field of human rights, the resolutions of the UN General Assembly and UN Human Rights Council have firmly established the principle that the same human rights that people enjoy offline must also be protected online.[9]

---

[7] The most prominent view of uniqueness of the Internet is formulated by John Perry Barlow's Declaration of the Independence of Cyberspace (1996): «[the Internet] is inherently extra-national, inherently anti- sovereign and your [states'] sovereignty cannot apply to us. We've got to figure things out ourselves». One of the first articles that questioned this approach was written by Judge Frank Easterbook, who argued in the article «Cyberspace and the Law of the Horse» (1996) that although horses were very important, there was never a Law of the Horse. See John Perry Barlow, «A Declaration of the Independence of Cyberspace», Electronic Frontier Foundation, 8 February 1996, <https://www.eff.org/cyberspace-independence>; and Frank Easterbrook «Cyberspace and the Law of the Horse», University of Chicago Legal Forum (1996), 207–216.

[8] United Nations, General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013, reissued for technical reasons on 30 July 2013).

[9] The principle that existing law applies to the Internet is supported by, among others, the following policy documents:

- General Assembly resolution 70/125, Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, A/70/125 (13 December 2015).
- General Assembly resolution 69/166, The right to privacy in the digital age, A/RES/69/166 (18 December

While the answer to the question *if* international law is applicable to the Internet is positive, the main remaining question is *how* to implement existing rules. For example, an important challenge is to ensure legal redress in cases related to the Internet that contain international elements. Individuals and companies can rely on international private law, while national governments can use international public law mechanisms. Both approaches have a long tradition, and were originally developed in an era of less intensive exchanges across national borders. They need to be examined and, when needed, further developed in order to provide affordable access to justice in Internet matters to individuals and institutions worldwide.

B. Legal sources of state responsibility

The main source on state responsibility is the International Law Commission's *Draft Articles*, which is considered to be the codification of international customary law on state responsibility.[10] The *Draft Articles* were adopted in 2011 by UN General Assembly Resolution 56/83[11], 52 years after state responsibility was selected by the UN as one of the fourteen topics for codification in 1949.[12] The long drafting process confirms that state responsibility has been one of the «most ambitious and most difficult topics of the codification work of the International Law Commission».[13] One of the reasons for this complexity resulted from states' reluctance to strengthen the rules of state responsibility, as they could affect states' sovereignty.[14]

Conceptually speaking, the *Draft Articles* create a two-level structure of state responsibility. Primary rules specify state obligations (e.g. not to cause harm to other states). Secondary rules identify «whether that obligation has been violated and what should be the consequences of the violation.»[15] The law of state responsibility deals with the secondary rules.

The 2015 UN GGE Report's approach to state responsibility closely reflects the *Draft Articles*. Namely, paragraph 28 of the UN GGE Report requires a breach of law (an 'internationally wrongful act') as pre-condition for state responsibility. This paragraph strengthens the restrictive use of the law of state responsibility in the Internet field by stressing that *«the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State.»* The *Tallinn Manual on the International Law Applicable to Cyber Warfare* ('*Tallinn Manual*'), which deals with the law of

---

2014).

- United Nations, General Assembly, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13.

10 General Assembly resolution 56/83, Responsibility of States for Internationally Wrongful Acts, A/RES/56/83 (28 January 2002).

11 General Assembly resolution 56/83, Responsibility of States for Internationally Wrongful Acts, A/RES/56/83 (28 January 2002). The International Law Commission (ILC) articles are annexed to the resolution.

12 Although law of state responsibility was listed in 1948, an effective work on the codification started in1956. For more information about the evolution of codification of state responsibility see James Crawford, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries, Cambridge 2002.

13 Peter Malanczuk, Akehurst's Modern Introduction to International Law, 7th rev ed. London 1997, p. 254.

14 The specificity of the law of state responsibility was also reflected in the fact that the ILC did not use its typical method of producing a draft convention, as was done in the case of the 1969 Vienna Convention on Treaty Law. Instead, the ILC produced Draft Articles as a less binding form of codifying norms on state responsibility.

15 Roberto Ago, «Second Report on State Responsibility», in: International Law Commission (ed.), Yearbook of the International Law Commission, New York 1970, at 306.

armed conflict in digital space,[16] also follows the restrictive approach on state responsibility regulation taken by the *Draft Articles*.

In his analysis of state responsibility on the Internet, Peter Margulies is critical of the restrictive approach towards state responsibility adopted by the Tallin Manual, which requires a breach of law and attribution to state organs. Such a high threshold could make state responsibility completely unusable in digital space.[17] Furthermore, a restrictive approach to the law of state responsibility based on the *Draft Articles* could collide with the 'no harm' principle, which could make states responsible to prevent the use of their territories in any way that could harm the interests of other states. It is the application of the traditional Roman law maxim: *sic utere tuo ut alienum laedas*[18] (use your own property so as not to injure that of another) to international law.[19]

This delicate balance between restrictive rules on state responsibility and the 'no harm' principle is addressed in other areas of international law with pronounced trans-border aspects, including the environment and outer space. Specialised fields of international law, which are analysed in the subsequent part, could inspire some solutions for state responsibility in the digital field.

C. Innovative solutions from environmental law and other specialised fields of international law

The restrictive approach to state responsibility taken by the Draft Articles has shown limited usability in fast emerging legal fields, such as the environment, outer space and other issues with profound trans-border aspects. In these legal fields, new legal solutions and practices on state responsibility have been developed, in particular around the application of 'no harm' principle. This section will focus on identifying similarities and differences between the digital field and other specialised fields of international law. This analysis will form the basis for identifying useful practices and analogous solutions on state responsibility in digital space.

1. Environment

The most frequently used parallel in the discussion on the development of international legal solutions for the Internet is with the environmental field. In particular, parallels are made with climate change and transborder pollutions, an area that has much in common with the Internet's transborder nature. However, there is much more to the comparison between the Internet and environment/climate change than their transborder nature alone.

While both the environment and the Internet are characterised by transborder dynamics, there are significant differences related to the degree of control over transborder effects. For climate change, it is almost impossible to manage these effects (for example, think about global warming),

---

16 See Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge 2013.

17 Peter Margulies, «Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility», 14 Melbourne J. of Int'l L. (2013), p. 496.

18 The principle sic utere tuo ut alienum laedas is one of the fundamental principles of international environmental law. Sic utere tuo… is the basis of Principle 21 of the Stockholm Declaration. The same legal reasoning was used in Corfu Channel Case of the International Court of Justice.

19 For more information on the «no harm» principle please consult section II.B.1.

whereas it is much easier to control the Internet's transborder dynamics. Geo-location tools anchor the Internet strongly into geography. For example, technology enables the blocking or filtering of Internet traffic to and from particular territories.

The immediacy of the impact of transborder dynamics also differs between climate change and Internet cases. Climate change has long-term consequences, whereas most of the Internet impacts are almost instant. A possible temporal analogy between climate change and the Internet would be in preserving Internet knowledge and data as global public goods for future generations.

The two fields further differ in the availability of an international legal framework. Climate change is regulated by the UN Framework Convention on Climate Change (1992). As for the Internet, there is no convention or treaty that regulates the digital field in a comprehensive way. The only international legal instrument is the Council of Europe's Convention on Cybercrime, which regulates a specific area (cybercrime) at the regional level, with global adherence.

The involvement of non-state stakeholders is another point of slight divergence. Governments negotiated at the COP in Paris; civil society, academia and business were part of lobbying activities, similar to many other global policy processes (migration, trade, food, human rights, etc.). The only difference is that non-state actors were a bit 'noisier' in climate change policy than in other policy processes. Similarly, non-state actors have had an active role in the World Summit on the Information Society (WSIS), the International Telecommunications Union (ITU), and many other related digital processes. A novel element in digital policy is the participation of all major stakeholders on an 'equal footing' in the activities of the Internet Governance Forum and The Internet Corporation for Assigned Names and Numbers (ICANN).

Finally, there is a difference related to the evidence that is used for decision-making. Climate change policy making is based on scientific evidence provided by the International Panel on Climate Change (IPCC). Scientists indicated the likelihood of climate change, and created a framework for diplomatic negotiations. Evidence is not used as widely as one would expect in an engineering field as the Internet. For example, we know very little about the impact of cybercrime (estimates of global impact range from US$ 300 billion to 3 trillion). This creates a major evidence gap in global digital policy making.

These similarities and differences are important to consider, in order to understand the applicability of environmental and climate state responsibility solutions to the Internet. The most advanced use of environment-related state responsibility is in the field of transborder pollution. The first major case was the Trace Smelter case of 1941, which was based on the 'no harm' principle, later on used in many declarations and conventions in the environmental field. The case will be explained in further detail in section II.B.1 of this paper.

2. Watercourses

Both watercourses and the Internet share resources across national borders. The equitable and reasonable utilisation of common resources is the key concept in international watercourse legislation, as it was specified in Article 5 of the UN Watercourses Convention:

> *«Watercourse States shall in their respective territories utilize an international watercourse in an equitable and reasonable manner. In particular, an international watercourse shall be used and developed by watercourse States with a view to attaining optimal and sustainable*

utilization thereof and benefits therefrom, taking into account the interests of the watercourse States concerned, consistent with adequate protection of the watercourse.»[20]

In addition, Article 7 of the UN Watercourse convention introduced the principle of 'no harm' to other states. When related to the debate on Internet's legal matters, the debate around absolute vs. limited territorial sovereignty over waterflows is particularly relevant. Absolute sovereignty was adopted in the so-called 'Harmon Doctrine', named after an American Attorney-General in 1895, during a dispute between the U.S. and Mexico over the use of the Rio Grande waters. According to the 'Harmon Doctrine', states are free to decide on the use of rivers flowing through their territory. The Harmon Doctrine has not gained following. Instead, the practice of international water management has continued to follow the approach of limited sovereignty, which implies taking the interests of other states into consideration. The Internet is likely to require the same approach, given the high degree of interdependence among societies in developing and using the Internet.

3. Nuclear activities

State responsibility in the nuclear field is stricter than the general international law codified in the *Draft Articles*. A set of international instruments dealing with state responsibility in the field of nuclear energy include the 1960 Convention on Third Party Liability in the Field of Nuclear Energy, 1963 Vienna Convention on Civil Liability for Nuclear Damage, 1986 Convention on Early Notification of Nuclear Accidents, 1986 Convention on Assistance in Case of Nuclear Accidents.

State responsibility in the nuclear field could be triggered by failure of states to exercise due diligence over activities of nuclear facilities. In addition «states are responsible for transfrontier harm at least when it results from negligence or intentional pollution and possibly even for harm resulting from accidents».[21]

4. Law of the sea

The 1982 UN Convention on the Law of the Sea (UNCLOS) introduces state responsibility in article 194 (paragraph 2)

> *«…2. States shall take all measures necessary to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment, and that pollution arising from incidents or activities under their jurisdiction or control does not spread beyond the areas where they exercise sovereign rights in accordance with this Convention.»*[22]

UNCLOS covers both state responsibility towards other states and for damages of areas beyond the limits of national jurisdiction such as the open sea. It also triggered an analogy between the open sea and the Internet, and introduced the application of the concept of 'common heritage of

---

[20] Convention on the Law of the Non-navigational Uses of International Watercourses, New York 21 May 1997, U.N. Doc. A/51/867.

[21] Alexandre Kiss, «State Responsibility and Liability for Nuclear Damage», 35 Denver J. of Int'l L. & Policy (2006), p. 133.

[22] United Nations Convention on the Law of the Sea (UNCLOS), Montego Bay, 10 December 1982, 1833 U.N.T.S. 3.

mankind' to the Internet.[23] This would mean that the Internet's infrastructure is beyond individual states' jurisdiction and subject to the protection of all states. Classifying the Internet as 'common heritage of mankind' would have a significant impact on state responsibility on the Internet.

5. Outer space

The legal regime related to outer space involves a high level of state responsibility as specified in Outer space: 1972 Convention on International Liability for Damages Caused by Space Objects.[24]

Article 6 of the 1967 Outer Space Treaty[25] extends state responsibility to non-government actors by specifying that:

> *«Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the moon and other celestial bodies, and each State Party from whose territory or facility an object is launched, is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air or in outer space, including the moon and other celestial bodies.»*

Compared to all other mentioned fields, the Outer Space Treaty provides the broadest coverage of state responsibility. A possible explanation for this stipulation is that back in 1967, when the Convention was drafted, only states had sufficient financial and technical means to launch satellites. In the meantime, more and more private entities have gained the capacity to launch satellites. Still, the requirements for launching satellites remain higher than for, for example, conducting cyber attacks. The low threshold for cyber activities (they are just 'a click away'), means that it is not very realistic for states to assume responsibility for cyber activities of any actor under their territorial or personal jurisdiction as States can do for limited number of non-state actors involved in outer space activities.

II. Application of state responsibility to the Internet

After examining the law of state responsibility in the previous section, this section will apply state responsibility to a hypothetical case in which Country A (CyberStan) suffered major damage at its electronic grid system caused by a cyberattack. The only certain fact is that the attack comes from a computer based in country B (DigiLand). CyberStan's diplomatic legal team needs to explore all possibilities for legal action against DigiLand. The analysis of their legal options will be supported by the main academic and policy approaches to state responsibility.

---

[23] See «Statement by Dr. Alex Sceberras Trigona, Special Envoy of the Prime Minister of the Republic of Malta», World Summit on the Information Society Review Process, 15 December 2015, <https://www.gov.mt/en/Government/Press%20Releases/Documents/pr152897a.pdf>.

[24] Convention on International Liability for Damage Caused by Space Objects, 29 March 1972, 961 U.N.T.S. 187.

[25] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Washington, D.C., 27 January 1967, 610 U.N.T.S. 205.

A. Types of state responsibility

For CyberStan, the legal options to claim responsibility of DigiLand for this attack are summarised in the enclosed table, which presents the main types of responsibility/liability (row) and elements of responsibility (column).

Types of responsibility **Elements of responsibility**	"FAULT" SUBJECTIVE RESPONSIBILITY	"RISK" OBJECTIVE RESPONSIBILITY	STRICT RESPONSIBILITY
Breach of rules of international law	Required	Required	NOT Required
Intention to breach the rule (fault/culpa)	Required	NOT Required	NOT Required
Territorial link (action originating computer or network under state juridiction)	Required	Required	Required
Attribution to state (including its organs)	Required	Required	NOT Required
Damage and loss	Required	Required	Required

1. 'Fault' Responsibility

Firstly, CyberStan could try to base the case against DigiLand on fault responsibility, an approach that was used by traditional international law. This concept was particularly dominant during the interwar period (1918-1941). However, it has started losing relevance in the second half of the 20th century. The incompatibility between modern states and 'fault' responsibility was highlighted by I. Brownlie: «In the conditions of international life, which involve relations between highly complex communities, acting through a variety of institutions and agencies, the public law analogy of the *ultra vires* acts is more realistic than a seeking for subjective culpa in specific natural persons who may, or may not, "represent" the legal person (the state) in terms of wrongdoing.»[26] Brownlie's concern can be extended to our case. It is not likely that CyberStan will have enough evidence to first identify and subsequently prove fault of DigiLand's officials.[27] As a result, CyberStan is likely to look for the next option on the state responsibility 'menu'…

2. 'Risk' Responsibility

'Risk' or 'objective' responsibility lowers the threshold for responsibility. It does not require fault, but it requires the attribution of the action to other states and their officials. 'Risk' responsibility is

[26] Ian Brownlie, System of the Law of Nations, State Responsibility, Part I, Oxford 1983, p. 38.
[27] Attribution in cyber cases is discussed under II.B.2

based on a breach of rules (ex delicto). In our case, CyberStan would need to find the primary rule of international law that was breached. For example, this could be a breach of the 'no harm' principle, which requires a state «to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein...» as it was specified in Trail Smelter Case (1941).[28] The application of the 'no harm' principle could be linked to an examination on whether a state has taken the necessary 'due diligence' measures in order to avoid any negative effects on the territory of other states (for more on this, see section II.B.2.a.2).

3. Strict responsibility

If CyberStan cannot prove a breach of primary law, the last possibility would be to resort to 'strict responsibility', which requires proving that the cyberattack originated from the territory of another state; in this case, from DigiLand. Strict responsibility in its purest form is rarely applied. Namely, it is not possible for states to monitor all activities on their territory that may cause harm to other states. In the digital field, it is particularly difficult to control all digital activities conducted by non-state actors. In addition, in many cases, it is not even desirable to request states to monitor all digital activities. It may increase surveillance and endanger the delicate balance that societies worldwide need to strike between the protection of human rights and safeguarding public interests.

While it is important to establish a territorial link of the cyber action to the territory of the other state, this is not sufficient to establish state responsibility. As it will be discussed further down – in section II.B.2.b – the 'territorial link' should be supplemented by the due diligence requirement, which makes a state responsible for not taking all adequate steps to protect other states from harm.

4. Direct and indirect responsibility

Another classification, introduced by Oppenheim[29], divides state responsibility into two categories. Direct responsibility is based on actions of states and their organs. Both 'fault' and 'risk' responsibilities are direct responsibilities. Indirect or vicarious responsibility is responsibility of damage caused by other entities under the state's jurisdiction, including individuals and companies. Strict responsibility is an example of indirect responsibility.

B. Elements of state responsibility

State responsibility to Internet cases will be analysed on three main elements: 1) breach of rule of international law, 2) attribution and 3) existence of damage or loss. The other two elements of state responsibility that were mentioned in the table – fault/culpa and the territorial link - are not further analysed in this section. Fault/culpa is not included since it is used for 'fault responsibility', which is no longer applied in international practice. The 'territorial link' is assumed to exist whenever state responsibility is discussed, as it is in the CyberStan case. Namely, the basis for any

[28] Trail Smelter Case (United States v Canada). Arbitral Trib., 3 UN Rep. Int'l Arb. Awards 1905 (1941).
[29] Robert Jennings & Arthur Watts, Oppenheim's International Law, 9th ed., Oxford 2008.

discussion on DigiLand's responsibility is that the cyber incident in CyberStan was initiated from the computers located in the territory of DigiLand.

1. Breach of rules of international law

State responsibility is initiated by a breach of rules, which could be done by both acts and omissions to act. The International Court of Justice confirmed omission as the basis for state responsibility in several cases, including *Corfu Channel* (UK v. Albania)[30], *United States Diplomatic and Consular Staff in Teheran* (US v. Iran)[31], and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro)[32].

Primary rules dealing specifically with the Internet are limited. If CyberStan and DigiLand are parties to the 2001 Budapest Convention on Cybercrime, they are supposed to follow the primary rules preventing cybercrime activities as stipulated by this Convention. If they are not parties to the Budapest Convention, they will have to rely on general international law and, in particular, the UN Charter. CyberStan could base this case on the 'no harm' principle, which is considered to be part of international public law.

The 'no harm' rule specifies that a state should not allow the use of its territory for activities that could harm other states. This rule dates back to the Roman law and maxim *sic utero tuo, ut alineum non laedas* (literally, use our own so as not to injure another). The legality of the 'no harm' rule is supported by a wide range of conventions, court cases and policy documents.

An intensive discussion on the use of the 'no harm' principle started with the Trail Smelter case on transboundary pollution, which took place in 1941 and stipulated that «no state has the right to use or permit the use of territory in such a manner as to cause injury by fumes in or to the territory of another of the properties or persons therein».[33]

A few decades after the Trail Smelter case, the 'no harm' rule became one of the core principles of global environmental policy. In 1972, the Stockholm Declaration stipulated in Principle 21 that states have a responsibility «to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction».[34] The Rio Declaration in Principle 2 reiterates the 'no harm' principle.[35]

The 'no harm' principle is also used in many international conventions: the 1982 UN Convention of the Law of the Sea (Article 194-2)[36], the Convention on Biological Diversity (Article 3),[37] 1985

---

30 Corfu Channel (UK v. Albania), ICJ Reports 1949, p. 4, (Merits).

31 United States Diplomatic and Consular Staff in Teheran (US v. Iran), 1980 ICJ Reports p. 63, 124 (Judgment), at p. 3.

32 Case Concerning Application of the Convention on the Prevention and Punishement of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), 2007 ICJ Reports 43 (Judgment) at p. 428–450.

33 Trail Smelter Case (United States v. Canada). Arbitral Trib., 3 UN Rep. Int'l Arb. Awards 1905 (1941).

34 See United Nations Conference on the Human Environment, Report of the United Nations Conference on the Human Environment, A/CONF48/14/Rev1 (15–16 June 1972).

35 Report of the United Nations Conference on Environment and Development, Rio de Janeiro, 3–14 June 1992, A/CONF.151/26/Rev.1 (Vol. I), at 3.

36 «States shall take all measures necessary to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment, and that pollution arising from incidents or activities under their jurisdiction or control does not spread beyond the areas where they exercise sovereign rights in accordance with this Convention» (United Nations Convention on the Law of the Sea, supra n. 21).

Convention for the Protection of the Ozone Layer (Article 1), 1967 Outer Space Treaty, 1973 Marine Pollution Convention, 1972 London Duping Convention, and the UN Watercourse Convention (Article 7).[38] Furthermore, the 'no harm' rule was reiterated in a few judgments of the International Court of Justice: the *Legality of the Threat or Use of Nuclear Weapons* [39] and *the Case concerning the Gabčíkovo-Nagymaros Project*.[40] The Budapest Convention on Cybercrime specifies that states have the responsibility to prevent the use of their territories by non-state actors to conduct cyber-attacks against other states.

2. Attribution

State responsibility cannot be established without attribution of the act that would trigger state responsibility. The *Draft Articles* specify that attribution must be established to the state and its organs.

Attribution in Internet cases has technical and legal aspects. On the technical level, it is very difficult to attribute Internet acts, due to the technical architecture of the Internet and the use of various techniques that ensure anonymity, including the use of ToR software, multiple Internet routes, encryption, etc. In addition to technical evidence, there is a need to ensure legal attribution in order to initiate cases based on state responsibility. Typically, legal evidence requires a higher level of certainty than technical evidence.

It is highly demanding to gather sufficient proof to ensure attribution of acts to state organs. Most Internet-related cases remain on the level of 'alleged' attribution. This was the case in the 2007 Denial of Service attack on Estonia's digital infrastructure[41] and the 2014 Stuxnet attack on Iranian nuclear enrichment facilities.[42]

Traditional state responsibility, which requires attribution of acts to state organs, is of very limited use in the digital field, where most activities are conducted by non-state actors. Most Internet infrastructure facilities are owned by private companies and the Internet economy is driven by the private sector. Typically, the need for legal redress in the digital sphere is linked to activities of non-state actors, being individuals or companies. This opens the question of whether a state can

---

37 «States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction» (Convention on Biological Diversity, Rio de Janeiro, 5 June 1992, 1760 U.N.T.S. 79).

38 Article 7 of the 1997 UN Watercourses Convention. The «no harm principle» is also used in other watercourses conventions, see the United Nations Economic Commission for Europe's Water Convention (Article 2.1); the 1994 Danube River Protection Convention (Article 2); and the 1995 Mekong Convention (Article 4).

39 Legality of the Threat or Use of Nuclear Weapons, 1996 ICJ Reports 226 (Advisory Opinion) at 241 et seq. (para. 29).

40 Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), 1997 ICJ Reports, p. 7 (Judgment), at 41 (para. 53).

41 For more information, see: Steve Mansfield-Devine, «Estonia: What Doesn't Kill You Makes You Stronger», 7 Network Security (2012), 12-20; and R. Ottis, «Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective», Proceedings of the 7th European Conference on Information Warfare and Security. Reading: Academic Publishing Limited, 2008, 163–168.

42 For more information, see: Daniel Terdiman, «Stuxnet delivered to Iranian nuclear plant on thumb drive», CNET, 12 April 2012, < http://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-planton-thumb-drive/>.

be held responsible for acts of individual and non-state entities under its jurisdiction according to strict or vicarious responsibility.

The traditional view on attribution for state responsibility is taken by Draft Article 11: «Conduct of persons or a group of persons not acting on behalf of the State shall not be considered as an act of the State under international law».[43] However, the UN Law of the Sea Convention broadens state responsibility to natural and juridical persons under its jurisdiction. Article 139, paragraph 1, specifies that: «States Parties shall have the responsibility to ensure that activities in the Area, whether carried out by States Parties, or State enterprises, or natural or juridical persons which possess the nationality of States Parties or are effectively controlled by them or their nationals, shall be carried out in conformity with this Part...»[44];

State responsibility is further reinforced in Article 235, paragraph 2[45]: «States shall ensure that recourse is available in accordance with their legal systems for prompt and adequate compensation or other relief in respect of damage caused by pollution of the marine environment by natural or juridical persons under their jurisdiction.» Similar approach to state responsibility are used in the Treaty on Principles Governing the Activities in the Exploration and Use of Outer Space of 1967 (article 6)[46]: «States Parties to the Treaty shall bear responsibility for national activities in outer space… whether such activities are carried out by government agencies or by non-governmental entities». Finally, in international jurisprudence, the ICJ ruled in the Namibia case: «Physical control of a territory and not sovereignty or legitimacy of title, is the basis of state liability for acts affecting other states.»[47]

Legal writers have intensively debated the topic of state responsibility for non-state actors under a state's jurisdiction. For example, Ian Brownlie argued that «The State is under a duty to control the activities of private persons within its state territory»[48] and Oppenheim argues for vicarious responsibility for unauthorised acts of the agent of the state and the other legal entities (individuals, companies, etc.).[49]

Alexander Kiss stressed that apart from the ILC *Draft Articles*, which do not hold a State responsible, «this view does not appear to be accepted for environmental matters. The general rule seems rather to be that the State whose territory serves to support the activities causing environmental damage elsewhere or under whose control it occurs is responsible for the resulting harm».[50] Karl Zemanek introduced an economic argument to the discussion on state responsibility for acts by private persons on their territory, by stressing that "the most convincing answer is provided by the fact that the national economy of the State on whose territory the activity takes place benefits from that activity generally, and the government through revenues in particular.» [51]

---

43 International Law Commission, Yearbook of the International Law Commission 1975, Volume II, New York: United Nations, 1976, at 51–61.

44 Art. 139(1) UNCLOS.

45 Art. 235(2) UNCLOS.

46 Art. 24(6) Outer Space Treaty.

47 Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (advisory opinion), 1971 ICJ Reports, p. 16, at 54, para. 118.

48 Brownlie, suppra no. 25, at 163.

49 Robert Jennings & Arthur Watts (eds.), supra n. 28.

50 Alexandre Charles Kiss & Dinah Shelton, International Environmental Law, Leiden 1991, at 353–354.

51 Karl Zemanek, «State Responsibility and Liability», in: W. Lang, H. Neuhold, & K. Zemanek (eds.), Environmental protection and international Law, London 1991, at 195.

This survey of legal cases and academic arguments shows that there are serious attempts in jurisprudence and doctrine to overcome the rather rigid criterion for state responsibility of the *Draft Articles*, and to broaden the coverage of state responsibility to private entities and actors under a state's jurisdiction.[52] There are two major directions in which CyberStan would need to search for state responsibility of DigiLand for acts of non-state actors. Firstly, CyberStan could prove a certain level of control of DigiLand's state organs over the activities of the non-state actors who are behind the cyber attack. Secondly, it can argue for the lack of due diligence of DigiLand in ensuring that its territory is not used against other states.

i. Control over non-state actors by state organs.

Jurisprudence and legal doctrine have developed three main criteria for identifying states' control over non-state entities: effective control, overall control and indirect control.

Firstly, the 'effective control' criterion was introduced by the International Court of Justice (ICJ) in the Nicaragua vs. the United States Case. Although the United States supported and trained rebel fighters against the Nicaraguan government, the ICJ ruled that the United States were not responsible for rebel fighters' actions, since the US did not have «effective control of the military or paramilitary operations in the course of which the alleged violations were committed».[53]. The Tallinn Manual also follows the principle of 'effective control', as it stresses that «mere financing and equipping» is not sufficient for qualifying state support to private actors as 'effective control'.[54] According to this approach, it would not be sufficient for CyberStan to prove that – for example – DigiLand's official networks were used for the attack. In order to request DigiLand's state responsibility, it would need to prove that DigiLand's officials were involved in the operationalisation of the cyber incident.

Secondly, the 'overall control' criterion was introduced by the International Criminal Tribunal for the former Yugoslavia in the case of Prosecutor v Tadic (Appeals Chamber Judgement).[55] It lowered the threshold for state responsibility by specifying that a state is responsible if it has overall control, rather than effective control, over activities of non-state actors. Thus, the support for military groups and other non-state actors would be sufficient for establishing state responsibility. If CyberStan can prove that the organisation from which network the attack came had received grants from the government of DigiLand, it could use this evidence as the basis to develop an argument for state responsibility via the 'overall control' criterion. The main legal battle would be conducted on the question if DigiLand exercised 'due diligence' on matters that could have affected this attack.

Thirdly, according to Graham, the 'indirect responsibility' criterion was used after the 9/11 attacks as the policy basis for attacking the Taliban government of Afghanistan.[56] Although the Taliban did not have effective nor overall control over the al Qaeda terrorist group, they were held responsible for providing a sanctuary for al Qaeda. It is still ambiguous whether the principle of 'indirect responsibility' constitutes a new practice on state responsibility or if it is confined only to

---

[52] The term «individual» is used for natural actors and «entities» for legal actors.

[53] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, 1986 ICJ Reports p. 14, 181.

[54] Michael N. Schmitt (ed.), supra n. 15, at 32–3.

[55] Prosecutor v. Tadić, 1999 ICTY, IT-94-1-A, I.C.T.Y. Appeals Chamber (15 July)(Judgment) at 49.

[56] David E. Graham, «Cyber Threats and the Law of War», 87 J. of National Security: Law & Policy (2010), at 93–4.

the use in specific circumstances, such as in response to the 9/11 terrorist attacks. If it has become a new legal principle, it would introduce the principles of strict responsibility of a state for any act committed by individuals and other entities in its territory. Using this criterion would lead towards pure strict responsibility, which considers only the fact that an attack originated from the other territory.

Thus, the most realistic legal ground for the case could be found in the 'overall control' criterion. If CyberStan's lawyers cannot prove DigiLand's overall control over its non-state actors who committed the cyberattack, they can build the case around proving that DigiLand did not use 'due diligence' in preventing the attack.

ii. Due diligence[57]

While states cannot be held responsible for every act of individuals and non-state entities in their territory, they can make due diligence steps in order to prevent the use of their territory against individuals and entities in other states (based on the 'no harm principle').

In field of human rights, due diligence tests have been used to evaluate whether states are responsible for breaches of human rights regulations by private entities under their jurisdiction. For example, in the case *Velásquez Rodríguez v Honduras*[58], the Inter-American Court of Human Rights ruled that a state can be held responsible for violations by private actors if the state failed to exercise 'due diligence' to prevent and respond to the violations. The Court indicates that the state must

> *take* reasonable steps *to prevent human rights violations and to use the means at its disposal to carry out a* serious *investigation of violations committed within its jurisdiction, to identify those responsible, to impose the appropriate punishment and to ensure the victim adequate compensation.*[59]

The due diligence principle was also used in *The Asian Agricultural Products Ltd (AAPL) v Sri Lanka*. The judgement ruled that Sri Lanka could not be held responsible for the destruction caused by the Tamil Tigers, but it could be held responsible for not taking due diligence to protect destroyed installations.[60]

The application of the concept of 'due diligence' to cyber matters could also be inspired by solutions in international diplomatic law, where a state is obliged to take 'all appropriate' steps in order to protect the embassies of foreign countries. The omission to take these steps was one of the legal bases of the ICJ judgment in the case of *United States Diplomatic and Consular Staff in Teheran* (1980).[61]

---

[57] For a discussion on «due diligence» in cyberspace, consult Katharina Ziolkowski, «Rights and Obligations of States in Cyberspace», in: Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, Talinn 2013, pp. 165–170.

[58] *Velasquez Rodriguez Case,* Judgment of July 29, 1988, Inter-Am. Ct. H. R. (Ser. C) No. 4 (1988).

[59] *Ibid*, at 93.

[60] *Asian Agricultural Products Ltd. v. Republic of Sri Lanka*, 1990 ICSID Case No. ARB/87/3 (27 June).

[61] United States Diplomatic and Consular Staff in Teheran (US v. Iran), supra n. 30.

Due diligence steps could include measures such as the adoption of strategy and legislation against cybercrime. Thus, while CyberStan cannot request DigiLand's responsibility for the concrete attack, it can base its claim on DigiLand's responsibility to take all necessary measures to prevent such an attack.

Graham indicates the following steps to determine due diligence:

- To enact stringent criminal laws against the commission of international cyber attacks from within national boundaries.
- To conduct meaningful, detailed investigations into cyber attacks.
- To prosecute those who have engaged in these attacks.
- To cooperate with the victim states' own investigations and prosecutions of those responsible for the attacks.[62]

'Due diligence' is flexible enough to adjust to new technological developments and the way in which the Internet is (mis)used. Due diligence criteria and mechanisms are likely to develop through state practice in dealing with cyber incidents, which could be the basis for norm creation through instant customary law.

C. Damage and reparation

In requesting state responsibility, CyberStan will have to prove damage and loss, which will also form the basis for reparation. Given the ambitious role of cyber in modern life, damage and loss by cyber activities could be very diverse, ranging from direct effects on the attacked object (e.g. damage to the power grid) to damages affecting the health and well-being of the broader population. The starting point for dealing with questions of damage and reparation should be the Draft Articles, which identifies three types of reparations.

Firstly, Article 35 indicates restitution as a way «….to re-establish the situation which existed before the wrongful act was committed… ». Restitution could be used if it is possible and proportional. In digital cases, restitution could be used only if the cyberattack has triggered physical damage, which is not frequent in the digital field.

Secondly, if restitution cannot be used, the Article 36 specifies compensation as '…financially assessable damage including loss of profits…'. In our case, it is most likely that CyberStan will seek compensation for damage triggered by the cyber-attack. The exact level of requested compensation would depend on establishing a causal link between the cyberattack and the resulting damage.

The third possibility is satisfaction, which, according to Article 37, '… may consist in an acknowledgement of the breach, an expression of regret, a formal apology or another appropriate modality.' Satisfaction as reparation approach could be used in state responsibility in digital cases. In sum, possibilities for reparation in digital cases will depend on the type of damage that has resulted from the cyberattacks. Typically, restitution will rarely be used, leaving the other two mechanisms of compensation or satisfaction.

[62] Graham, supra n. 55, at 93–94.

III. Conclusion

As our analysis shows, CyberStan is unlikely to find a legal basis to request state responsibility of DigiLand for the cyberattack. Namely, the objective responsibility, as is outlined in the 2001 Draft Articles on State Responsibility and supported by the 2015 UN GGE Report, is too restrictive to be applied to cyber cases. Out of two core elements for objective state responsibility – breach of rules and attribution of action to state organs – CyberStan may have an easier case of proving a breach of the 'no harm' rule, which requires a state not to allow the use of its territory in ways that are harmful to other states. However, the attribution of the cyberattack to the state organs of DigiLand poses high burden to prove.

The limited usability of objective responsibility in digital issues is likely to trigger alternative solutions for state responsibility, similar to environmental law and other specialised fields that have faced similar limitations. One of the main challenges will be to deal with the responsibility of non-state actors, which are the main players in the cyber-field. This challenge could be addressed by further developing the 'no harm' principle, which should prevent any use of a state's territory, including by non-state actors, for cyber-attacks against other states.

However, the complexity of cyber activities will make it difficult for states to guarantee the application of the 'no harm' principle by ensuring that no cyber activity under their jurisdiction will harm entities beyond their national borders. A potential solution could be identified in 'due diligence' requirements, which would require states to take all reasonable measures to prevent cyberattacks against other states by, among other measures, introducing law against cyber-crime activities, participating in international cooperation, prosecuting perpetrators of cyberattacks, etc.

The concept of state responsibility in the digital field, which is still in an early stage, is likely to emerge through state practice, decisions of international courts and policy processes such as UN GGE.

State responsibility is one of the ways for legal redress in digital cases beyond national borders. Together with other mechanisms from international private law for dealing with contract and torts, international criminal law for addressing cybercrime and alternative dispute resolutions, state responsibility should contribute towards ensuring legal stability and the rule of law in the modern digitally-driven society.