Securing Cyber Space:
The Obligation of States to Prevent Harmful International Cyber Operations

Irène Couzigou*

Senior lecturer in Law
Law School
University of Aberdeen
High Street
AB243UB Aberdeen
E-mail: irene.couzigou@abdn.ac.uk
Tel.: 01224 272437

World count: 10,871 words, excluding the abstract, keywords and references.

* Senior Lecturer at the University of Aberdeen Law School (Email: irene.couzigou@abdn.ac.uk). The drafting of the paper was finalised on 1st December 2017.

Abstract

The paper argues that the obligation of States to prevent harmful international activities perpetrated within their territory, or any other area under their exclusive control, applies to activities conducted in cyber space. Thus, a State is bound by an obligation to prevent detrimental cyber conduct committed from its territory or transiting through its territory, or any other area under its exclusive control, when it knows or should have known of the conduct, when the conduct contradicts the rights of another State, and when it may cause or is causing serious harm. Where a State is aware or should have been aware of the misuse of its territorial cyber infrastructure, the State must attempt to prevent or to react to the harmful transboundary operation, applying all reasonable measures. The content of the obligation of due diligence to prevent damaging cross-border cyber activities depends on the economic, financial and human resources of the State. The paper concludes that the obligation to preclude harmful international cyber operations constitutes only a first step in securing information and communication technology and should be sustained and improved by the introduction of a treaty on cyber security.

Keywords: States, Obligation to Prevent, Harmful International Cyber Operations

1. Introduction

States and non-State actors have become increasingly dependent on computers and the networks that connect them for the performance of many of their functions. As the reliance on digital technology grows, the impact of failure in networks and information systems and the opportunities for those who seek to compromise those systems increase. Cyber technology is likely to become an essential international offensive tool, in particular for non-State actors such as hackers, criminal organisations or terrorists. It is even more the case that malicious transboundary cyber operations can be carried out quite easily and with a low risk of detection: an access to a computer and an Internet connection wherever in the world are sufficient. Harmful cyber activities launched from

one State with negative consequences on other States are increasing in both frequency and potency. Thus, recent events, such as the massive ransomware cyber attack on nearly 100 countries, including on British hospitals, in spring 2017, have drawn attention to the increasing risk of harmful transboundary cyber operations against governments and/or private actors (Wong and Solon 2017).

Harmful international cyber operations can be classified into different types. First, a harmful transboundary cyber activity might be designated as a cyber crime, an act perpetrated with a criminal intent without any political motivation such as an electronic related credit card fraud or an online bank account manipulation. A detrimental cross-border cyber interference can also be cyber espionage. It then refers to an intrusion into the network based in another State with the purpose of gaining confidential information of the State's governmental services or of private entities in the State. A damaging international cyber operation can also be identified as a cyber attack. It is a deliberate action, politically or strategically motivated, taken through the use of computer networks to disrupt, manipulate, or destroy information that resides in the target information system (Cartwright 2010). A cyber attack may produce effects that are only internal to a computer network, for instance in limiting the ability for electronic communication. It may also produce effects that are external, by causing harm to connected facilities, for example in crashing planes, derailing trains or disrupting electricity supply. Here, the targeted computer network is the conduit for an attack on a physical target. In practice, it may be difficult to classify a harmful international cyber operation as appertaining to one of these three categories described above and some cyber activities may incorporate elements of all three categories (Henriksen 2015, 330). Finally, a harmful international cyber interference can be an accident and not an intentional action. Indeed, a digital information system can be disrupted by human mistakes, natural events, or technical failures. The paper will adopt a broad understanding of harmful international cyber operations. They are here defined as activities perpetrated within the territory of a State through the use of computer networks that intrude, disrupt, manipulate or destroy information in the target computer information system and that cause an international harm, physical or not, on the territory of another State (or of other States).

A malicious international cyber operation may be perpetrated by a State. Where a harmful cyber activity can be traced back to a government's computer, the activity will be attributed to the State to which the government belongs, unless the State provides a

convincing explanation that the computer was externally used (Walter 2015a, 72). A cyber conduct may also be committed by a non-State actor. A State is responsible for the conduct of a non-State actor that causes harm to another State only if the conduct can be attributed to the State. Under international law, the cyber operation of a non-State actor can be attributed to a State especially in the following three circumstances. When the cyber act is performed by a person or entity empowered by the State to exercise governmental authority (Art. 5 International Law Commission (ILC) Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries 2001 *Official Records of the General Assembly,* Fifty-sixth session, Supplement No 10 (A/56/10), 44).[1] For instance, this can occur if a State charges a private company with elements of authority normally associated with the government, and asks it to perpetrate a cyber operation. Furthermore, a cyber operation is considered as an act of a State if the State explicitly acknowledges and adopts the operation as its own (Art. 11 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries 2001 *Official Records of the General Assembly,* Fifty-sixth session, Supplement No 10 (A/56/10), 45). The third and most usual situation in which a cyber activity may be attributed to a State is where the acting entity operated under the instructions, direction or control of a State, for example when a State hires an individual or an organisation to conduct a cyber attack (Art. 8 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries 2001 *Official Records of the General Assembly,* Fifty-sixth session, Supplement No 10 (A/56/10), 45). The degree of direction or control must be high, which means that the State should have effectively directed or controlled the specific cyber activity. This should be assessed on a case-by-case basis (ICJ *Case concerning Military and Paramilitary in and against Nicaragua* (*Nicaragua v. United States*) 1986 *ICJ Reports*, para. 115).

Holding States responsible for harmful cyber conduct perpetrated by non-State actors, through the implementation of the attribution criteria, is unlikely to occur. Indeed, to establish the requisite link between the State and the non-State actor, the non-State actor that committed the cyber conduct must first be identified. The author of a cyber operation may claim responsibility for it. For instance, a group that commits a cyber attack may claim credit for it in a message or videotape posted online. The style of a cyber attack may also help to

[1] The International Law Commission (ILC) is a United Nations (UN) organ whose aim is to prepare treaties' drafts codifying the customary rules of a particular field of international law. It has prepared the Draft Articles on Responsibility of States for Internationally Wrongful Acts. This text has been extensively cited in State practice as well as by international courts and tribunals, so that most of its provisions can be considered as an authoritative statement of the customary international law on State responsibility.

identify its perpetrator (Brenner 2007, 408). Otherwise, identification of a cyber perpetrator is a complicated exercise. First the cyber operation must be traced back to its source. Second, the individual who operated the computer must also be identified or his affiliation determined. The Internet protocol (IP) address assigned to every computer connected to the Internet does not reveal the specific identity of the computer, but only its general geographic location. Furthermore, the recourse to anonymising techniques like Botnets and anonymising software such as Virtual Private Networks (VPNs) or the Onion Router (Tor) reroutes harmful cyber operations through the cyber infrastructure of other States. This process assigned different IP addresses to the operations, showing to the victims that they were conducted from computers in geographical locations different from their original source (Buchan 2016, 430). With the improvement of digital technology, cyber tracing is becoming possible but remains very difficult. To trace back an international cyber operation to its true point of origin will often necessitate assistance from governmental and other entities in the State in which the computer was used or from third parties. Months may be necessary before international assistance is obtained and the identification of the cyber perpetrator established (Brenner 2007, 420).

The responsibility of States may be engaged not only for harmful international cyber operations attributed to them, but for their failure to prevent those cyber operations from occurring. A State may incur responsibility where it fails to take positive action or takes action other than the one required in relation to a harmful international conduct of a non-State actor operating within its territory or any other area under its exclusive control. Indeed, in accordance with the International Court of Justice (ICJ) in the *Corfu Channel case* of 1949, every State is under an obligation 'not to allow knowingly its territory to be used for acts contrary to the rights of other States' (ICJ *The Corfu Channel Case (United Kingdom v. Albania)* 1949 *ICJ Reports*, 22). It is a general principle of law that States have a positive obligation to prevent their territory, or more generally any other area under their exclusive control, to be used for the perpetration of activities that inflict damage on persons and objects protected by the territorial sovereignty of another State (ICJ *Case concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay)* 2010 *ICJ Reports*, para. 101).[2]

[2] General principles of law are the third source of international law, along with treaties and customary international law, as provided by the Statute of the ICJ.

The obligation to protect the rights of other States is the corollary of the right to exclusive jurisdiction of each State on its territory or any other space under its exclusive control (*Island of Palmas Case (Netherlands v. USA)* 1928 *UN Reports of International Arbitral Awards* II, 839). If the obligation to prevent harmful transboundary conduct perpetrated from a State's territory or any other area under its exclusive control is applicable to the cyber sphere, then it will protect States better from damaging cross-border cyber operations than the application of the attribution criteria. Indeed, the obligation of a State to prevent harmful international cyber conduct committed from its territory or under any other space under its effective control does not require to specifically identify the perpetrator of the cyber conduct and to attribute it to the territorial State. It is enough to trace the location of the computer from which the cyber act is perpetrated. Under international law, there is a general agreement that the more grave the charge the more confidence there must be in the evidence (Separate Opinion of Judge Higgins in *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)* 2003 *ICJ Reports*, paras 30-39). International law practice indicates that there should be strong evidence that a harmful cyber operation originates from one particular State before engaging its responsibility for failure to protect the rights of another State. However, even if the required standard of proof is high, cyber tracing to a computer is much easier than cyber tracing to the individual who operates the computer.

Chapter 2 of this paper argues that the obligation of a State to prevent harmful international activities perpetrated from its territory or any other area under its exclusive control applies in cyber space. Chapter 3 outlines the requirements for the implementation of the obligation to preclude damaging transboundary cyber operations. Chapter 4 analyses the scope and content of that obligation. To inform the obligation to prevent the misuse of a State's territorial cyber infrastructure, reference will be made to general international law and to different fields of international law where States have an obligation to prevent a conduct or to act, such as the law of the environment, the law of the sea, and international human rights law. Finally, in Chapter 5 we apply the results of this article to recent cases of cross-border harmful cyber activities; we conclude that the obligation of a State to prevent damaging cyber conduct against the rights of another State ensures only a limited international cyber security and should be upgraded by a treaty on cyber security.

2. Implementation of the Obligation to Prevent International Harm to Cyber Space

In the early to mid-1990s, it was argued that cyber space was an a-territorial and borderless environment different from the physical and bonded spaces that are subject to sovereign claims. Cyber space was considered to be an area *sui generis,* outside of both State authority and regulation. As explained by some, the cyber domain could not be regulated by laws based on geographical location but had to have its own legal system based on self-regulation (Johnson and Post 1996, 1378-1395).

Cyber space can be defined as:

> a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies (Kuehl 2009, 28).

In practice, electronic information needs physical elements such as computers, routers, servers, and cables that are territorially based. Thus, States do exercise their territorial jurisdiction over those aspects of cyber space which are supported by physical infrastructure based in their territory - that encompasses the State's land area, its internal waters, its national airspace, when applicable its territorial sea and its archipelagic waters - or an area under their exclusive control - e.g. a territorial area occupied by the State. The digital world does not constitute a new form of 'outer space' where no State could exercise its jurisdiction but is subject to the national law of the competent State (Pirker 2013, 193-194). States have, in fact, regularly asserted their jurisdiction over cyber activities conducted on their territory (von Heinegg 2013, 126).

Hence, 'international norms and principles that flow from sovereignty apply to State conduct of ICT [Information and Communications Technology]-related activities, and to their jurisdiction over ICT infrastructure within their territory' (UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, Report 2013 UN Doc. A/68/98, para. 20). In particular, the obligation upon States to prevent transboundary harm perpetrated within their territory or any other area under their exclusive control applies to harmful international conduct committed with the cyber infrastructure located in their territory (UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, Report 2015

UN Doc. A/70/174, para. 17(b)). This was recognised by States. Thus, most of the States of the United Nations (UN) General Assembly, called upon States to prevent their territories from being used as a safe haven from which to launch cyber attacks, and to cooperate in the investigation and prosecution of such attacks (Resolution on Combating the criminal misuse of information technologies 2001 UN Doc. A/RES/55/63, Art. 1). The obligation to prevent harmful international operations also applies with regard to those operations launched from cyber infrastructure that is outside a State's territory but is nevertheless under the exclusive control of the State, for instance in a military installation in a foreign country, in a platform on the high seas or in international airspace, or in diplomatic premises (Schmitt (ed.) 2017, 33). According to Rule 6 of the Tallinn Manual 2,

> '[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States' (Schmitt (ed) 2017, 30).[3]

Furthermore, the obligation to prevent detrimental transboundary conduct applies to harmful international cyber conduct that is rerouted through the cyber infrastructure of a State. In the *Nicaragua* case, the ICJ held that Nicaragua had to prevent its territory from being used as a trafficking route for arms for insurgents in El Salvador. It acknowledged an obligation of a State to prevent the transit of harmful activity through its territory (ICJ *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)* 1986 *ICJ Reports*, para. 157). Therefore, by analogy, the obligation to prevent harmful international cyber activity does not only apply to the State from where the activity is launched, but also to the State where the activity may transit (Schmitt (ed.) 2017, 33).

3. Requirements for the Implementation of the Obligation to Prevent Harmful International Cyber Operations

3.1. Current or Constructive Knowledge of the Cyber Operation

Knowledge is the most important element of the obligation to prevent harmful international conduct from a State's territory. Once a State has knowledge of a

[3] The so-called Tallinn Manual 2, initiated by the North Atlantic Treaty Organization Cooperative Cyber Defense Centre Excellence, was drafted by an international group of international law experts and aimed to producing a non-binding document applying existing international law to cyber space in peacetime.

detrimental international act, the State is bound by the obligation to use its capacity to prevent or, if the act is already underway, to stop it (ICJ *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports* 2007, para. 431). States cannot have knowledge of all what is happening on their territory or in any other area under their exclusive control. The ICJ held that 'it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known' what was happening (ICJ *The Corfu Channel Case (United Kingdom v. Albania)* 1949 *ICJ Reports*, 18; European Court of Human Rights, *Osman v United Kingdom* 1998 ECHR 1998-VIII., para. 116). It is not because a harmful international cyber conduct emanates from a State's territory or transits through a State's territory that the State is automatically assumed to have known of it.

Since a State exercises exclusive control over its territory, it may be difficult for the victim State to directly prove the actual knowledge of the harmful international act by the territorial State. Thus, the ICJ has adopted a quite lenient standard of proof. The victim State does not need to furnish direct proof that the host State knew that a damaging operation was taking place on its territory or any other area under its exclusive control. 'The proof may be drawn from interferences of fact, provided that they leave *no room* for reasonable doubt' (ICJ *The Corfu Channel Case (United Kingdom v. Albania)* 1949 *ICJ Reports*, 18). There must be a 'series of facts linked together and leading logically to a single conclusion' (ICJ *The Corfu Channel case (United Kingdom v. Albania)* 1949 *ICJ Reports*, 18). A State should be seen has having actual knowledge if, for instance, its intelligence agencies have detected a malicious cyber operation launched from its territory or when another State or institution puts the State on notice on such an operation.

The obligation to prevent is also activated when the State was in fact unaware of the harmful cyber conduct, but objectively should have known of the conduct. As explained by the ICJ in the *Corfu Channel* judgment:

> [i]t is true, as international practice shows, that a State on whose territory or in whose waters an act contrary to international law has occurred, may be called upon to give an explanation. It is also true that that State cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the

act and its authors (ICJ *The Corfu Channel Case (United Kingdom v. Albania)* 1949 *ICJ Reports*, 18).

More precisely, in the *Genocide* judgment, the ICJ stated that

> to incur responsibility ... it is enough that the State was aware, or should normally have been aware, of the serious danger that acts of genocide would be committed' (ICJ *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports*, para. 432).

The question is whether it is reasonable to expect that the State should have had knowledge of harmful international conduct in the particular circumstances (Buchan 2016, 441). Thus, in the cyber context, a State should be presumed to have knowledge of a damaging transboundary cyber operation when the State intensively guards its cyber infrastructure; when malwares and other vulnerabilities infecting the State's cyber infrastructure are widely reported; when the cyber operation involves a cyber activity that is generally always detected such as a Distributed Denial of Service (DDoS) attack that significantly increases bandwidth usage compared to normal usage; or when the State's cyber infrastructure has already been exploited for the purpose of conducting a series of similar offensive cyber operations (Pirker 2013, 205-206).

The obligation to prevent harmful international cyber conduct can apply more easily to the State from which the conduct was performed than to those States through which the conduct may be transmitted. Indeed, identification of such conduct across the cyber infrastructure on a State's territory is complicated. However, technological tracing capabilities are improving. Moreover, in some circumstances, the presumption can be made that the State was aware or ought to have been aware of the transit through its territorial cyber infrastructure of a damaging cyber activity. For instance, repeated or continuous cyber attacks through the domestic network of a State can serve as evidence that the transit State knew or should have known of the attacks. Thus, if a State knows or should have known of a harmful cyber operation traveling through its territory, it is bound by an obligation to attempt to terminate it (Schmitt 2015, 73; Shackelford, Russell and Kuehn 2016, 20).

Does the obligation of a State to prevent harmful conduct perpetrated from, or transiting through, its territory encompass an obligation to monitor what is happening on its territory or any other area under its exclusive control? In its *Nuclear Weapons* advisory

opinion of 1996, the ICJ seems to have abandoned the requirement of knowledge by States of the harmful activities of non-State actors on their territory with respect to serious environmental damage. There, States have a general obligation 'to ensure that activities within their jurisdiction and control respect the environment of other States' (ICJ *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion 1996 *ICJ Reports*, para. 29). This case-law was specified in the *Pulp Mills* case, where the ICJ stated: '[a] State is thus obliged to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State' (ICJ *Case concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay)* 2010 *ICJ Reports*, para. 101). This broad obligation of prevention has been asserted by the Stockholm Declaration (Principe 21 Stockholm Declaration of the United Nations Conference on the Human Environment 1972 UN Doc. A/CONF.48/14/Rev.1, 5) and the Rio Declaration (Principle 2 Rio Declaration on Environment and Development 1992 UN Doc. A/CONF 151/26/Rev 1 (Vol I), Annex I 3). It was also included in an extensive number of other declarations and in international treaties (Koivurora 2017, 4), and was acknowledged by the ILC:'[t]he State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof' (Art. 3 ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities 2001 Report on the Work of its 53rd Session UN Doc. A/56/10, 153). Therefore, States have the obligation to ensure that no activity performed on their territory causes severe damage to the environment of other States (Dörr 2015, 91-92). This entails the obligation to monitor private activities that risk seriously damaging the environment of other States (ICJ *Case concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay)* 2010 *ICJ Reports*, para. 197). The obligation to monitor is justified by the higher risk of significant potential damage. In practice, a State could control large construction projects or industrials plants that may produce a hazard to neighbouring States. The standard of care applied to potentially dangerous physical activities for the environment cannot be translated to cyber activities. Indeed, it is not possible to classify cyber operations to the degree of danger they pose. Every computer could be the instrument of serious harmful damage. A State can however not be expected to monitor the use of every private computer with an access to the Internet. This would be practically impossible and in contradiction with international human rights, in particular the freedom of expression and the right to privacy (Walter 2015b, 688).

Under general international law, States should be able to govern their territory and to ensure the fulfilment of their international obligations (Crawford 2006, 59 and 62). This entails an obligation to get an overall overview of what is happening on their territory. Thus, in respect to cyber activities conducted from their territory or transiting through their territory or any other area under their exclusive control, States should apply a certain standard of care. The level of this standard should be lower than the one applied to activities that may have a serious transboundary polluting effect (Dörr 2015, 95.). A State should pursue 'reasonable efforts ... to inform itself' of transboundary disruptions on the Internet (Council of Europe Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet, 2010, para 73. http://www.umic.pt/images/stories/publicacoes5/MC-S-CI%20Interim%20Report.pdf). The degree of control to be exercised by States over their cyber infrastructure should be higher for technologically developed States. It should also be higher for highly connected States whose cyber infrastructure is more likely to be used for harmful cyber operations against other States. In any case, the obligation of monitoring should be done in conformity with international law, in particular with international human rights law (Dörr 2015, 95; Bannelier-Christakis 2014, 31). As a general statement, the ICJ has held that in exercising its obligation to prevent - in that case, genocide - 'it is clear that every State may only act within the limits permitted by international law' (ICJ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports*, para. 430).

3.2. Contradiction with the Rights of another State

In conformity with the *Corfu Channel case,* a State should not let its territory to be used 'for acts contrary to the rights of other States' (ICJ *The Corfu Channel Case (United Kingdom v. Albania)* 1949 *ICJ Reports*, 22). The expression 'contrary to the rights' refers to acts that breach an international obligation owed to the victim State. Thus, the obligation to prevent harmful international conduct, including harmful international cyber conduct, applies only in relation to an act that, if committed by the territorial or transit State itself, would amount to an internationally wrongful act of that State (Schmitt (ed) 2017, 34-36). Indeed, if a conduct by State A or a non-State actor perpetrated on, or

transiting through, the territory of State B and harming a State C were not unlawful if committed by the territorial or transit State B, it would be incongruent to impose an obligation on State B to prevent or stop the conduct (Schmitt (ed) 2017, 34-36). For instance, a State knows of a cyber attack perpetrated by a terrorist organisation within its territory, aiming to interfering with the air traffic control system of another State. The territorial State infringes its obligation to prevent malicious cross-border activities if it does not try to terminate the attack. Indeed, such an attack would violate the territorial integrity and thus the sovereignty of the target State if it had been conducted by the territorial State itself. Now, consider the situation where a State is aware of a malware launched by another State that travels through its territory and that disrupts the electronic system used for a national election in a third State and thus manipulates the electoral result. The transit State violates its obligation of prevention if it does not attempt to stop the cyber operation. Indeed, such an operation would violate the customary principle of non-intervention into the domestic affairs of a State if it were perpetrated by the transit State (ICJ *Case concerning Military and Paramilitary in and against Nicaragua* (*Nicaragua v. United States*) *ICJ Reports* 1986, para. 202).[4]

3.3. Serious Prospective or Current Harm

It is a general principle of law that where a State violates an international legal norm, responsibility attaches regardless of whether damage is caused (Commentary on Art. 2 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries 2001 *Official Records of the General Assembly,* Fifty-sixth session, Supplement No 10 (A/56/10), 73 para. 9). The breach of the international legal obligation itself provides sufficient grounds for invoking the responsibility of the State. There are exceptions to this general principle. A primary obligation may stipulate that responsibility attaches to the violation of an obligation only where serious damage occurs.

[4] The principle of non-intervention is a corollary of a State's sovereignty that is understood as the exercise of full and exclusive authority over the State's territory to the exclusion of any other authority. 'A prohibited intervention must accordingly be one bearing on matters in which each State is permitted…to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices.' ICJ *Case concerning Military and Paramilitary in and against Nicaragua (Nicaragua v. United States) ICJ Reports* 1986, para 202.

In the *Corfu Channel* case, the ICJ did not seem to require that damage must exist for the State responsibility to be engaged. It is the violation of the obligation to prevent harmful action against another State that gives rise to the responsibility of the territorial State, regardless of whether damage is caused. In the *Trail Smelter* case, however, the arbitral tribunal hold that the obligation of prevention is breached only where there is a damage of 'serious consequence' to the victim State (*Trail Smelter Case (United States v. Canada)* 1941 UN *Reports of International Arbitral Awards* III, 1965). Similarly, for the ILC, a State has an obligation to prevent related to 'significant transboundary harm' (Article 1 ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities 2001, Report on the Work of its 53rd Session UN Doc. A/56/10, 149). The Tallinn Manual 2 adopts the same view and explains that the obligation to prevent harmful international cyber operations encompasses activities resulting 'in serious adverse consequences' (Schmitt (ed) 2017, 37). Damage here does not only refer to physical damage on objects or persons but includes damage to computer systems or networks that produce severe consequences such as where a network sustaining a critical national infrastructure is disabled (Schmitt (ed) 2017, 37-38). Thus, the obligation to prevent transboundary harmful cyber operations applies only if the prospective or current harm rises 'to such a level that it becomes a legitimate concern in intra-State relations' and is more than 'mere irritation or inconvenience' (Schmitt 2015, 76. See also Shackelford, Russell and Kuehn 2016, 11). Indeed, many harmful transboundary cyber activities cause no damage or only minor inconvenience to another State, such as website defacement or the temporary minor denial of non-critical service. The obligation of prevention should not encompass an obligation to mount comprehensive defences against all possible harmful international cyber operations but should be based on a relationship between cost and outcome. It remains up to international State practice to specify the threshold of harm at which the obligation of prevention of harmful transboundary conduct applies in cyber space.

4. Scope and Content of the Obligation to Prevent Harmful International Cyber Operations

4.1. An Obligation to Act

Once a State knows or should have known of a cyber operation that will be mounted or will transit through its territory and that will affect the rights of another State as well as cause serious adverse consequences to it, the State must attempt to prevent the operation. As held by the ICJ, 'a State's obligation to prevent, and the corresponding duty to act, arise at the instant the State learns of, or should normally have learned of, the existence of a serious risk that genocide will be committed' (ICJ *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports*, para. 431). Thus, as soon as a State has reliable knowledge that a harmful international cyber activity will be carried out from its territory or will travel through its territory or any other area under its exclusive control, it is bound by an obligation to prevent it (Schmitt (ed.) 2017, 43-44). Such would be the case if the intelligence services of a State were to discover that a terrorist organisation had installed destructive malware in the gas pipeline control system of another State that it is about to activate. A *fortiori*, if a State is aware or should have been aware of a cyber conduct that is perpetrated from its territory or is transiting through its territory or any other space under its exclusive control, that is contrary to the rights of another State and is giving rise to serious damage, the State is bound by an obligation to terminate the conduct.

The precise content of the obligation to prevent harmful transboundary conduct, including harmful transboundary cyber conduct, is determined according to what is reasonable in the specific context. The question is whether the State has taken all reasonable measures in the circumstances to prevent or, if the operation is already underway, to stop a harmful international operation. The obligation to prevent damageable transboundary conduct is an obligation of due diligence that can be defined as an obligation, in the particular circumstances, to exercise best possible efforts to try to prevent the conduct from happening or to terminate the conduct if it is already ongoing (International Tribunal for the Law of the Sea (ITLOS), *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion 2011 *ITLOS Reports*, para. 110). A State should do what can 'be reasonably expected' of it (European Court of Human Rights *Osman v United Kingdom* 1998, para. 116). Thus, the obligation to prevent harmful international cyber activities depends on the specific context and has an elastic nature. The assessment as to whether the obligation to prevent has been complied with is necessarily subjective (Kolb 2015,

116). If a damaging transboundary cyber operation is about to be mounted or is already launched from computers located in different States, then each of those States must attempt to prevent or terminate the attack (similarly: ICJ *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports*, para. 430).

Determining whether a State acted reasonably in addressing a threat or, an occurrence, of a harmful cyber conduct requires consideration of a number of factors, primarily the adoption of all available means by the State (ICJ *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports*, para. 430). It is worth noting that the majority of cyber space is owned and operated by private companies. Thus, the State will often have to request from private actors operating on its territory to take the necessary action to prevent or terminate detrimental international cyber conduct. A State is required to take only those measures that are 'reasonably available' or 'within its power' (ICJ *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports*, para. 430). Therefore, to assess whether a State complies with its obligation of due diligence, an identification of its financial, technical and human resources is necessary. As hold by the International Centre for Settlement of Investment Disputes, 'tribunals will likely consider the state's level of development and stability as relevant circumstance in determining where there has been due diligence' (International Centre for Settlement of Investment Disputes, *Pantechniki S.A. Contractors & Engineers (Greece) v. The Republic of Albania*, Case No. ARB/07/21, Award 2009, para. 81. https://www.italaw.com/documents/PantechnikiAward.pdf). For the ILC, 'the degree of care expected of a State with a well-developed economy and human and material resources and with highly evolved systems and structures of governance is different from States which are not so well placed.' (Commentary on Art. 3 para. 17 ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities 2001 Report on the Work of its 53rd Session UN Doc. A/56/10, 155).

In consequence, '[t]he due diligence standard ... varies in many contexts on the basis of common but differentiated responsibilities' (International Law Association, *Study Group on Due Diligence in International Law*, First Report 2014, 27. http://www.ila-hq.org/index.php/study-groups). It is common because applying to all States but it is

differentiated because States have unequal technological levels. Technologically developed States are required to do more to counter, or to react to, harmful transboundary cyber activities emanating from their territory or transiting through their territory than States with less technological capacity. Indeed, technologically advanced States are more capable of preventing or terminating harmful cyber conduct than other States. They have better technical and financial tools at their disposal, and they exercise better control over their territorial cyber infrastructure (Schmitt (ed.) 2017, 47; Buchan 2016, 444). Thus, they possess sophisticated cyber tracing methods enabling them to identify the perpetrators of harmful cyber activities; they can better decipher computer codes to determine whether they are infected with malwares; they can hire a private Internet company to help them stopping complex and dynamic cyber attacks. To give an example, if a technologically advanced State is informed by the target State that hostile cyber operations are emanating from IP addresses that have been allocated to the territorial State, it is reasonable to expect that the territorial State blocks those IP addresses. Logically, the higher degree of care imposed on advanced States requires them to keep abreast of technological advancements in the prevention of damaging international cyber activities (Art. 3 para. 11 ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities Commentary on 2001 Report on the Work of its 53rd Session UN Doc. A/56/10, 154).

Other factors in establishing whether a State acted reasonably in light of the circumstances are both the probability and the magnitude of the harm that could be caused, or is caused, by the harmful international cyber operation. According to the ILC, '[t]he standard of due diligence against which the conduct of the State of origin should be examined is that which is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance' (Art. 3 para. 11 ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities Commentary 2001 Report on the Work of its 53rd Session UN Doc. A/56/10, 154). 'The standard of due diligence has to be more severe for the riskier activities' whose occurrence is very likely (ITLOS, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion 2011 *ITLOS Report*, para. 117). A State will have to dedicate more of its resources to prevent a transboundary cyber activity if there is a great likelihood that a significant harm will happen (International Law Association, *Study Group on Due Diligence in International Law*, First Report 2014, 26.

http://www.ila-hq.org/index.php/study-groups). *A fortiori,* a State will have to adopt all means at its disposal to react to an international cyber conduct that is already underway and is going to cause severe damage. For instance, the territorial State is aware of the launch of a malware that will disable, or is in the process of disabling, a critical national infrastructure in another State, such as energy or water supply, transport or health services, and in so doing put the life of people at risk. The State cannot identify the cyber attack's signature. Giving the consequences of the attack on the victim State, the territorial State should shut down its computer network entirely.

The reaction of the State may have negative effects on that State, the target State or even third-parties countries. The balance must be made between the nature, scale, and scope of the potential harm to the territorial (or transit) State and the harm to the victim State in order to establish whether the contemplated action considered is necessary and proportional (Schmitt (ed.) 2017, 49-50; Kolb 2015, 126). For instance, a large botnet is used to conduct a DDoS operation against the cyber infrastructure of another State. The only possibility to terminate the operation would be by taking its network offline. Doing so would negatively affect its own activities on the network, including critical national services, and would thus be disproportionate (Schmitt (ed.) 2017, 49-50). Furthermore, the means to which a State has recourse to implement its obligation of due diligence must be compatible with international law, especially international human rights law such as freedom of expression, the right to privacy and the right to property (Kolb 2015, 121).

When a State is technologically unable to prevent harmful international cyber conduct, it must notify and warn the State that is likely to be the victim of the conduct. It must then share any information related to the known or foreseeable harm (Dörr 2015, 97-98; Shackelford, Russell and Kuehn 2016, 9). In the *Corfu Channel* case, the ICJ considered Albania under an obligation to warn the British warship of the presence of mines (ICJ *The Corfu Channel Case (United Kingdom v. Albania)* 1949 *ICJ Reports*, 22-23). Similar obligations of warning can be found in treaties relating to the environment (Birnie, Boyle and Redgwell 2009, 182-183). Given the speed of cyber communications, the obligation to warn of imminent harmful cyber operations may seem of limited value. On the other hand, some cyber attacks may last for several years, such as the so-called conficker worm, which lasted from 2008 to 2010. It primary attacked Microsoft Windows operating systems, infecting among other institutions the German

Bundeswehr, the French Navy, and the Greater Manchester Police. During such a prolonged period, warning may help mitigating the consequences of a cyber attack (Walter 2015a, 80). The implementation of the obligation of information must take into account individual rights, such as rights to intellectual property.

The question is raised on whether a State that is unable to prevent the misuse of its territorial cyber infrastructure bears an obligation to request assistance from the victim State or another State or to accept such an assistance. The obligation of a State to protect the rights of other States within its territory derives from the principle of sovereignty (*Island of Palmas Case* (Netherlands v. USA) 1928 *UN Reports of International Arbitral Awards* II, 839). Thus, it is normally up to the State to attempt to prevent or to stop detrimental international conduct against another State, without any interference of that latter State or a third State. Unless an international instrument obliges it to do so, under general international law, a State does not usually have to ask for international help to prevent or stop damaging transboundary cyber activities. In this author's view, there is however one situation where the territorial State should seek assistance or accept offer for assistance by the victim State or any other State: when the territorial State is obviously not able to preclude cross-border cyber activities perpetrated within its territory that cause considerable damage to another State. This is especially the case when the cyber operations lead to the injury or death of persons or damage to property similar in scale and effects to severe kinetic attacks or 'armed attacks' that, if attributed to a State, would trigger the right to self-defence of the victim State (Couzigou 2016, 258; Trapp 2007, 147 fn 82; Kittrich 2009, 145).[5] Such a scenario would exist if, for instance, the territorial State is unable to suppress, on its own, the perpetration on its territory of repeated cyber attacks by non-State actors shutting down the computers controlling the electricity supply of hospitals located in another State. As stated by the *Institut de Droit International*, '[t]he State from which the armed attack by non-State actors is launched has the obligation to cooperate with the target State' ('Present Problems of the Use of Armed Force in International Law. A. Self-defence' 10A Resolution 2007, Art. 10. https://igps.files.wordpress.com/2008/02/idi-sd.pdf). In the cyber context, the UN GGE has emphasised that 'States should also respond to appropriate requests to mitigate malicious ICT activity aimed at another State's critical infrastructure emanating from their

[5] Under Art 51 UN Charter, armed attacks are a necessary requirement for the resort to the right to self-defence by a State. Armed attacks have been defined as severe uses of armed force. ICJ *Case concerning Military and Paramilitary in and against Nicaragua (Nicaragua v. United States)* 1986 *ICJ Reports*, para. 191.

territory, taking into account due regard for sovereignty' (UN GGE, Report 2015 UN Doc. A/70/174, para. 13(h)).

The State engages its responsibility where it is proved that it failed to take measures that were reasonably available, and that such action might have prevented serious harm (physical or not). For instance, in the *Genocide* judgment, the ICJ held that the responsibility of a State for failure to prevent genocide is incurred 'if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide' (ICJ *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 2007 *ICJ Reports*, para. 430). Thus, occurrence of harm is necessary to engage State responsibility for failure or lack of due diligence in the prevention of transboundary cyber conduct (Art. 14(3) ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts 2001 *Official Records of the General Assembly, Fifty-sixth session, Supplement No 10* (A/56/10), 46).

4.2. An Obligation of Result and an Obligation of Conduct

Where a State has an obligation to take positive action, the international obligation can be an obligation of result or an obligation of conduct. An obligation of result imposes an obligation upon a State to reach a precise result. If the State does not achieve the result, this constitutes an internationally wrongful act (Pisillo-Mazzeschi 1993, 48). By contrast, an obligation of conduct does not require a specific result to be achieved but instead wants the State 'to deploy adequate means, to exercise best possible efforts, to do the utmost, to obtain this result' (ITLOS, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion 2011 *ITLOS Reports*, para. 110. See also para. 117). The ICJ specified the scope of an obligation of conduct:

> it is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide as far as possible (ICJ *Application of the Convention on the*

Protection and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) 2007 *ICJ Reports*, para. 430).

The obligation to prevent harmful international conduct encompasses the obligation to adopt a proper State organisation, so that the State is able to exercise effective control over its territory and thus to protect the rights of other States (Kolb 2015, 127; Pisillo-Mazzeschi 1993, 26-27). As explained by the ILC, 'a State should possess a legal system and sufficient resources to maintain an adequate administrative apparatus to control and monitor' detrimental activities for the rights of other States (Commentary on Art. 3 para. 17 ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities 2001 Report on the Work of its 53rd Session UN Doc. A/56/10, 155). States cannot claim the insufficiency of their apparatus to justify their failure in preventing international harm (*Alabama Claims of the United States of America against Great Britain* 1872 *UN Reports of International Arbitral Awards* XXIX, 131). The obligation of a State to adopt legal, administrative or other measures to be able to exercise its jurisdiction on its territory, or any other area under its exclusive control, and hence protect the rights of other States, is an obligation of result.

Is that general obligation upgraded in the cyber context? Do States have to enact specific legislation as well as to establish a particular administrative and judicial apparatus related to the prevention, prohibition, investigation and punishment of harmful international cyber conduct organised on their territory or transiting through their territory? Do States have to establish cyber specialists, who keep up with the latest developments in cyber technology, and to create institutions specialised in the detection of, and reaction to, damaging cyber conduct? The adoption of such measures would of course be one of the best ways to implement the obligation to prevent harmful international cyber activities. Under general international law, the obligation to prevent damaging cross-border cyber operations does not encompass the obligation to take particular legislative, regulatory or other measures related to such cyber operations (Schmitt (ed.) 2017, 48). An international treaty is necessary to impose on States the adoption of relevant dispositions to counter and react to harmful cyber activities. For instance, the Convention on Cybercrime requires States Parties to take 'legislative and other measures' to ensure that the four categories of offenses listed in the Convention are sanctioned (Chapter II, Section 1 Convention on Cybercrime (Council of Europe) 2001

European Treaty Series No 185).[6] Furthermore, the Convention contains provisions on mutual assistance in investigations or proceedings between the States Parties as well as on extradition (Chapter III Convention on Cybercrime (Council of Europe) 2001 *European Treaty Series* No 185). However, in the absence of a specific international instrument, under general international law, States are only required to possess a general legal, administrative and judicial apparatus that can normally enable them to respect their obligation of prevention of harmful international conduct, including harmful transboundary cyber conduct.

As seen above, States should use their apparatus with due diligence and attempt, as best as possible, to prevent a contradiction with the rights of other States (Ricardo 1993, 26-27). For the ILC, '[o]bligations of prevention are usually construed as best efforts obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur' (Commentary on Art. 14(3) ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries 2001 *Official Records of the General Assembly, Fifty-sixth session, Supplement No 10* (A/56/10), 145). Thus, once a State is aware or ought to be aware of a severely harmful international cyber operation that affects the right of another State, it is bound by an obligation of conduct to prevent the operation from happening or to terminate the operation. (Kulesza 2016, 267; Schmitt (ed.) 2017, 49). States do then have the choice of the best measures to take, in consideration of the circumstances, to attempt to prevent, or to stop, the cyber misuse of their territory. For instance, to terminate a cyber attack perpetrated through the launch of a malware, a State can arrest the perpetrator of the attack and compel him to uninstall the malware, or it can infiltrate the perpetrator's computer and terminate the attack itself. Where a State fails to adopt reasonable measures to prevent or stop an international cyber activity and where damage occurs in another State, the responsibility of the territorial or transit State is engaged for the violation of its obligation of conduct and not for the occurrence of the cyber activity.

In conclusion, the obligation to prevent detrimental international cyber operations is both an obligation of result, where the State is bound by an obligation to acquire an efficient legal order, and an obligation of conduct, where the State is bound by an obligation of due diligence to prevent or to stop the operations when necessary. The double nature of the obligation to prevent has been clearly recognised in relation to the obligation to prevent a

[6] Offenses against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and offences related to infringement of copyrights and related rights.

violation of human rights. The Inter-American Court of Human Rights interpreted the obligation of Article 1(1) of the Inter-American Convention of Human Rights to respect and ensure the exercise of the rights enshrined in the Convention. For the Court, the obligation to ensure the exercise of those rights

> 'is not fulfilled by the existence of a legal system designed to make it possible to comply with this obligation - it also requires the government to conduct itself so as to effectively ensure the free and full exercise of human rights' (Inter-American Court of Human Rights *Velasquez Rodriguez Case v. Honduras* 1988 Series C No. 4, paras 166-167).

5. Conclusion

The obligation of States to prevent international harm applies to cyber space. States must then prevent the cyber infrastructure based on their territory, or any other area under their exclusive control, from being used to perpetrate or to reroute damaging international cyber operations. States are not obliged to prevent the occurrence of any harmful cross-border cyber conduct. This would be impossible. States must prevent the misuse of their territorial cyber infrastructure only if they know or should have known of harmful transboundary cyber operations that are contrary to the rights of another State and that may cause or are causing serious harm in that State. Thus, once a State is aware or should have been aware that a harmful international cyber operation will occur or is underway, the State must adopt reasonable measures to prevent or to stop the operation. Determining whether a State acted reasonably in addressing a threat or occurrence of a harmful cross-border cyber operation depends on the means available to the State - technologically developed States are required to do more - as well as on the probability and magnitude of the harm - States have to dedicate more of their resources if the cyber operation is very likely to occur or is already underway and if it will cause or is causing severe damage. The obligation of States to preclude detrimental international cyber activities is both an obligation of result and an obligation of conduct. It is an obligation of result because it requires States to adopt a legal, administrative and judicial apparatus that could be resorted to when adopting measures to prevent or to stop harmful international activities, including cyber activities. It is also an obligation of conduct because, once States know of imminent or occurring harmful international

cyber activities, they have to attempt to prevent or terminate those activities, as well as possible, using their apparatus.

The results of this article can be applied to well-known cases of harmful international cyber operations. Starting in April 2007, and for approximately two weeks, Estonia's digital infrastructure was the victim of DDoS attacks. They severely disrupted governmental services, banks, and much of the media. Since Estonia relied heavily on Internet services, the cyber assaults were very damaging. Most of the attacks emanated from abroad, principally Russia. It could not, however, be firmly demonstrated that the Russian government either conducted or orchestrated them (Schmitt 2011-2012, 569-570). The common view today is that a group of hackers perpetrated the attacks for a patriotic reason - in order to react to the relocation of a Soviet war memorial in Estonia - , without any involvement of the Russian institutions. Since the attacks lasted for several days, the Russian government must have been aware of them. Furthermore, those attacks affected the rights of the Estonian State and caused severe damage in that State. Russia was thus bound by an obligation of due diligence to prevent or terminate them. Russia however tolerated the cyber offensives and thus violated its obligation of due diligence (Kerschischnig 2012, 62). DDoS attacks were also launched in Georgia in August 2008, one day before Russia invaded Georgia in support of the Ossetian and South Abkhazian separatist movements. The attacks were perpetrated from the Russian cyber infrastructure but, as was the case with Estonia, there was no conclusive proof that Russia directed them (Tikk, Kaska, Rünnimeri, Kert, Talihärm and Vihul 2008, 12). The cyber assaults lasted for several days and disrupted governmental, financial institutions and media sites. Considering Georgia's relative backwardness with regard to the Internet availability of its population, the significance of the services' disruptions was different from the one in Estonia. The damage caused by the DDoS attacks in Georgia was probably not severe enough to trigger the application of the obligation of due diligence of Russia to prevent or terminate those attacks (Tikk, Kaska, Rünnimeri, Kert, Talihärm and Vihul 2008, 13). Another precedent of cyber offensive that received important media coverage was the launch of the Stuxnet virus. It damaged Iran's centrifuges for uranium enrichment at Natanz in 2010. Despite extensive investigation, the geographic origin, less alone the institutional origin, of the virus has not been established (Buchan 2012, 219-220). The obligation of due diligence to prevent harmful international cyber operations can however be applied to another case of cyber attacks.

Governmental institutions and media outlets in Ukraine became the victims of DDoS assaults and website defacements in November 2013, when the pro-European movement *Euromaidan* organised protests against the pro-Russian policy of the Ukrainian President. The cyber offensives increased in number with the invasion of Crimea by Russia in March 2014 and have continued, in parallel to the conflict between Ukrainian forces and pro-Russian separatist groups in Eastern Ukraine. Furthermore, two hostile cyber operations shut down the power of Ukrainian power plants in December 2015 and December 2016 for several hours. Most of the cyber attacks in Ukraine have been perpetrated from computers located in Russia whose control by the Russian government could not be proved. Since they went on for a while, Russia must have known of the attacks. They contradicted the rights of Ukraine. Furthermore, seen as a whole, those attacks caused sufficient damage in Ukraine to trigger the obligation of due diligence of Russia. Russia however has been sympathetic towards the attacks and thus did not comply with its obligation of due diligence to prevent or stop them (Baezner and Robin 2017, 6-7 9-10 and 12-13). In March and April 2016, while the presidential American campaign was taking place, Russian hackers stole emails from members of the Democratic National Committee, the governing body of the Democratic Party, as well as of the campaign manager of Mrs Clinton, the Democratic Party candidate. The emails were then published online. There is strong evidence that the Russian government was behind the hackings (Lipton, Sanger and Schane 2017). There is then no necessity to apply to obligation of due diligence to prevent harmful international cyber conduct. The international norm that Russia violated here is the customary principle of non-intervention into the domestic affairs of the American State (ICJ *Case concerning Military and Paramilitary in and against Nicaragua* (*Nicaragua v. United States*) *ICJ Reports* 1986, para. 202). Indeed, this principle was infringed if Russia ordered the theft and release of emails written by influent Democratic Party officials, probably in an attempt to influence the American presidential election in favour of Mr Trump, the Republican Party candidate. More recently, the WannaCry ransomware cyber operation spread through the Internet from 12 May 2017 and infected thousands of computers around the world. Damage was in particular caused in the United Kingdom. The cyber offensive disrupted at least 81 out of 236 National Health Service trusts in England: thousands of medical appointments and operations were cancelled and in some areas patients had to travel further to accident and emergency departments

(National Audit Office. 2017, 11 and 14. *Investigation: WannaCry Cyber Attack and the NHS*. 24 October. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/). Some believe that the attack had its origin in North Korea (Hern 2017). This allegation is however not substantial enough. Furthermore, there is not proof that North Korea was aware of the preparation of the attack. Given that the attack was launched once and not repeated, it is also difficult to argue that North Korea should have been aware of it. Thus, the North Korean State was not bound by an obligation to prevent the cyber assault.

The obligation to prevent harmful international cyber operations provides States with legal protection from damaging cyber activities committed from the territory, or transiting through the territory of other States, or any other area under their exclusive control, never mind the identity of the cyber perpetrator. However, as shown by the examples above, the effectiveness of this obligation is limited. The victim State will not always be able to trace back an international cyber attack to the cyber infrastructure of another State. Even so, the territorial State or transit State is only obliged to react depending on its economic, financial and human resources. Furthermore, if the territorial State or transit State is technologically unable to prevent or terminate harmful transboundary cyber conduct, the obligation to prevent does not usually impose upon it an obligation to cooperate with more technologically advanced States. The obligation to prevent detrimental cross-border cyber conduct should be seen as a starting point in securing cyber activities. If the international community wants to improve the security of digital communications, it should adopt an international treaty on cyber security which would entail State obligations on prevention, reaction and cooperation. Such a treaty should require States to criminalise, investigate and prosecute certain forms of cyber conduct.[7] An international treaty on cyber security should impose stronger cyber security standards upon Internet providers as well as an obligation to report harmful cyber conduct to State's authorities. Such a treaty should also provide for the creation of a Computer Emergency Response Team responsible for detecting harms to the State's digital information system and reacting to them.[8] More

[7] Such a treaty should have a wider scope than the Council of Europe Convention on Cyber Crime that criminalises only 4 categories of cyber activities and, as of November 2017, was ratified by only 56 States, including non-members of the Council of Europe.

[8] The EU has already adopted such an instrument. See directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, 19.07.2016, L 194/1.

importantly, given the inherent international character of cyber communications, the treaty should organise cooperation between the relevant stakeholders (States, international organisations, Internet providers, Computer Emergency Response Teams, cyber security companies etc) in the prevention, and the reaction to, harmful cyber conduct. The Council of Europe was the first international organisation that has called upon States to cooperate with other stakeholders in order 'to prevent, manage and respond to significant transboundary disruptions to ... the infrastructure of the Internet' (Council of Europe, 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 2011, pt. 1.3. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8). More recently, at the international level, the UN GGE on Development in the Field of Information and Telecommunications in the Context of International Security strongly recommended the increase of cooperation between States and other stakeholders in order to address threats to information and telecommunications systems (UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, Report 2015 UN Doc. A/70/174, Chapter V). For the moment, at the international level, only soft-law mechanisms organise cooperation in cyber security issues. In particular, the Global Forum for Cyber Expertise, launched in April 2015 and containing over 50 members, including States, international organisations and private companies, aims to exchanging 'best practices and expertise on cyber capacity building' (See https://www.thegfce.com/about). These soft law institutions should be replaced by an effective international legal instrument that compels States to work in close cooperation with the relevant stakeholders. Thus, a treaty could establish cooperation between States in the investigation and prosecution in international cases of criminal misuse of digital information systems, as recommended by the UN General Assembly as early as 2001 (Resolution on Combating the criminal misuse of information technologies 2001 UN Doc. A/RES/55/63, Art. 1). The treaty could also set up procedures related to the exchange between States and other stakeholders of their information on cyber threats and how they handle them. Furthermore, the treaty could organise the assistance to be provided to less technologically developed States in the enhancement of the security of their cyber infrastructure. Otherwise, those States may become safe havens for the commission of international cyber attacks. Thus, the UN General Assembly stressed 'the necessity to facilitate the transfer of information technology and capacity-building to developing countries'(Resolution on the Creation of a global culture of cybersecurity 2002 UN Doc.

A/RES/57/239, para. 5) and the United States recognised the necessity to provide 'knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity' (The White House. 2011, 22. *International Strategy for Cyberspace.* https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf). Technological developments take place in cyber space quickly and any treaty rule on cyber security runs the risk to be outdated within a few years. Therefore, a treaty on cyber security should not be too overly detailed and leave leeway for interpretation to the States Parties. In the long run, ideally, supervision and coordination of the implementation of an international cyber security treaty should be given to a supranational organisation.

References

Bannelier-Christakis, Karine. 2014. "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?" *Baltic Yearbook of International Law* 14: 23-39.

Baezner Maria and Robin Patrice. 2017. *Cyber and Information warfare in the Ukrainian Conflict.* Zurich: Center for Security Studies.

Birnie, Patricia, Boyle Alan and Redgwell Catherine. 2009. *International Llaw of the Environment.* Oxford: Oxford University Press.

Brenner, Susan W. 2007. "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare." *Journal of Criminal Law and Criminology* 97 (2): 379-475.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict & Security Law* 17 (2): 212-227.

Buchan, Russell. 2016. "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm." *Journal of Conflict & Security Law* 21 (3): 429-453.

Cartwright, James E. 2010. *Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directorates*. Washington DC.

http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

Couzigou, Irène. 2016. “The Challenges Posed by Cyber-Attacks to the Law on Self-Defence.” in *International Law and…*, edited by Reinisch August, Footer Mary, and Binder Christin, 245-260. Oxford: Hart Publishing.

Crawford, James. 2006. *The Creation of States in International Law*. Oxford: Clarendon Press.

Dörr, Olivier. 2015. “Obligations of the State of Origin of a Cyber Security Incident.” *German Yearbook of International Law* 58: 85-99.

Henriksen, Anders. 2015. “Lawful State Responses to Low-Level Cyber-Attacks.” *Nordic Journal of International Law* 84 (2): 323-351.

Hern, Alex. 2017. “NHS could have avoided WannaCry hack with 'basic IT security', says report.” *Guardian*, 27 October.

Johnson, David R and Post David. 1996. “Law and Borders - The Rise of Law in Cyberspace.” *Stanford Law Review* 48: 1367-1402.

Kerschischnig, Goerg. 2012. *Cyberthreats and International Law*. The Hague: Eleven International Publishing.

Kittrich, Jan. 2009. “Can Self-Defense Serve as an Appropriate Tool against International Terrorism?” *Maine Law Review* 61: 133-169.

Koivurora, Timo. 2017. “Due Diligence.” in [online] *Max Planck Encyclopedia of Public International Law*, edited by Rüdiger Wolfrum. Oxford: Oxford University Press.

Kolb, Robert. 2015. “Reflections on Due Diligence Duties and Cyberspace.” *German Yearbook of International Law* 58: 113-128.

Kuehl, Daniel T. 2009. “From Cyberspace to Cyberpower: Defining the Problem.” in *Cyberpower and National Security*, edited by Kramer Franklin D, Starr Stuart H, and Wentz Larry, 24-42. Washington DC: National Defense University Press.

Kulesza, Joanna. 2016. *Due Diligence in International Law.* Leiden/Boston: Brill Nijhoff.

Lipton, Eric, Sanger David E. and Schane Scott. 2017. “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.” *The New York Times,* 31 October.

Pirker, Benedikt. 2013. “Territorial Sovereignty and Integrity and the Challenges of Cyberspace.” in *Peacetime Regime for State Activities in Cyberspace* edited by Ziolkowski Katharina, 189-216. Tallinn: NATO CCD COE Publication.

Pisillo-Mazzeschi, Ricardo. 1993. “The Due Diligence Rule and the Nature of International State Responsibility.” German Yearbook of International Law: 9-51.

Schmitt, Michael N. 2011-2012. “Cyber Operations and the *Jus Ad Bellum* Revisited.” 56 *Villanova Law Review* 56: 569-570.

Schmitt, Michael N. 2015. “In Defense of Due Diligence in Cyberspace.” *The Yale Law Journal Forum* 125: 68-81.

Schmitt, Michael N (ed.). 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

Shackelford, Scott J., Russell Scott and Kuehn Andreas. 2016. “Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors.” *Chicago Journal of International Law* 17(1): 1-50.

Tikk, Eneken, Kaska Kadri, Rünnimeri Kristel, Kert Mari, Talihärm Anna-Maria and Vihul Liis. 2008. *Cyber Attacks against Georgia: Legal Lessons Identified.* Tallinn: Cooperative Cyber Defence Centre of Excellence.

Trapp, Kimberley N. 2007. “Back to Basics: Necessity, Proportionality, and the Right of Self-Defence against Non-State Terrorist Actors.” *International and Comparative Law Quarterly* 56 (1): 141-156.

Von Heinegg, Wolff Heintschel. 2013. “Territorial Sovereignty and Neutrality in Cyberspace.” *International Law Studies* 89: 123-156.

Walter, Christian. 2015b. “Cyber Security als Herausforderung für das Völkerrecht.“ *Juristen Zeitung* 14: 685-693.

Walter, Christian. 2015a. “Obligations of States Before, During and After a Cyber Security Incident.” *German Yearbook of International Law* 58: 67-86.

Wong, Julia Carrie, and Solon Olivia. 2017. “Massive ransomware cyber-attack hits nearly 100 countries around the world.” *Guardian*, 12 May.