International Economic Law Clinic

A "DIGITAL" GENEVA CONVENTION TO PROTECT CYBERSPACE?

Evaluating the prospects for and content of a Convention on Cybersecurity

10th January, 2018, Geneva

Submitted by

Francesca Casalini,

Stefania Di Stefano,

Fabiola Rosi

To : Michael Kleiner, Economic Development Officer
REPUBLIC AND STATE OF GENEVA

Centre for Trade and Economic Integration, Graduate Institute of International and Development Studies

P.1 805 - Maison de la Paix, chemin Eugène-Rigot 2, 1202 Gèneve, Switzerland

TradeLab

International rules on cross-border trade and investment are increasingly complex. There is the WTO, World Bank and UNCTAD, but also hundreds of bilateral investment treaties (BITs) and free trade arrangements ranging from GSP, EU EPAs and COMESA to ASEAN, CAFTA and TPP. Each has its own negotiation, implementation and dispute settlement system. Everyone is affected but few have the time and resources to fully engage.
TradeLab aims to empower countries and smaller stakeholders to reap the full development benefits of global trade and investment rules. Through pro bono legal clinics and practica, TradeLab connects students and experienced legal professionals to public officials especially in developing countries, small and medium-sized enterprises and civil society to build lasting legal capacity. Through 'learning by doing' we want to train and promote the next generation of trade and investment lawyers. By providing information and support on negotiations, compliance and litigation, we strive to make WTO, preferential trade and bilateral investment treaties work for everyone.

More at: https://www.tradelab.org

What are Legal Practica

Legal practica are composed of small groups of highly qualified and carefully selected students. Faculty and other professionals with longstanding experience in the field act as Academic Supervisors and Mentors for the Practica and closely supervise the work. Practica are win-win for all involved: beneficiaries get expert work done for free and build capacity; students learn by doing, obtain academic credits and expand their network; faculty and expert mentors share their knowledge on cutting-edge issues and are able to attract or hire top students with proven skills.
Practicum projects are selected on the basis of need, available resources and practical relevance. Two to four students are assigned to each project. Students are teamed up with expert mentors from law firms or other organizations and carefully prepped and supervised by Academic Supervisors and Teaching Assistants. Students benefit from skills and expert sessions, do detailed legal research and work on several drafts shared with supervisors, mentors and the beneficiary for comments and feedback. The Practicum culminates in a polished legal memorandum, brief, draft law or treaty text or other output tailored to the project's needs. Practica deliver in three to four months. Work and output can be public or fully confidential, for example, when preparing legislative or treaty proposals or briefs in actual disputes.

Centre for Trade and Economic Integration (CTEI)

The Centre for Trade and Economic Integration (CTEI) CTEI is the Graduate Institute's Centre of Excellence for research on international trade. The Centre brings together the research activities of eminent professors of economics, law and political science in the area of trade, economic integration and globalization. The Centre provides a forum for discussion and dialogue between the global research community, including the Institute's student body and research centres in the developing world, and the international business community, as well as international organisations and NGOs. The Centre runs research projects and organises events. A core goal of the Centre is to foster genuine, interdisciplinary research and to work across discipline to foster solutions that address the major societal issues of today. The Centre for Trade and Economic Integration fosters world-class multidisciplinary scholarship aimed at developing solutions to problems facing the international trade system and economic integration more generally. It works in association with public sector and private sector actors, giving special prominence to Geneva-based International Organisations such as the WTO and UNCTAD. The Centre also bridges gaps between the scholarly and policymaking communities through outreach and training activities in Geneva.

More at: www.graduateinstitute.ch/ctei

Table of Content

Executive Summary 1

1. Introduction 2

1.1. The Microsoft Proposal 2

1.2. How international law could fill the gaps identified by Microsoft: overview 6

1.3. Structure of the commentary 7

2. Cybersecurity as governance *of* the internet 8

2.1. The difference between governance *of* the internet and governance *on* the internet 8

2.2. Microsoft proposal addresses the issue of governance *of* the internet 9

2.3. Microsoft proposal addresses the issue of State-sponsored operations 10

3. Existing legal framework 13

3.2. Multilateral fora 14

3.2.1. NATO Cyber Defence 14

3.2.2. The Budapest Convention 15

3.2.3. Organization for Security and Co-operation in Europe 15

3.2.4. United Nations Group of Governmental Experts 15

3.2.5. The G7 group has committed to promote security and stability in cyberspace and the protection of human rights 18

3.2.6. International Code of Conduct for Information Security proposed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan 18

3.2.7. Concluding remarks 19

3.3. Bilateral Agreements 19

4. Case studies 21

4.2. Stuxnet 21

4.3. WannaCry 23

4.4. Sony Pictures Entertainment attack 26

5. A suggested way forward 28

5.1. A neutral entity for cybergovernance, a centralised place of discussion for fast changing technologies 28

5.2. The specific functions of the third-party entity 29

Conclusion 31

Annex I: The analogy with the Geneva Conventions is not tenable 34

Annex II: General issues in governance of the internet 37

1. The issue of distinction 37

5.3. The principle of distinction does not exist in times of peace and there are difficulties in transposing it in the context of the Microsoft proposal 37

5.4. The lack of military necessity in times of peace creates the need to establish a new rationale allowing for the definition of certain objects as legitimate targets of cyberoperations 38

6. The issue of proportionality 39

6.1. The tests on proportionality can lead to different outcomes and it is important to take into account the principle of technology neutrality 39

7. The issue of "dual-use" 42

8. The issue of non-proliferation 43

9. The issue of the defence responsibility 44

9.1. The defence responsibility of the private sector in the cyberspace is a new phenomenon in international relations and there is a gap to be filled 45

9.2. The assistance in detecting and containing events involves a question of responsibility 45

9.3. The assistance in responding and recovering from events remains a matter that pertains to domestic law 46

Annex III: Factual background of the case studies 48

Bibliography 50

Table of abbreviations

ARSIWA: Articles on State Responsibility for Internationally Wrongful Acts
ATT: Arms Trade Treaty
CCDCOE: Cooperative Cyber Defence Centre of Excellence
GC: Geneva Conventions
ICRC: International Committee of the Red Cross
ICT: Information and Communications Technology
IHL: International Humanitarian Law
ILC: International Law Commission
MLAT: Mutual Legal Assistance Treaties
NATO: North Atlantic Treaty Organization
NSA: National State Agency
OSCE: Organization for Security and Co-operation in Europe
UN GGE: United Nations Group of Governmental Experts

Executive Summary

This is a commentary that aims at evaluating the Microsoft's proposed "Digital Geneva Convention" on cybersecurity. It evaluates the inputs that come from this proposal, and it tries to understand how these inputs could inform future efforts in the field of cyber governance.

The Microsoft proposal addresses the issue of State-sponsored cyberoperations which affect internet infrastructure and software. The six principles that Microsoft proposes indeed highlight important questions, and they underscore the main novelty of the cyberspace: the defence responsibility of the private sector.

This commentary highlights that, in reality, States are already discussing these problems. However, although there is agreement that international law applies to cyberspace across State-led initiatives, States have not been outspoken about *how* they believe that international law should apply to governmental cyber activities in the specific.

Rather, States' efforts have been limited to producing norms of responsible State behaviour in cyberspace which are only voluntary. The non-binding nature of these norms is challenging from the point of view of compliance and enforcement. An argument could be made that international law principles already prohibit conducts outlined in these voluntary norms, but this has not been explicitly recognized by States for the time being.

This commentary is divided into 5 parts. The first part presents the Microsoft proposal, and the way in which some of the gaps that it highlights could be filled by existing international law principles. The second part underlies that the Microsoft proposal is relevant to the behaviour of States, not common criminals, in cyberspace, and it highlights that the private sector's control of the technical infrastructure on which the internet operates is novel and thus central to the security discussion in cyberspace. The third part provides a description of the existing framework relevant to State behaviour in cyberspace, noting that the effectiveness of such framework is undermined by the voluntary and non-binding nature of States' commitment to the norms that they propose The fourth part presents three case studies of cyber events, assessed in the light of the Microsoft's proposal rules, and the 2015 UN GGE voluntary norms on Responsible State Behaviour in the

Cyberspace. This exercise highlights that Microsoft identifies existing gaps in the current legal framework, but it also shows that States are already aware of them. This finding makes the prospect of a convention constraining State behaviour in the cyberspace unlikely in the short term, and it suggests looking for unconventional, *ad hoc*, tools, to achieve more responsible State behaviour in cyberspace. Lastly, the fifth part follows up on the Microsoft's suggestion of a third-party entity that could serve key functions in cybergovernance, as the next necessary step to achieve a more secure cyber environment. The starting point for the creation of such an entity could be a multi-stakeholder discussion around the Tech Accord, as cybersecurity is a concern that touches upon private and public interests together. The entity could develop to serve as a centre for the evolution of standards in a fast-developing technology landscape; it could allow the strategic inclusion of the private sector in cybersecurity discussions; it could work as an attribution centre and peaceful dispute settlement organ; and it could become a centre for response coordination in defence from harmful cyber events.

In conclusion, a more engaged cooperation between States and the private sector is necessary in order to achieve efficient and universally harmonised solutions. Dialogue to understand both private and public interests is still needed, before finding conventional legal means to reconcile the two.

Finally, Annex I contains a brief analogy between the principles proposed by Microsoft and the 1949 Geneva Conventions on the Laws of Armed Conflict; Annex II contains a discussion of the general legal issues to keep in mind when attempting to regulate the cyberspace; Annex III contains a more detailed description of the case studies analysed in the main text.

1. Introduction

1.1. The Microsoft Proposal

This commentary seeks to develop a legal evaluation of the "Digital Geneva Convention", proposed by Microsoft. The Digital Geneva Convention was first suggested in a blogpost by Brad Smith, Microsoft's President and Chief Legal

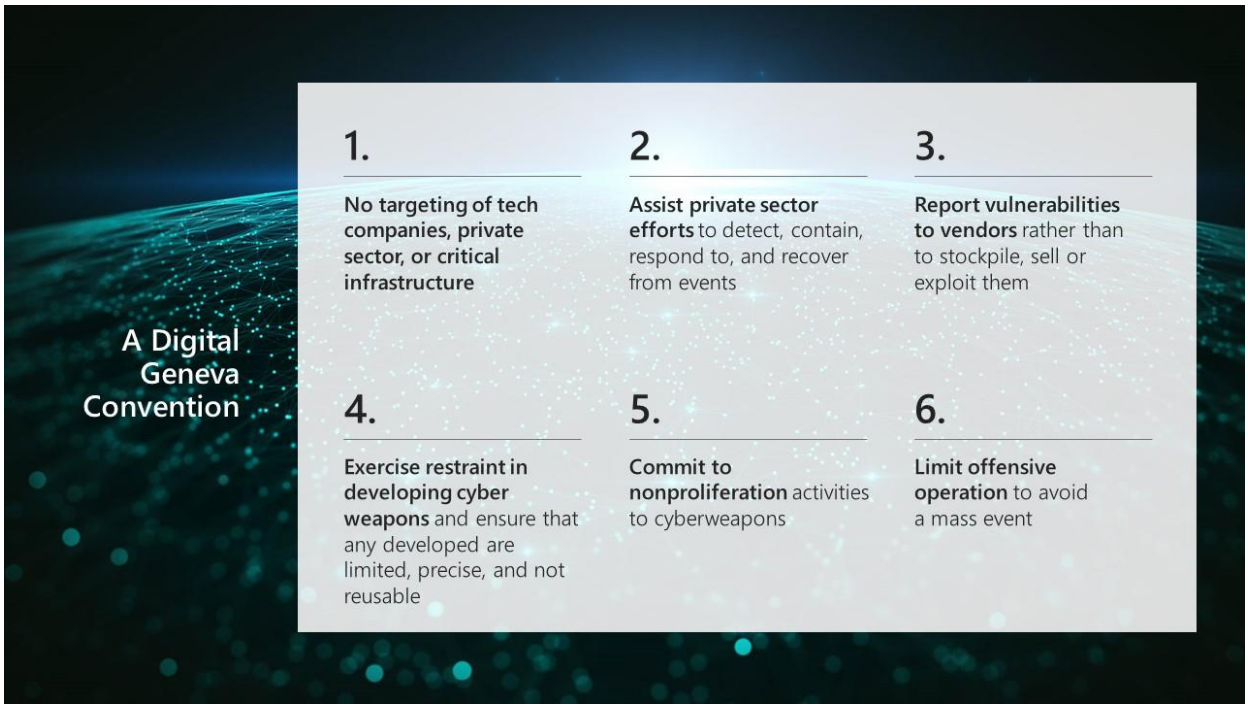
Officer, at the beginning of 2017.[1] The proposed Convention is not a draft treaty text, but, more properly, it is a concept that Microsoft suggests should be developed keeping in mind six overarching goals.

The six rules that Microsoft outlines in its proposal are:

1. No targeting of tech companies, private sector or critical infrastructure;
2. Assist the private sector efforts to detect, contain, respond to, and recover from events;
3. Report vulnerabilities to vendors, rather than stockpile, sell, or exploit them;
4. Exercise restraint in developing cyberweapons, and ensure that any developed are limited, precise, and not reusable;
5. Commit to non-proliferation activities to cyberoperations;
6. Limit offensive operations to avoid mass events.[2]

[1] 'The Need for a Digital Geneva Convention' <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> accessed 17 November 2017.

[2] ibid.



As it has been presented, all these principles ultimately relate to governmental action. Whereas the first three points concern the role that governments should set vis-à-vis the private sector in cybersecurity, the last three points concern independent commitments that States should undertake regarding their behaviour in cyberspace, to reduce overall security threats. Indeed, while cybersecurity threats can come from both States and non-state actors, Microsoft's primary concern for putting forward such a proposal is the increasing number of State-sponsored cyberoperations.

In addition to these six principles, the proposal also suggests the adoption of a text, the Tech Accord, setting out a set of principles and behaviours to which tech companies should adhere in order to protect their customers.

According to this Tech-Accord, private companies should:

1. Refrain from offensive cyber operations;
2. Protect their customers everywhere;
3. Collaborate for a first-response effort;
4. Support government's response effort;
5. Coordinate to address vulnerabilities;

6. Fight the proliferation of vulnerabilities.[3]

Finally, Microsoft forwards the idea of an independent organization that "spans the public and private sector", and that "could investigate and share publicly the evidence that attributes nation-state attacks to specific countries".[4]

Microsoft's concerns about the regulation of State-sponsored cyberoperations affecting the ICT sector and society as a whole are not unfounded. Indeed, States themselves have started to address the question of how to regulate their relation in cyberspace.

A remark on the peacetime qualification

The Microsoft proposal specifies in its title that the rules it envisages would be applicable in times of peace, and it would therefore leave the regulation of these conducts to the realm of IHL if the threshold of armed attack is attained. Indeed, the ICRC considers that IHL is already capable of regulating cyberwarfare.[5] At the same time, by making this specification, Microsoft underlines that these rules would govern behaviour in the cyberspace even in scenarios that remain well below the use of force or armed attack (which triggers the laws of war)[6].

Since it remains unclear when a cyber operation would attain the level of armed attack for the purposes of IHL, and since the aims pursued by the Microsoft proposal are somehow different from those pursued by the laws of war, it would seem more appropriate to conceive the Microsoft proposal as an instrument that aims to establish a system of internet governance, that does not aim at affecting or replacing any existing legal regime, but that wants to acknowledge that there are new phenomena that still need to be regulated. Thus, the 'peacetime' qualification does not add value and generates a risk that the proposed rules would be considered as displaceable in times of war, whereas the particular relationship that exists between the State and the private sector in the cyber realm would persist even in times of war. For these reasons, it is suggested to remove this qualification altogether.

[3] 'A Tech Accord to Protect People in Cyberspace | Microsoft Cybersecurity' <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-tech-accord-to-protect-people-in-cyberspace> accessed 17 November 2017.

[4] 'The Need for a Digital Geneva Convention' (n 1).

[5] Cordula Droege, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 International Review of the Red Cross 533.

[6] McKay and others (n 10) p. 10.

1.2. How international law could fill the gaps identified by Microsoft: overview

Before engaging with a thorough analysis of the proposal, it is important to highlight how international law could already be capable of addressing some gaps highlighted by the six rules that Microsoft has put forward.

1. **No targeting of tech companies, private sector or critical infrastructure**: This goal could be achieved through renewed commitments of compliance with the principles of non-interference in the domestic affairs of other States, and the prohibition of the use of force, as enshrined in the UN charter. The applicability of the UN Charter in this sense to the cyberspace has already been confirmed. This political commitment should be leveraged on to actually achieve compliance. This aspect will be further analysed in section 3.2.

2. **Assist the private sector efforts to detect, contain, respond to, and recover from events**: The assistance could be provided by governments as well as by the independent organisation suggested by Microsoft. Governments are responsible, under the principle of sovereignty as responsibility, to protect their citizens, while also having a duty to cooperate in the maintenance of global peace and security, in line with the UN Charter. The independent organisation could be the institution exerting political pressure on States to fulfil their international obligations. The analysis of a potential third-party entity will be presented in section 5.

3. **Report vulnerabilities to vendors, rather than stockpile, sell, or exploit them*:*** This goal could also be achieved through renewed commitment of compliance with the UN principles in the cyberspace. Reporting vulnerabilities would arise as an obligation from the duty to cooperate to maintain global peace and security, according to the UN Charter, and it has already been recognised by States in political declarations.

4. **Exercise restraint in developing cyberweapons, and ensure that any developed are limited, precise, and not reusable**. This is perhaps the most significant gap identified by the Microsoft proposal, but lacks States' commitment even at the political level. This goal could be achieved through the authoritative re-interpretation and application of existing rules of international law.

5. **Commit to non-proliferation activities to cyberoperations**: This could be achieved through an authoritative re-interpretation of the Arms Trade Treaty which is assessed in Annex II.

6. **Limit offensive operations to avoid mass events**. This goal could also be achieved through the authoritative re-interpretation and application of existing rules of international law, as well as compliance with the already-existing international agreements including the UN charter.

1.3. Structure of the commentary

This commentary aims at evaluating the inputs coming from Microsoft's proposal, in order to understand how Microsoft's principles could shape future discussions on cybersecurity and eventually be translated into a governance design and legal framework for the cyberspace.

Firstly, the commentary will offer an explanation of the difference between governance *of* the internet, and governance *on* the internet, and assess how the Microsoft proposal falls within the first category.

Secondly, the commentary will offer an overview of the existing political and legal framework dealing with States' conduct in cyberspace. It will present and analyse multilateral fora that have engaged with cyber-specific discussions regarding State behaviour.

Thirdly, the commentary will assess how real cases of cyber operations could have engaged State responsibility, if Microsoft's proposed rules on the one hand, and the voluntary norms of responsible State behaviour stipulated by the 2015 UN GGE on the other, were legally binding. The aim of this section is to show that Microsoft's proposal spots important gaps in the current legal framework, given the relative

unaccountability that these operations have encountered despite their dangerousness to citizens' security.

Fourthly, the commentary will propose to use the Tech Accord as a starting point for initiating multi-stakeholder discussions on cybersecurity standards, suggesting that this may eventually lead to the establishment of an ad-hoc entity for cybergovernance, as suggested by Microsoft. Some key functions that the entity could fulfil will be highlighted.

Finally, Annex I contains a brief analogy between the principles proposed by Microsoft and the 1949 Geneva Conventions on the Laws of Armed Conflict; Annex II contains a discussion of the general legal issues to keep in mind when attempting to regulate the cyberspace; Annex III contains a more detailed description of the case studies analysed in the main text.

2. Cybersecurity as governance *of* the internet

2.1. The difference between governance *of* the internet and governance *on* the internet

It is of utmost importance that the two distinctions outlined below (governance *of/on* the internet; cyberoperations coming from States and non-state actors) be kept in

mind when seeking solutions, and that dialogue on cybersecurity keeps the related discussions separated.

The internet functions at three levels. There is the infrastructure layer, the logical layer (e.g. Internet and networking protocols, operating systems, software and applications), and the content layer.

Accordingly, cybersecurity is a complex endeavour that requires at least two types of governance:

1. Governance *of* the internet, needed to address the issues arising from the novel functioning of internet systems, which among other things alter assumptions about how harm can be made to physical things and persons. Governance of the internet is mostly concerned with the infrastructure and logical layer;
2. Governance *on* the internet, needed to ensure that certain fundamental principles of the traditional social contract are respected even in their digital space manifestation. Governance on the internet is mostly related to the content layer, and it is challenged by the difficult assertion of State sovereignty and enforcement jurisdiction over the non-tangible position of content in cyber, i.e. there is no single State's territory.

The key consequence of such distinction for the purposes of this work is that, whereas for governance on the internet it is a matter of transposing existing laws to online conditions, such as governing content, governance of the internet may need *ad hoc* laws or at least a radically evolved reading of existing laws to govern issues such as remote cyberoperations.

2.2. Microsoft proposal addresses the issue of governance *of* the internet

The Microsoft's Digital Geneva Convention is concerned with the governance *of* the internet, i.e. with the infrastructure and logical layer.

In this sense, the first three points of the Microsoft proposal seek to address the exploitation of vulnerabilities in information systems, which allows for a malware to enter into a system and obtain administrative privileges over it. Once these privileges over the system have been obtained, malwares can take advantage of the ability of

the infected system to interact with other systems, and to expand into other systems. A vulnerability can be a mistake in the code of the infected system, but it can even be a person, deceived by words to authorize the entrance of the malware into the system. A very crucial note shall be made that vulnerabilities are bound to exist in the internet infrastructure.

Of course, even governance *of* the internet is not completely outside the reach of existing law, for its negative effects are ultimately an encroachment on the social contract as well. Negative effects for the users of infected systems include damaging their system or changing their settings, or denying them use of internet services or stealing their money and personal data, or even causing kinetic effects. However, what is fundamentally different and requires new thinking, is that security, traditionally an interest protected by the State, in cyberspace is dependent on privately owned infrastructure, systems, and software. Thus, the private sector has an unusual position in the governance of the internet: it is the necessary vector of vulnerabilities exploitations, while also being the first responder to those events, and also being responsible for fixing their consequences.

The exclusive role of the private sector in protecting the security of users, and of itself, is the fundamental challenge posed by the governance *of* the internet, which requires for policymakers a mindset that is different than for content-related law enforcement, where content is visible, and it ultimately has negative effects after a person-to-person interaction has taken place. Again, it may be ultimately the same substantial effect that is being prevented, but the *how* entails crucial differences of viable governance schemes. For these reasons, constructive engagement between governments and private companies is necessary to achieve security.

2.3. Microsoft proposal addresses the issue of State-sponsored operations

In principle, the deployment of malwares can come from State and non-state actors. But without a doubt, Microsoft is here concerned with State-sponsored events, rather than cyberoperations deployed by non-state actors. In fact, it can be easily understood that actions operated by individuals or other non-state entities fall within the category of cyber-criminality. This is not to downplay the importance of cyber-criminality, nor to underestimate the challenges that it poses for law enforcement, but clearly it is a phenomenon that comes down to the need for mutual legal assistance

treaties (MLATs) between States. As the existence of some legal instruments demonstrate, States already are concerned about cyber-criminality.[7]

Cyberoperations deployed by non-state actors – brief considerations

Malwares can indeed be deployed by non-state actors. While an assessment of this specific issue would be beyond the scope of this commentary, some brief details are provided below.

The regulation of malicious cyberoperations conducted by non-state actors pertains to the legal domain of criminal law, and therefore it remains a matter for domestic legislation, rather than international law, to regulate. States have already begun to establish some forms of cooperation to respond to cybercriminality. The Budapest Convention (which will be assessed in the following section) is the first international treaty that regulates crimes committed either through the internet or through other computer networks, and it establishes a common criminal policy that aims at protecting society against cybercrime. Mainly, it fosters international cooperation and harmonious criminal legislation for cybercriminality. Nonetheless, the treaty imposes on State parties to "adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law". This means that international law, is therefore the tool through which harmonisation and cooperation against cybercriminality are achieved, but the conduct of the non-state actor is finally regulated by domestic criminal law.

Microsoft would not have proposed a Digital Geneva Convention regulating State behaviour if it were not for some other outstanding issues. In fact, it is State-sponsored operations that are increasingly sophisticate and dangerous to the protection of fundamental rights of individuals as well to the functioning of societies, while the law applicable to them remains uncertain. Accordingly, the last three points that Microsoft proposes no longer address the role of the private sector, but rather

[7] See, for example, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JH http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040; OAS Cybersecurity Strategy; http://www.oas.org/juridico/english/cyber_security.htm; *Convention on Cybercrime, ETS 185, Council of Europe (Budapest, 2001);.* for additional information UNODC Cybercrime Repository https://www.unodc.org/cld/v3/cybrepo//.

aim at preventing States' cyber weapons development. Microsoft's rules 4, 5 and 6 encapsulate the type of conduct that is currently being discussed under the name of "Responsible States' behaviour in the cyberspace"[8] or "International Code of conduct for information security" (China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan letter to UN Secretary General)[9]. As it will be further explained below, the avoidance of more assertive terms such as "lawful" States' behaviour in the cyberspace indicates the reluctance of States to consider themselves bound to *new* rules of law in cyberspace, or not consider themselves as already legally bound by international law rules.

What is particularly problematic, is that geopolitical reasons often move exploitations of vulnerabilities for malicious purposes, and they have become a new tool of conducting international affairs and exercising political pressure. Remarkably, Microsoft's proposal speaks of "cyber events." In this sense, Microsoft highlights concern for events caused by governmental actors, that are potentially highly disruptive, while remaining quite undoubtedly below the threshold of armed attack. Microsoft here seems to make a case for when such events affect non-state actors. Because it would be politically difficult to imply that, by *ab contrario* reasoning, State actors would then be a lawful target of cyber operations in peacetime, and because it is often difficult to draw a clear distinction between a governmental and non-governmental infrastructure or software in cyber, this work will consider that it is the general relationship between States and the cyberspace, and the cyberspace operators, that needs to be better defined. The 2013 United Nations Group of Governmental Experts[10] has found that international law applies in the cyberspace, but the precise scope of allowed cyber activities for States largely remains a question mark. Instruments and initiatives that concern the behaviour of States in the cyberspace are often vague and progress slowly in explaining *how* international law would be satisfactorily upheld in the cyberspace, due to political reasons. Clarifying the *how* remains necessary because the international law principles of sovereignty

[8] 'G7 Declaration on Responsible States Behaviour in Cyberspace' (Lucca, 11th April 2017).

[9] 'Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General' <http://dag.un.org/handle/11176/158448> accessed 17 November 2017.

[10] 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (UNGA 2013) UN Doc A/69/723

and attribution are ill-defined in the cyberspace at the moment, and this makes a smooth enforcement of existing law in the cyberspace difficult.

In sum, in elaborating on the Microsoft proposal, it is the private sector's control of the technical assets on which the internet operates, and the behaviour of States in such regard, that are at the centre of the discussion.

3. Existing legal framework

Means have been found to exploit ICT vulnerabilities as fast as digital technologies have developed. Due to the borderless nature of cyberspace, States as well as international organizations have sought international solutions. However, where legislative measures have developed quickly for addressing cyber-criminality and cyber-terrorism, less has been done for addressing States' behaviour in cyberspace.

In this section, we look at some of these key multilateral and bilateral instruments. We demonstrate that there are a plethora of political declarations and confidence building measures regarding States' behaviour in cyberspace. They represent important assets to highlight consensus, and should be leveraged on. We conclude that only voluntary norms on responsible state behaviour have been formulated with specific regards to cyberspace, but States are not accountable for the purposes of international law, and compliance with these norms continues to lack. As it will be further explored below, the establishment of a third-party entity could be a means through which incentivise compliance.

3.2. Multilateral fora

3.2.1. NATO Cyber Defence

The North Atlantic Treaty Organization (NATO) was the first to deal with cyber threats at the national and international level. The focus of NATO's cyber strategy is on cyber defence, particularly preventive measures that strengthen resilience of its members. Still, national networks remain under national jurisdiction and NATO considers that it will intervene only in case of a military cyber threat,[11] although no legal definition of armed attack is agreed upon, as it has already been argued above.

The Tallinn Manual is also a NATO initiative. The 2017 "Tallinn Manual on the International Law Applicable to Cyber Warfare"[12] aims at clarifying how the laws of armed conflict apply in the cyberspace, i.e. it is a manual on "cyber warfare." Although it is yet unclear what constitutes a cyber armed attack, it is safe to say that, just like in the traditional world of international affairs, not all wrongful acts amount to a violation of the prohibition of the use of force. Accordingly, the framework of behavior that the Tallinn Manual regulates is beyond the scope of this work, as there are many States' cyber operations to which the rationale of warfare does not apply, but for which we still need clearer regulation. Incidentally, the Tallinn Manual is not a multilaterally agreed document, hence it is not binding for the purposes of international law.

Since 2014, NATO cooperates with the private industry through the NATO Industry Cyber Partnership[13], but these partnerships remain at the level of two-way information sharing.

NATO focuses on cyberwarfare, but it does not establish the threshold for armed attack, nor does it clarify what behaviour should be considered appropriate below this threshold.

[11] NATO Policy on Cyber Defence Factsheet 2016.

[12] Michael N Schmitt and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017).

[13] See http://www.nicp.nato.int/

3.2.2. The Budapest Convention

The Council of Europe Convention on Cybercrime[14], also referred to as the Budapest Convention, entered into force into 2001. The relevance of this Convention for the purposes of regulating States' conduct in the cyberspace is watered down by article 27(4), which entitles a party to refuse assistance under the Convention if it considers that that would harm its national political interests. It seems reasonable to assume that if a State deployed a cyberoperation intended to harm another State, it would invoke this article and refuse legal assistance to the injured State. This article *de facto* works as a legal shield for State-sponsored operations in the cyberspace, i.e. the Budapest Convention does not create any constraint to State behaviour, which is to the contrary the concern that the Microsoft proposal tries to address.

3.2.3. Organization for Security and Co-operation in Europe

On matters of cybersecurity, OSCE has worked mainly through confidence building measures. Until now, these have not focused on State behaviour, and States are contributing on a voluntary basis.[15] On November 3, 2017 an OSCE conference has taken place in Vienna, to discuss rules for responsible state behaviour in cyberspace, but the outcome of this meeting has not been released yet.

3.2.4. United Nations Group of Governmental Experts

The 2013 UN GGE has stipulated that international law is applicable in the cyberspace.[16] This alone is not sufficient to regulate States' behaviour in the cyberspace, yet it provides a solid foundation for further discussion on the specifics of an international legal regime regulating States' responsibility. State practice could be a pivotal instrument for defining interpretative developments of international law in a more decisive manner. States have been vague in their declarations about how they believe that international law should apply to governmental cyberactivities. In

[14] *Convention on Cybercrime, ETS 185, Council of Europe (Budapest, 2001).*

[15] 'OSCE Permanent Council Decision No.1106. Available at Http://Www.osce.org/Pc/109168?download=true'.

[16] 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (n 10).

fact, they have mostly established norms of responsible State behaviour that only constrain them on a voluntary basis.

The 2015 UN GGE[17] report and the 2015 G20 Leaders' Communiqué[18] have articulated "*voluntary* norms of responsible state behaviour during peacetime" (emphasis added).

Below is an overview of how some of these norms promote obligations already very similar to those that Microsoft would like to include in a Cybersecurity Convention.

- Microsoft's rule number one says: "No targeting of tech companies, private sector or critical infrastructure". Similarly, the UN GGE has already formulated the notion that "(f) a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public";[19]
- Microsoft's rule number three says: "Report vulnerabilities to vendors, rather than stockpile, sell, or exploit them". Similarly, the UN GGE has already formulated the notion that "(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;" and that "(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products."
- Microsoft's rule number four says: "Exercise restraint in developing cyberweapons, and ensure that any developed are limited, precise, and not reusable". Similarly, the UN GGE has already formulated the notion that "(i) […] States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."[20]

[17] 'Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security' (UNGA 2015) UN Doc A/70/174.

[18] 'G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015'.

[19] 'Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security' (n 17).

[20] ibid.

The UN GGE has only noted these norms as non-binding and voluntary in nature, hence States have no liability for failing to respect them. It is unclear whether these norms are directly derived from international law. Moreover, it has been underlined that these norms "do not seek to limit or prohibit action that is otherwise consistent with international law".[21] Problematically, there is scope for actions that do not comply with the voluntary norms, while still allegedly complying with international law. The threshold at which the non-compliant conduct becomes unlawful has not been made explicit. Notwithstanding this interpretative uncertainty, the effects of these conducts could undoubtedly result in a violation of international law under certain circumstances.

In situations where violations of these principles have been witnessed through cyber means, this has not been taken as an opportunity for the international community to condemn such actions and clarify how and why such actions were unlawful. (See, for example, the US development of a highly indiscriminate malware to exploit a vulnerability, instead of reporting it, as further described in Section 5, Case Studies). In sum, lacking cyber-specific identifiable state-practice, and consistent *opinio juris*, it is difficult to understand what the application of international law in the cyber space truly entails for States' behaviour.

Notably, the 2017 UN GGE[22] was not able to find a consensus, indeed due to the disagreement over the extent to which international law applied, with some States especially contesting whether the regime of State Responsibility and the right to self-defense applied at all. These States (most notably Cuba) advocate for a peaceful settlement of cyber disputes.

Both views have their strengths and weaknesses:

- The Cuban approach is desirable to avoid escalation and would help those States that have less cyber capabilities, but the complexity of the cyberspace makes it implausible that a purely dispute-settlement framework would be respected;

[21] ibid.

[22] 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (UNGA 2017) A/72/315.

- The Western approach carries the risk of escalation, yet it would have a deterrent effect and would be helpful in stabilizing the environment.

Finally, we highlight that Cuba suggested opening a Working Group of the General Assembly to create a new binding instrument after the failure of the 2017 UN GGE.

The UN GGE work should be considered as an important milestone for future discussions on cybersecurity regulation. The relevance of these norms will be highlighted in the next section, where they will be used for the analysis of the case studies.

3.2.5. The G7 group has committed to promote security and stability in cyberspace and the protection of human rights

On April 11th, 2017, the G7 signed a Declaration on Responsible States' Behaviour in Cyberspace. They reiterated that international law applies in the cyberspace, and committed to the promotion of the 2015 UN GGE "*voluntary* norms of responsible state behaviour during peacetime"[23] (emphasis added).

3.2.6. International Code of Conduct for Information Security proposed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan

China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan proposed an International Code of Conduct for Information Security to the United Nations (last proposed version was released on January 9th, 2015).[24] The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) reports that a number of objections were raised: "[f]irst, the Code was seen as a step towards formalising new rules governing cyberspace and the use of information technology, a notion generally opposed by the US and other liberal democracies which have mostly adopted the stance that existing international law is sufficient and that new rules would, for

[23] 'G7 Declaration on Responsible States Behavior in Cyberspace' (n 8).

[24] 'Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General' (n 9).

example, limit technological innovation and growth".[25] Further, the Code suggests that a 'multilateral' (intergovernmental) system for Internet governance should be developed, but such a system would be at the expenses of a multi-stakeholder approach, that is favoured by Western countries.[26]

We note that the Code aims at prioritizing security and control over international human rights law. In particular, when reaffirming the principle that the rights of the individual in the physical space should be equally protected in the digital space, it seems that the rights referred to are those granted by the domestic policy of different countries. Such an understanding would be in line with the general attempt of the proposing countries to reinforce the idea that territorial State sovereignty applies in the digital space. Indeed, the Code also does not mention that existing international law generally applies to cyberspace.

3.2.7. Concluding remarks

Consensus has been found on some key cybersecurity norms that State should abide by, for the protection of the internet infrastructure. Still, these norms remain voluntary, and are qualified as "responsible behaviour" rather than "lawful behaviour." As the case may be, it seems that this consensus cannot be consolidated further due to the current political stalemate on how human rights considerations should inform these norms. The content and the hierarchy of human rights norms are not universally agreed and have led to regionally fragmented initiatives in this field. More dialogue is needed to straighten out these issues.

3.3. Bilateral Agreements

Some States have also opted for bilateral agreements which are easier to discuss, to implement and to withdraw from, if needed. The problem of such agreements is that their exact content is unknown, so that it is difficult to infer from them what sort of

[25] 'An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?' (*CCDCOE*, 10 February 2015) <https://www.ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new> accessed 17 November 2017.

[26] ibid.

understanding States have, with regard to responsible States' behaviour in the cyberspace. Examples of such agreements are:

- US and Russia: negotiations started in 2013, aiming to establish a cyber-hotline between the two countries as well as a bilateral working group to increase cooperation in national security. However, due to the political crisis in Ukraine, the negotiations were frozen.[27]

- **US and China**: reciprocal abstention from cyber-espionage[28].

- China and Russia: reciprocal engagement not to launch cyber-attacks against the other party and mutual support to other party's cyber-sovereignty[29]

- **US and India**: parties engage to cooperate with CERTs and law enforcement agencies as well as to restrain from cyber-espionage and cyberattacks. [30] According to the DiploFoundation report, "*[t]he agreement supports the multi-stakeholder model of Internet governance, which moves India closer to the position of the USA and its allies and further from the position of China and Russia*".[31]

Although these bilateral agreements represent commendable efforts to make cyberspace a safer environment, there is a risk of fragmentation in the approach taken in relation to cybersecurity.

[27] 'The White House (2013) FACT SHEET: US-Russian Cooperation on Information and Communications Technology Security. Available at Https://Www.whitehouse. Gov/The-Press-Office/2013/06/17/Fact-Sheet-Us-Russian-Cooperation-Informa- Tion-and-Communications-Technol'.

[28] M Spetalnick and M Martina, 'Obama Announces "understanding" with China's Xi on Cyber Theft but Remains Wary.' (26 September 2015) <http://www.reuters.com/article/2015/09/26/us-usa-china-idUSKCN0RO2HQ20 150926#QCl52gO5xlJVWVja.97>.

[29] Patryk Pawlak, 'Confidence-Building Measures in Cyberspace: Current Debates and Trends' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (Tallinn 2016) <https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf>.

[30] 'The White House (2016) Joint Statement: The United States and India: Enduring Global Partners in the 21st Century. Available at Https://Www.whitehouse.gov/ the-Press-Office/2016/06/07/Joint-Statement-United-States-and-India-Enduring-Global-Partners-21st'.

[31] Vladimir Radunovic and the DiploFoundation team, 'Towards a Secure Cyberspace via Regional Co-Operation' (DiploFoundation 2017).

4. Case studies

Although some could claim that all politically motivated cyberoperations are merely sophisticated attempts at sabotage, espionage, and subversion[32], recent incidents proved that cyberoperations can have much deeper effects. The following section aims at briefly describing the features of three selected international cyber events, chosen because of the destructive effect (Stuxnet), the indiscriminate nature and governmental origin (Wannacry) or targeting the private sector and its consumers (Sony attack).

The purpose of this section is to assess the features of these events, against the Microsoft's proposed rules, as well as the 2015 UN GGE Report on the Norms of Responsible State Behaviour. This exercise will show that the Microsoft proposal identifies existing gaps in the current legal framework, but also that States are already aware of these gaps. The problem highlighted is that they are only willing to subscribe to informal commitments in this regard, while continuing to adopt a non-responsible behaviour in violation of the same norms that they have crafted.

4.2. Stuxnet

Stuxnet is a computer worm that infected the software of at least fourteen industrial sites in Iran, including a uranium-enrichment plant.[33] Allegedly, it spread from a removable hard disk that showed false digital certificates. Remarkably, it did not require any Internet connection to be able to spread.[34]

[32] For more detailed arguments see : Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press 2013).

[33] David Kushner, 'The Real Story of Stuxnet' (*IEEE Spectrum: Technology, Engineering, and Science News*, 26 February 2013) <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet> accessed 17 November 2017.

[34] ibid.

Assuming that Stuxnet was a State-sponsored attack, the operation breached at least four of the rules put forward by Microsoft, and four of the UN GGE norms on Responsible State Behaviour:

Stuxnet's effects	Microsoft's violated rules	UN GEE violated norms
Fourteen industrial sites, including a uranium-enrichment plant, were affected	*"No targeting of tech companies, private sector or critical infrastructure"* (Microsoft rule 1)	"*a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public"* (UN GGE norm (f))
The malware was opensource, i.e. reusable, and could spread easily[35]	*"Commit to non-proliferation"* (Microsoft rule 5*); "Exercise restraint in developing cyber weapons and ensure than any developed are limited, precise, and not reusable"* (Microsoft rule 4)	*"*[…] *States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions"* (UN GGE norm (i))

[35] Kim Zetter, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon' (*WIRED*) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> accessed 17 November 2017.

The US and Israel did not report the vulnerability and they exploited the zero-day flaw instead	*"Report vulnerabilities to vendors"* (Microsoft rule 3)	*"States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure"* (UN GGE norm (j))
	"Limit offensive operation to avoid a mass event" (Microsoft rule 6)	

However, it needs to be noted that the "limited" and "precise" features of allowed cyberweapons under the Microsoft's proposal would have been respected in this case. This is relevant to show that such cyberweapons could in principle be developed.

4.3. WannaCry

WannaCry is a ransomware attack that hit more than 330,000 computers in more than 150 countries[36]. Unlike Stuxnet, it did not develop from a zero-day flaw, but used a malicious software developed to exploit vulnerabilities stolen from the United States National Security Agency, which it had discovered and was stockpiling.[37] We

[36] Julia Carrie Wong and Olivia Solon, 'Massive Ransomware Cyber-Attack Hits Nearly 100 Countries around the World' *The Guardian* (12 May 2017) <http://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs> accessed 17 November 2017.

[37] 'The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack' <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/> accessed 17 November 2017.

highlight that the exploit was developed by the US government on the basis of a vulnerability that it had discovered and failed to report.

WannaCry would amount to multiple international violations, if assessed in the light of the Microsoft proposal and of the UN GGE Norms of Responsible State Behaviour, the event breached five and three of the norms respectively:

WannaCry's effects	Microsoft's violated rules	UN GEE violated norms
The malware as deployed by North Korea targeted a tech company's software, and ultimately hospitals and banks.	*"No targeting of tech companies, private sector or critical infrastructure"* (Microsoft rule 1)	"*a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public"* (UN GGE norm (f))
The host State of the company, the United States, which had incidentally also developed the original malware, has not assisted the Microsoft in containing and responding to the event, of which the kill-switch was eventually found by a	*"Assist private sector efforts to detect, contain, respond to and recover from events" (*Microsoft rule 2)	

young security researcher, known as MalwareTech.[38]		
The US NSA did not disclose the vulnerability to Microsoft, and it stockpiled it instead	*"Report vulnerabilities to vendors"* (Microsoft rule 3)	*"States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure"* (UN GGE norm (j))
The malware developed by the NSA was reusable, unprecise, indiscriminate, and capable of leading (as it did) to a mass event.	*"Exercise restraint in developing cyber weapons and ensure than any developed are limited, precise, and not reusable"* (Microsoft rule 4); *"Limit offensive operation to avoid a mass event"* (Microsoft rule 6)	
Not enough information is available to establish whether the US NSA would be culpable of negligence with regard to the safe storage and		"[…] *States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful*

[38] 'Cyber-Attack "Unprecedented" in Scale' *BBC News* (13 May 2017) <http://www.bbc.com/news/world-europe-39907965> accessed 17 November 2017.

custody of the malware that it had developed. However, such responsibility could be invoked if circumstances of negligence existed.		*hidden functions"* (UN GGE norm (i))

Furthermore, the attack did not occur from a zero-day flaw and a patch had been previously distributed, States had the responsibility to ensure that the operating system of their public infrastructure would be most protected. For this reason, the affected States have allegedly violated UN GGE norm (i): "*States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden function*".

4.4. Sony Pictures Entertainment attack

On November 24, 2014, a series of personal data stolen from Sony computers, leaked to the public. These included employees' emails, information about salaries, credit card numbers as well as some of the company's unreleased movies.[39] Unlike the previous cases, where the attack was either indiscriminate (WannaCry) or reusable (Stuxnet), this attack was very precise and non-reusable. In addition, Sony's operating system was left inoperative for several days. It was only on December 8, 2014 that the company disclosed the attack to its employees.[40]

Assuming that the attack is attributable to North Korea, the operation against Sony entailed a violation of a Microsoft rule as well as of a UN GGE norm.

[39] Gabi Siboni and David Siman-Tov, 'Cyberspace Extortion: North Korea versus the United States' (2014) No. 646 INSS Insight 646.

[40] Sony Pictures Entertainment, 'Sony Notice Letter' (8 December 2014) <https://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf>.

Sony Attack's effects	Microsoft's violated rules	UN GEE violated norms
A private company was targeted.	*"No targeting of tech companies, private sector or critical infrastructure"* (Microsoft rule 1)	*"a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public"* (UN GGE norm (f))

As shown above, if the Microsoft rules and the UN GGE norms were binding, these incidents would have engaged state responsibility under international law.

	Key features	Breached Microsoft's rules	Breached UN GGE norms
Stuxnet	• Malware spread from removable hard disk • Performed four zero-day exploits	Breach of rules **1, 3, 4. 5, 6**	Breach on norms **f, i, j**

	• Iranian nuclear plant as a target		
Wannacry	• Large-scale ransomware attack • Did not develop from a zero-day flaw • Hit public infrastructure	Breach of rules **1,2,3,4,6**	Breach of norms **f, i, j**
Sony attack	• Series of attacks on Sony which led to the leak of the company's critical information • Political motive: movie mocking the dictator	Breach of rule **1**	Breach of norm **f**

5. A suggested way forward

This final section explores how the suggestion of Microsoft to establish a third-party entity could indeed provide a helpful instrument for furthering cybersecurity instruments in a multi-stakeholder system.

5.1. A neutral entity for cybergovernance, a centralised place of discussion for fast changing technologies

A starting point for the promotion of a discussion on cybergovernance could be the Tech Accord, that Microsoft has included in its proposal.

The Tech Accord is an instrument on which Microsoft is actively working, and that is already receiving attention from several tech companies. The interest of private companies in this project is due primarily to their economic interest in fostering trust between companies and users. In a way, the Tech Accord would serve as a trust guarantee in their market.

Moreover, if a majority of tech companies were to adhere to and implement this self-regulating instrument, it could have the potential of exercising political pressure on States, encouraging further discussion among them on the issue of cybersecurity. Indeed, the Tech Accord itself could be used as a basis for a multi-stakeholder discussion in the near future, involving States, private sector, and civil society. Further, it is suggested that multi-stakeholder discussions on the content of this Tech Accord could serve as a seed for the potential creation of a third-party entity for cybersecurity governance, on the model of existing entities that have governance power over a specific area of social interest.

The Tech Accord could be conceived as a standard-setting instrument for private companies, providing universally harmonised guidance, risk-management practices, appropriate tools and policies. Since the issue of cybersecurity concerns both States and the private sector, a Tech Accord that takes into consideration the positions of both kind of actors would be most effective. The multi-stakeholder character of this discussion is fundamental in order to establish transnational standards that enable the creation of a secure environment at large.

5.2. The specific functions of the third-party entity

The entity that could arise from these discussions, should also be multi-stakeholder, involving States, private sector, and civil society. The entity could fulfil at least four key functions:

1. The entity could serve as a centre for the evolution of standards, with all the stakeholders involved. A permanent entity dealing with the issue of cybersecurity could serve the purpose of ensuring that standards remain up-to-date with regards to a fast-developing technology landscape.

2. If a tech company wants to participate actively into the works of the entity, it would have to adhere to the Tech Accord principles, and implement them through self-regulation. Obviously, the active participation of the private sector entails both

privileges and responsibilities. In terms of responsibilities, the private sector would have to actively cooperate with the entity in detecting and fixing vulnerabilities, as well as sharing information in relation to a cyber-misconduct. Under these circumstances, the tech company would enjoy a privileged status.

3. The entity could be considered a neutral organ able to determine attribution of cyber-malicious activities, including State-sponsored ones. Once the conduct is attributed, the institution could work as a peaceful dispute settlement body, with States' consent, or alternatively, it could at least exercise reputational pressure in shaping States' behaviour.

4. There are instances where private companies may need to take measures that are beyond passive self-defence, in order to prevent, interrupt, or recover damage from malicious activities. However, private companies could not be immediately able to discern if the attack is coming from a private actor or from a State. It is unadvisable to suggest that there is an inherent right to self-defence for private companies against a State's security or military forces. However, it is a reality that private companies might be in the best position to undertake active self-defence measures to protect users from a malware. In addition, in these situations, there might be reasons for which the company could or would not be able to give access to its systems to the entity. For these reasons, the private company itself, under the scrutiny and monitoring of the entity, could act as the defence arm of the entity, to the extent that is necessary and proportionate[41].

[41] 'The Need for a Digital Geneva Convention' (n 1).

Conclusion

As the document has proved, there is a lack of willingness of States to feel constrained in their behaviour in the cyberspace.

The main reasons for this finding can be re-summarised in the three points. First, States in the 2015 UNGGE consensus report have drafted rules that they have labelled as voluntary norms. This means that it is relatively clear what the content of cybersecurity norms should be, yet there is not a willingness to consider these as part of international law. Second, States in fact largely do not comply with these voluntary norms. Third, States do not strongly complain about violations of these voluntary norms by other States. All these things suggest that States would be reluctant to join a negotiating table on binding norms for the cyberspace anytime soon. This is confirmed by the fact that States have recently questioned the validity of the 2015 voluntary norms, and have not been able to adopt a consensus report in the 2017 UNGGE.

The importance of having clear written rules establishing norms of good behaviour, such as the 2015 UNGGE voluntary norms, is indubitable. However, these rules still do not have enough traction to generate compliance with them. Thus, setting aside the possibility of a treaty on cyberspace as shown above, compliance with voluntary norms can be said to be the main gap of the current cybersecurity framework. Incentives to compliance should be the primary focus of cyber governance efforts.

Compliance with the norms suggested by the 2015 UNGGE (and the Microsoft rules) will have to be sought through non-conventional means. In this direction, the establishment of a third-party entity could lead to increased political pressure on States to comply with the rules, and it could generate greater social awareness, finally leading to a more secure cyber space.

An analogy with the environmental regulatory framework may be useful in assessing the prospect of cybersecurity norms. Both cybersecurity and pollution represent an externality to private as well as national interests. In environmental law, there was a dilemma between economic interests and protection. Cybersecurity faces a dilemma between innovation and security. Also similarly, although it is relatively clear what is needed to achieve a more secure cyber space, the willingness to implement the necessary measures is not as strong. The same reluctance to compliance that existed for environmental measures was however progressively redressed through creative regulation.

A few key features of the development of international environmental law to keep in mind include:

- until 1972 there were no rules or principles on the environment as such, and regulation was created only through arbitration cases;[42]

[42] Edith Brown Weiss, 'The Evolution of International Environmental Law' [2011] Georgetown Law Faculty Publications and Other Works 3–4 <http://scholarship.law.georgetown.edu/facpub/1669>.

- some of the most important developments were achieved through the private sector, that adopted a common template of requirements that apply across countries for corporations,[43] in a concept indeed similar to that of the Tech Accord;

- the UN Environmental Programme (UNEP) was created before binding treaties were, in a pattern of institutional governance;[44]

- no general agreement was established early on, but rather a number of treaties, each addressing a specific problem, were negotiated. Only later one general agreement to which these previous treaties became protocols was signed;[45]
- the environmental framework was built on the acceptance of certain protecting principles, that could be applied even as technology evolved. This would be a good strategy in the case of cyber issues as well.

The analogy with environmental law obviously has its limits, but it is helpful in showing that when it comes to externalities, rules need to be developed gradually, balancing the interests of the many stakeholders involved, in a bottom-up strategy

In conclusion, the Microsoft proposal raises legitimate concerns about the regulation of State-sponsored cyberoperations. While States have begun to tackle these issues, they seem to be approaching them by recognising that international law applies, but that cyber specific norms are to be abided to only on a voluntary basis. The coherent application of international law can offer some solutions to the

[43] ibid 12.

[44] ibid 5.

[45] ibid.; see also Stockholm Declaration of the United Nations Conference on the Human Environment, Report of the United Nations Conference on the Human Environment, U.N. Doc. A/ CONF.48/14/Rev.1 (1973), in particular principle 21, which provides that "States have [...] 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"; see also Rio Declaration on Environment and Development, Report of the United Nations Conference on Environment and Development, U.N. Doc. A/CONF.151/26/Rev.1 (1992), which addresses in Principle 12 the trade concerns. It provides, inter alia, that "[unilateral actions to deal with environmental challenges outside the jurisdiction of the importing country should be avoided."

problem, as explained in the analysis of the case studies. Nonetheless, it is suggested that a more engaged cooperation between States and the private sector is necessary in order to achieve efficient and universally harmonised solutions that cover all issues relevant to cybersecurity in a specific manner. To this end, a multi-stakeholder discussion on a potential Tech Accord, and the potential institution of a third-party entity could constitute a productive way forward, primarily by fostering dialogue between stakeholders and allowing them to find a way to reconcile their different interests. This will in turn, but only subsequently, inform stronger regulation on cybersecurity.

Annex I: The analogy with the Geneva Conventions is not tenable

As Microsoft calls for the implementation of a "Digital Geneva Convention", it is clear that the title recalls the 1949 Geneva Conventions[46].

Brad Smith, President of Microsoft, affirms that the idea of a Digital Geneva Convention takes inspiration from them[47]. He explains this analogy by affirming that, as the first responders at the battle of Solferino (the battle that inspired the creation of the ICRC) were the medics attached to the respective armies and the civilian volunteers that worked with them, today, in the context of cyberattacks, the first respondents are tech companies.

For these reasons, in the same way as medics and volunteers are treated as "neutrals" in the context of hostilities and for the purposes of the application of the GCs, tech companies should be neutral as well. The analogy is therefore born by equating the wounded with the private citizens who suffer from cyberattacks, and the medics and tech companies, which are the entities that can relief them.

[46] International Committee of the Red Cross, 'The Geneva Conventions of 1949 and Their Additional Protocols'.

[47] Brad Smith, 'What the Founding of the Red Cross Can Teach Us about Cybersecurity' <https://www.linkedin.com/pulse/what-founding-red-cross-can-teach-us-cyber-warfare-brad-smith/>.

Reasonably, Brad Smith is also aware that the analogy with the GCs cannot be taken too far.

There are several issues that arise when comparing the Microsoft proposal with the GCs.

The first problem is that the ideological underpinnings behind the GCs are different than the ones behind the Microsoft proposal, as the former are driven by the need to balance military necessity and the protection of civilians in the context of armed conflict, whereas the latter, as explained in the previous section, would be also applicable in a context that does not amount to armed conflict. This underlying difference leads to a series of difficulties when trying to transpose some IHL principles in the context of the Microsoft proposal.

First, there is a problem with the analogy between the protection of “civilians” and the protection of “private citizens”. This analogy entails in fact a borrowing of the principle of distinction, which presupposes that the category of “civilians” finds a counterpart in the category of “combatants”. However, the same cannot said to be true in relation to the category of “private citizen”, as it is quite problematic to envisage the creation of a counterpart category, especially outside the context of hostilities.

In principle, the protection to the private sector could be understood as meaning the protection of non-state actors. The rationale for this may be found in that States have existing diplomatic avenues and sovereign competences for addressing these attacks, that non-state actors do not have. This is an interesting input, and it could provide persuasiveness to the argument that States should refrain from damaging the private sector through cyber operations. However, the current wording used recalls the Geneva Conventions’ military rationale in an ambiguous manner, one which is unlikely to advance discussions with States.

Secondly, the private sector *per se* does not represent a protected category for the purposes of the GCs, but it would be protected as long as it does not engage in the hostilities, by falling within the category of “civilians”.

Thirdly, as far as the system of reporting vulnerabilities is concerned, this feature is peculiar to the cyberspace, and does not find an analogy in the GCs.

Fourthly, two of principles that govern the use of weapons in IHL are distinction and proportionality. Whilst their application to traditional weapons is quite well-established, the same cannot be said in relation to cyberweapons. This is so because with cyberweapons there seems to be a greater gap than with traditional weapons between their intended use and the actual outcome of the operation. Moreover, it is unclear how these two principles would apply outside the context of hostilities.

	Geneva Conventions	Microsoft Proposal
Analogy between civilians and private citizens	The principle of distinction applies between the categories of civilians and combatants	It is unclear to which categories the principle of distinction would apply, or what category would be the counterpart of the "private citizens"
The private sector status	The private sector is not a protected category *per se*, but only as civilian/civilian object	The private sector would become a protected category
Reporting vulnerabilities		As far as the system for reporting vulnerabilities is concerned, the analogy with the GCs cannot be made, as this is a peculiar feature of cyberspace
Analogy between traditional weapons and cyberweapons	The use of weapons is regulated by the principles of distinction and proportionality.	The principles of distinction and proportionality are difficult to apply because of the unpredictability of cyberweapons and their use outside the context of hostilities

Annex II explores the legal issues that arise when envisaging the implementation of the Microsoft proposal, presenting a deeper inquiry of the legal implications entailed.

Annex II: General issues in governance of the internet

The potential implementation of the Microsoft proposal into an actual binding text also entails considerations about the issues that might arise from a legal perspective.

It should be highlighted that these issues arise especially because of the language used in the Microsoft proposal that heavily recalls principles developed in the context of IHL.

1. The issue of distinction

The principle of distinction in armed conflict establishes an obligation to distinguish at all times between civilian and military targets.[48] Accordingly, under the rules of customary IHL, attacks may only be directed against military targets. Attacks must not be *directed* against civilian targets. An attack which affects civilians and civilian objects is not unlawful as long as it is directed against a military target and the incidental damage to civilians and civilian objects is not excessive[49].

5.3. The principle of distinction does not exist in times of peace and there are difficulties in transposing it in the context of the Microsoft proposal

The principle of distinction is based on the presupposition that there is a category of people that is always a lawful target, military, and another category that enjoys

[48] Jean-Marie Henckaerts and others (eds), *Customary International Humanitarian Law* (Cambridge University Press 2005) chs 1–2.

[49] ibid 1–2.

protection from attacks, civilian. Obviously, in the case of cyber operations, the distinction would have to be made between categories that are different than those recognized by IHL. However, a similar notion of distinction, and of different categories of people and objects, currently does not exist in peace time. In peace time, all people are human beings entitled to the same rights and protections, and the notion of military target simply has no *raison d'être*. While from a theoretical point of view, it is possible to infer that the Microsoft proposal seeks to operate a distinction between the private citizen and governmental objects, in practice it is not obvious to predict that States would be willing to introduce the principle of distinction in a potential legal instrument applicable outside of hostilities, as this would imply that some categories of objects or people would become lawful victims of cyber operations in peacetime.

5.4. The lack of military necessity in times of peace creates the need to establish a new rationale allowing for the definition of certain objects as legitimate targets of cyberoperations

Two further considerations may elucidate the problems arising from the distinction discourse. The idea that combatants and military objectives are targetable at all times during armed conflict finds its rationale in the principle of military necessity, arising from a state of hostilities. States can use lethal force against human beings, and destroy military targets, as a matter of warfare. In peace time, it is difficult to see what motives could give ground to the acceptance that certain objects be legitimate targets of cyber operations, (meaning targets of the use of force, or even interference short of the use of force). That would mean transforming the digital space in a battlefield per se, and certain hostile acts in international relations would no longer be considered as wrongful acts. Aside from the dubious compatibility of such a scenario with existing international law, transforming the cyber space into a space where hostile acts can be lawfully executed, is manifestly undesirable from a policy perspective as well, at least for the risk of escalation that would emerge.

As the case may be, if the principle of distinction were to make its way into internet governance discourse, Microsoft suggests that protected categories would be tech companies, private sector, or critical infrastructure. In detail, Microsoft also argues

that we should "*ban the nation-state hacking of all the civilian aspects of our economic and political infrastructures*".[50] Such a proposal raises two questions. Firstly, since tech companies provide services to governments, it is unclear how the private sector and its critical infrastructure could remain completely immune from attacks, even if these were directed towards lawful targets. Secondly, the notion of distinction stands strikingly at odds with the interconnected digital space, making any prediction about the result of an operation dangerously speculative. Finally, at least a clear definition of the term "critical infrastructure" would need to be provided.

In legal texts, it is common to find vague terms and structural ambiguities that allow for broader and policy-oriented interpretations. However, this is not always a desirable outcome, as it leaves a large degree of discretion to those that prefer not to take the most protective approach. Furthermore, and the dual-role played by most digital infrastructure (i.e. tech companies owning the infrastructure on which both governments and private citizens operate) only exacerbates the interpretative conundrum.

6. The issue of proportionality

As the ideological underpinning that would justify the principle of distinction in cyberoperations remains obscure, an unanswered question of the Microsoft proposal is that of whether the principle of distinction in cyberoperations would also be subject to the principle of proportionality in attack[51].

6.1. The tests on proportionality can lead to different outcomes and it is important to take into account the principle of technology neutrality

In law, there are different rules on proportionality, depending on the regime in which we are operating.

[50] 'The Need for a Digital Geneva Convention' (n 1).

[51] Henckaerts and others (n 48) ch 4.

- Proportionality and Law Enforcement

The measures that are used in investigations and law enforcement procedure may sometimes entail use of otherwise prohibited means, subject to a balance between the severity of the offence that is being prosecuted and the corrective measure that is being envisaged.

In this sense, States may be allowed to possess cyberweapons, but they would have to be usable and used in compliance with the legal framework applicable in times of peace, primarily human rights. For instance, in the cases of Finogenov and others v. Russia[52] and Isayeva v. Russia[53], the weapons used for law enforcement purposes were deemed to be in violation of art. 2 of the European Convention on Human Rights. In the first case, it was the use of opiate gas in order to retrieve hostages in a theatre that was disproportionate; in the second case, it was the bombing of a village that was "manifestly disproportionate" to the achievement of the purpose of effecting a lawful arrest.

- Proportionality in the context of countermeasures

Art. 51 of the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) establishes that "*countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.*[54]

The aim of this article is to establish an essential limit to the intensity of the countermeasure that an injured State may take: it provides that "*a measure of assurance inasmuch as disproportionate countermeasures could give rise to the responsibility on the part of the State taking such measures".*[55] This test is both *"qualitative"* and *"quantitative*".[56]

[52] *Finogenov and others v Russia* Appl Nos 1829903 and 2731103 (ECHR) 20 December 2011.

[53] *Isayeva v Russia* Appl No 5795000 (ECHR) 24 February 2005.

[54] Art. 51, International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries' (2001) Supplement No. 10 (A/56/10).

[55] ibid.

[56] ibid.

- Proportionality in the context of self-defence

Under the rules of *jus ad bellum*, the rule of proportionality establishes that a State is entitled to use military force in self-defence as a response to an armed attack.[57] Customary international law establishes that the force that a State is entitled to use must amount, but not exceed, that needed to repel the attack. The application of the rule on self-defence therefore depends on the definition of armed attack, and the exercise of the right itself depends on whether the State exercising it has been a victim of an armed attack. The applicability of the right to self-defence depends on the threshold that has to be attained by a cyberattack in order to be considered equivalent to an armed attack for the purposes of art. 51 of the UN Charter. Such threshold remains the object of legal debate for the time being.

In its 2013 report, the UN GGE has advised that international law applies to the cyberspace[58]; two years later the group confirmed that the rule of self-defence is implicitly included in the list of those cardinal principles that apply in the realm of cyber.[59] The Report refers to the "*inherent right of states to take measures consistent with international law and as recognized in the UN Charter*"[60]. This statement implicitly refers to self-defence, but the conspicuous absence of the word 'self-defence' can be explained by the aversion of some GGE members to the idea of "*militarization of cyberspace*"[61]. However, it must be mentioned that in 2017 the UN GGE was unable to find a consensus specifically on the issue of whether self-defence can be exercised with regards to a cyberoperation.

[57] Art. 51, 'Charter of the United Nations' (1945) 1 UNTS XVI.

[58] 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (n 10).

[59] '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law' (*CCDCOE*, 31 August 2015) <https://www.ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0> accessed 27 October 2017.

[60] ibid.

[61] ibid.

- Proportionality in the context of IHL

The rule on proportionality in IHL, demanding to balance the anticipated military advantage with the expected civilian damage in attack, only applies in the context of an armed conflict, i.e. under *ius in bello*, notwithstanding whether the armed conflict is national or international. As a result, its applicability is relevant in the context of cyberwar and it falls within the competence of the ICRC to define which kind of weapons would be allowed in hostilities, to accommodate military necessity.

To conclude, even when Microsoft refers to the development of cyberweapons that are limited and precise, it is important to keep in mind that cyberweapons would have to pass different proportionality tests at different moments. From a legal perspective, it would be advisable to keep the focus on the intended use of the weapon and the responsibility of the user of such weapon, rather than on the prohibition of the development of a certain weapon technology as such, which could incidentally represent a violation of the general principle of technology neutrality.[62] The responsibility of the developer of a certain cyber weapon also includes the safe custody of such weapon from third parties that may use in a manner different than that envisioned by the developer.

Notably, the development of cyberweapons is the one norm proposed by Microsoft that cannot be retraced in any State-agreed instrument, highlighting scarce political will in this direction.

7. The issue of "dual-use"

The fact that tech companies are those that provide services to governments is strictly interconnected with the notion of "dual-use" of cyberinfrastructure.

Cyberinfrastructure is used for both civilian and military purposes, and because of this "dual-use", it becomes almost impossible to apply the principle of distinction between civilian and military infrastructure in the realm of cyberspace.

[62] Technology neutrality is here used to indicate the principle according to which there is no distinction between good and bad technology, as this qualification could only be made on the basis of the intended use of such technology.

As the ICRC has already considered, the main humanitarian concern in relation to cyberoperations is the potential impact on the civilian population. In fact, most military network relies on civilian infrastructure, such as undersea fibre optic cables, satellites, routers, nodes; equally, civilian network rely on infrastructure that is used by the military, such as global positioning system (GPS).[63]

8. The issue of non-proliferation

The commitment to non-proliferation seems to be aiming at prohibiting the transfer of cyber weapons if these weapons would be likely to violate human rights obligations.

This concept recalls the 2013 Arms Trade Treaty, which is not a treaty about controlling how many arms a State owns, but it is concerned with the transfer of those arms between countries.

The object and purpose of the Treaty are the establishment of the highest possible common international standards governing the international trade of conventional arms, with the aim of contributing to international and regional peace and security, reducing human suffering, and promoting cooperation, transparency and responsible action by States.[64] Most importantly, art. 7 of the ATT establishes that an export of conventional arms shall not be authorised if, *inter alia*, they would contribute to or undermine peace and security, or could be used to commit or facilitate a serious violation of IHL or international human rights law.[65]

This Treaty could serve as guidance for establishing a commitment to control the transfer of cyberweapons across borders.

An international agreement on the matter already exists. The Wassenaar Arrangement (1996) is a document signed by 41 States[66], aiming at contributing “to

[63] Droege (n 5) 541.

[64] Art. 1 Arms Trade Treaty 2013.

[65] Ibid, art. 7

[66] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of

regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies".[67] This Arrangement is conceived as a document that complements and reinforces, without duplication, the existing control regimes for weapons of mass destruction and their delivery system, as well as other internationally recognised measures designed to promote transparency and greater responsibility. It has recently been amended in order to include "cyberweapons". However, the wording through which this inclusion has been made is problematic. The Wassenaar Arrangement refers, in fact, to "intrusion software", therefore giving a very vague definition of what this encompasses. The main fear is that "intrusion software" covers too much technology and a lot of practices that do not necessarily fall within the scope of protection envisioned by the Arrangement itself. The main fear is that this also includes software developed for research purposes and for enhancing the inter-state cooperation in the fight against cyber-threats. In short, this rule impinges on the collaboration between cybersecurity firms and researches across the world, as they would potentially need export licenses to exchange in order to share the relevant information to provide a remedy to vulnerabilities.

In sum, whilst the rationale behind these two legal instruments can be applied to cyberweapons, the biggest challenge is to define cyberweapons in a way that would not undermine the principle of technology neutrality, but that would encompass those cyberweapons which have the potential of resulting in a violation of IHL, human rights law, or undermining international peace and security.

9. The issue of the defence responsibility

When Microsoft affirms that States should assist the private sector efforts to detect, contain, respond to, and recover from events, the problem it addresses is that the private sector, as the entity that builds, owns, and provides most digital infrastructures, is often the first-line responder in the case of an offensive cyber

Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

[67] 'The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, July 11-12, 1996, as Amended in 2016' <http://www.wassenaar.org/wp-content/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf>.

operation. This is the case regardless of what the primary target of the operation is and of whether it is moved by private or political motives.

9.1. The defence responsibility of the private sector in the cyberspace is a new phenomenon in international relations and there is a gap to be filled

Generally speaking, international law does not provide a framework in which the private sector would be allowed to exercise self-defence in cyberspace. A company that is a victim of a State-sponsored activity, even if the operation was aimed at a governmental item, or moved by political reasons, would not be entitled to act in self-defence against the offending State. However, for economic reasons, ICT companies are increasingly required to engage in increasingly active, as opposed to passive, self-defence measures against cyber-threats.

A framework to allow private companies to act beyond passive self-defence measures indeed requires an accountability scheme with States. This is not impossible to achieve, and could draw inspiration from the Montreux Document, but it will be thoroughly addressed in the final section on the potential role of a third-party entity.

9.2. The assistance in detecting and containing events involves a question of responsibility

The rule proposed by Microsoft needs to be considered against a specific backdrop: in the instance of offensive cyberoperations being state sponsored, the private sector is mostly responsible for the defence action[68]. This is largely new in international relations, and it is in this context that the private sector calls for support, to fill in the power gap of an asymmetrical relationship. As the case may be, the proposal as laid down by Microsoft needs to be considered from a legal perspective in two different phases.

[68] 'Data Breach Investigations Report - 10th Edition' (Verizon 2017).

The first phase is that of assisting in detecting and containing events. This could work both ways, as there would be instances in which either the private sector or the State know first about the intrusion, and in which one could be more effective than the other in containing the event. In this phase, the legal question rotates around the issue of liability, i.e. of responsibility, for events that have adverse effects and that could have been avoided or curbed, by enhanced communication between State agents and the private sector. This aspect will be further explored in the next section on vulnerabilities reporting, as well as in the Menu of Options section envisioning liability schemes in light of the varied nature of cyber operations.

9.3. The assistance in responding and recovering from events remains a matter that pertains to domestic law

The second phase is that of assisting in responding to and recovering from events. In this phase, the question is that of what rules govern the assistance that the State could give to the private sector, and vice versa. Some considerations are in order, when considering the mutual assistance system that is needed to respond once an operation is causing adverse effects. What is sure is that repelling a malicious activity in the digital space often requires action both of the public and of the private sector[69].

[69] Such as disruption of a global botnet and sink-holing of its command-and-control server, for more information see Georg Kerschischnig, Cyberthreats and International Law (Eleven International Publishing ; Sold and distributed in USA and Canada, International Specialized Book Services 2012).

Legal issues	
No targeting of tech companies, private sector or critical infrastructure	• The IHL principle of distinction does not exist in times of peace • The lack of military necessity in times of peace creates the need to establish a new rationale allowing for the definition of certain objects as legitimate targets of cyberoperations • The "dual-use" of cyberinfrastructure is problematic for the principle of distinction • The applicability of the principle of proportionality remains an unsolved question
Assist the private sector efforts to detect, contain, respond to, and recover from events	• The defence responsibility of the private sector is a new phenomenon and there is a legal gap to be filled • The question of the assistance in detecting and containing events involves a question of responsibility • The question of the assistance in responding and recovering from events remains a matter of domestic law
Report vulnerabilities to vendors, rather than stockpile, sell, or exploit them	• Reporting vulnerabilities could come within the State's responsibility to protect its citizens
Exercise restraint in developing cyberweapons, and ensure that any developed are limited, precise, and not reusable	• The application of the principle of distinction remains dubious • The tests on proportionality (law enforcement, countermeasures, self-defence) can lead to different outcomes • It is important to bear in mind the principle of technology neutrality • Non-proliferation is conceived as a negative obligation on States
Commit to non-proliferation activities to cyberweapons	• The commitment does not recall non-proliferation *per se*, but rather the rationale behind the Arms Trade Treaty 2013 (prohibition of transfer of weapons which would violate human rights)
Limit offensive operations to avoid mass events	• There is no definition of "offensive operation" in cyberspace • An offensive operation in cyberspace could lead to a violation of the prohibition of use of force (art. 2(4) of the UN Charter)

Annex III: Factual background of the case studies

Stuxnet

Stuxnet is a computer worm that infected the software of at least fourteen industrial sites in Iran, including a uranium-enrichment plant.[70] Allegedly, it spread from a removable hard disk that showed false digital certificates. Remarkably, it did not require any Internet connection to be able to spread.[71]

The sophistication that the Stuxnet malware required to be developed, suggests that it is the product of the resources of a State[72]. Also, it did not aim at financial gains, but only at spying and destroying Iranian critical infrastructure.[73]

The weaponized code attacked in three phases. Firstly, it targeted devices using Microsoft Windows as the operating system, while replicating itself; secondly, it attacked the Siemens Step7 software which runs vital industrial equipment, such as centrifuges in the Iranian nuclear enrichment program. Finally, once it found its target, it attacked the logic controllers and caused the overspinning of the centrifuges in the nuclear plant.[74] The real trick of the infectious malware was that, instead of simply destroying its target, it modified the functioning of the target, while providing false feedbacks to the outside controllers.[75] This went on and on for months until eventually the centrifuges wore down and broke.[76]

Firstly, unaccountability is cause of main concern. Attribution of a cyber-operation is not an easy task due to the anonymity of the web. Furthermore, despite rumors, neither the US, nor Israel have ever officially confirmed their involvement in creating and developing the weapon.

[70] Kushner (n 33).

[71] ibid.

[72] ibid.

[73] ibid.

[74] ibid.

[75] Ryan Fleming, 'Bits before Bombs: How Stuxnet Crippled Iran's Nuclear Dreams' (*Digital Trends*, 2 December 2010) <https://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/> accessed 17 November 2017.

[76] ibid.

Secondly, the malware proliferated easily for two reasons: it did not require an internet connection to enter and infect the targeted device and, after the attack occurred, the code remained open source. This means that extremist groups and other States could obtain it, modify it, and use it against other civil infrastructure, with even greater consequences.

WannaCry

WannaCry is a ransomware attack that hit more than 330,000 computers in more than 150 countries,[77] and used a malicious software developed to exploit vulnerabilities stolen from the United States National Security Agency, which it had discovered and was stockpiling.[78]

Once stolen, the exploit was turned into a ransomware encrypting consumers' data and demanding a payment in exchange for unblocking them.

Indiscriminately, across the globe, public infrastructures such as government buildings, hospitals as well as business and private computers, were affected.[79] Most notably, England's National Health Service (NHS) was a victim: the staff was locked out of their computers, patients were diverted, surgery and appointments were canceled.[80]

WannaCry has not been attributed to any State or non-State actor yet. However, although North Korea denies any involvement, Microsoft's president claimed that North Korea was behind the event.[81]

The malware kill-switch was found by a young security researcher, known as MalwareTech.[82] Immediately after the event, Microsoft released a patch that could be

[77] Wong and Solon (n 36).

[78] 'The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack' (n 37).

[79] ibid.

[80] Wong and Solon (n 36).

[81] Nicola Harley, 'North Korea behind WannaCry Attack Which Crippled the NHS after Stealing US Cyber Weapons, Microsoft Chief Claims' *The Telegraph* (14 October 2017) <http://www.telegraph.co.uk/news/2017/10/14/north-korea-behind-wannacry-attack-crippled-nhs-stealing-us/> accessed 17 November 2017.

[82] 'Cyber-Attack "Unprecedented" in Scale' (n 38).

installed on older operating systems that had not been updated, and on which the previous patch could not be installed. Microsoft also provided detection and protection services for the victims.[83] However, Microsoft claimed that the NSA should not be stockpiling vulnerabilities in the first place.[84] Indeed, the incident was just the tip of the iceberg of a much broader issue which still remains unsolved, namely that of rights and obligations of State and non-state actors in the cyberspace.

Sony Pictures Entertainment attack

On November 24, 2014, a series of personal data stolen from Sony computers, leaked to the public. These included employees' emails, information about salaries, credit card numbers as well as some of the company's unreleased movies.[85] this attack was very precise and non-reusable. In addition, Sony's operating system was left inoperative for several days.

A hacking group named *Guardians of Peace* claimed responsibility. The FBI and the Obama Administration accused North Korea for the attack[86]. This is plausible, as Kim Jong-un, leader of North Korea, had previously threatened the US of a terrorist attack if the movie "*The Interview*", meant to ridicule and mock the dictator, was released.[87]

Bibliography

a. Treaties

Arms Trade Treaty 2013

[83] Chris Graham, 'NHS Cyber Attack: Everything You Need to Know about "Biggest Ransomware" Offensive in History' *The Telegraph* (13 May 2017) <http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/> accessed 17 November 2017.

[84] Harley (n 81).

[85] Siboni and Siman-Tov (n 39) 646.

[86] Jose Pagliery, 'What Caused Sony Hack: What We Know Now' (*CNNMoney*, 24 December 2014) <http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/index.html> accessed 17 November 2017.

[87] Siboni and Siman-Tov (n 39) 646.

‘Charter of the United Nations’ (1945) 1 UNTS XVI

‘The Geneva Conventions of 1949 and Their Additional Protocols’, International Committee of the Red Cross

b. Legal documents

‘G7 Declaration on Responsible States Behavior in Cyberspace’ (Lucca 2017)

‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (UNGA 2013) UN Doc A/69/723

‘Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security’ (UNGA 2015) UN Doc A/70/174

‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (UNGA 2017) A/72/315

International Law Commission, ‘Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries’ (2001) Supplement No. 10 (A/56/10)

‘Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General’

‘OSCE Permanent Council Decision No.1106. Available at Http://Www.osce.org/Pc/109168?download=true’

Rio Declaration on Environment and Development, Report of the United Nations Conference on Environment and Development, U.N. Doc. A/CONF.151/26/Rev.1 (1992)

Stockholm Declaration of the United Nations Conference on the Human Environment, Report of the United Nations Conference on the Human Environment, U.N. Doc. A/ CONF.48/14/Rev.1 (1973)

‘The Montreux Document on Private Military and Security Companies’ (*International Committee of the Red Cross*, 1 December 2015)

‘The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, July 11-12, 1996, as Amended in 2016’ <http://www.wassenaar.org/wp-content/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf>

‘The White House (2013) FACT SHEET: US-Russian Cooperation on Information and Communications Technology Security. Available at Https://Www.whitehouse.

Gov/The-Press-Office/2013/06/17/Fact-Sheet-Us-Russian-Cooperation-Informa-Tion-and-Communications-Technol'

'The White House (2016) Joint Statement: The United States and India: Enduring Global Partners in the 21st Century. Available at Https://Www.whitehouse.gov/ the-Press-Office/2016/06/07/Joint-Statement-United-States-and-India-Enduring-Global-Partners-21st'

c. Case law

Finogenov and others v Russia [2011] Appl Nos 1829903 2731103 (ECHR)

Isayeva v Russia [2005] Appl No 5795000 (ECHR)

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, (1996) ICJ Rep 226 (ICJ)

d. Books

Henckaerts J-M and others (eds), *Customary International Humanitarian Law* (Cambridge University Press 2005)

Kerschischnig G, *Cyberthreats and International Law* (Eleven International Publishing ; Sold and distributed in USA and Canada, International Specialized Book Services 2012)

Pawlak P, 'Confidence-Building Measures in Cyberspace: Current Debates and Trends' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (Tallinn 2016) <https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf>

Schmitt MN and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017)

Rid Thomas, *Cyber War Will Not Take Place* (Oxford University Press 2013)

e. Journal Articles and Research Papers

Brown Weiss E, 'The Evolution of International Environmental Law' [2011] Georgetown Law Faculty Publications and Other Works <http://scholarship.law.georgetown.edu/facpub/1669>

Droege C, ‘Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians’ (2012) 94 International Review of the Red Cross 533

Radunovic V and the DiploFoundation team, ‘Towards a Secure Cyberspace via Regional Co-Operation’ (DiploFoundation 2017)

Siboni G and Siman-Tov D, ‘Cyberspace Extortion: North Korea versus the United States’ (2014) No. 646 INSS Insight

f. Reports

‘Data Breach Investigations Report - 10th Edition’ (Verizon 2017)

NATO Policy on Cyber Defence Factsheet 2016

g. Newspaper articles

‘Cyber-Attack “Unprecedented” in Scale’ *BBC News* (13 May 2017) <http://www.bbc.com/news/world-europe-39907965> accessed 17 November 2017

Graham C, ‘NHS Cyber Attack: Everything You Need to Know about “Biggest Ransomware” Offensive in History’ *The Telegraph* (13 May 2017) <http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/> accessed 17 November 2017

Harley N, ‘North Korea behind WannaCry Attack Which Crippled the NHS after Stealing US Cyber Weapons, Microsoft Chief Claims’ *The Telegraph* (14 October 2017) <http://www.telegraph.co.uk/news/2017/10/14/north-korea-behind-wannacry-attack-crippled-nhs-stealing-us/> accessed 17 November 2017

Kushner D, ‘The Real Story of Stuxnet’ (*IEEE Spectrum: Technology, Engineering, and Science News*, 26 February 2013) <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet> accessed 17 November 2017

Pagliery J, ‘What Caused Sony Hack: What We Know Now’ (*CNNMoney*, 24 December 2014) <http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/index.html> accessed 17 November 2017

Spetalnick M and Martina M, ‘Obama Announces “understanding” with China’s Xi on Cyber Theft but Remains Wary.’ (26 September 2015) <http://www.reuters.com/article/2015/09/26/us-usa-china-idUSKCN0RO2HQ20150926#QCl52gO5xlJVWVja.97>

‘What Is WannaCry Ransomware and Why Is It Attacking Global Computers? | Technology | The Guardian’

<https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20> accessed 27 October 2017

Wong JC and Solon O, 'Massive Ransomware Cyber-Attack Hits Nearly 100 Countries around the World' *The Guardian* (12 May 2017) <http://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs> accessed 17 November 2017

Zetter, K, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon' (*WIRED*) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> accessed 17 November 2017

h. Blog posts

'2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law' (*CCDCOE*, 31 August 2015) <https://www.ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0> accessed 27 October 2017

'A Tech Accord to Protect People in Cyberspace | Microsoft Cybersecurity' <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-tech-accord-to-protect-people-in-cyberspace> accessed 17 November 2017

'An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?' (*CCDCOE*, 10 February 2015) <https://www.ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new> accessed 17 November 2017

McKay A and others, 'International Cybersecurity Norms - Reducing Conflict in an Internet Dependent World' (Microsoft 2014) <https://www.microsoft.com/en-us/download/details.aspx?id=45031> accessed 1 December 2017

Smith B, 'What the Founding of the Red Cross Can Teach Us about Cybersecurity' <https://www.linkedin.com/pulse/what-founding-red-cross-can-teach-us-cyber-warfare-brad-smith/>

'The Need for a Digital Geneva Convention' <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> accessed 17 November 2017

'The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack' <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/> accessed 17 November 2017

i. Other

'G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015'

Sony Pictures Entertainment, ‘Sony Notice Letter’ (8 December 2014) <https://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf>