University of Aberdeen

School of Law

Working Paper Series

002/19

Centre for Commercial Law

Research Centre for Constitutional and Public International Law

‘Towards a State-Private Actor Partnership in Securing Cyberspace ‘

By:

Dr. Irene Couzigo

Towards a State-Private Actor Partnership in Securing Cyberspace

Dr. Irene Couzigou

Senior Lecturer in International Law at the
University of Aberdeen School of Law

Email address: irene.couzigou@abdn.ac.uk

1. Introduction

As the reliance on digital technology grows so does the possibility for a State or non-State actor to harm another State or non-State actor through cyber means in cyber space. Considering the rapid development of the "Internet of Things", the private sector in particular faces a growing risk of malicious cyber operations. Cyber space is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information and communications technology.[1] In the early to mid-1990s it was argued that cyber space was an a-territorial and borderless environment different from the physical and bonded spaces that are subject to sovereign claims. Cyber space was considered to be an area *sui generis*, outside of both State sovereignty and regulation. As explained by some, the cyber domain could not be regulated by laws based on geographic location but had to have its own legal system based on selfregulation.[2] Others have likened cyber space to the global commons, domains that lie outside the exclusive sovereignty of States, such as the high seas, outer space and the Antarctic, and proposed that it should be governed collectively for the common benefit of all mankind. For example, the 2005 US Strategy for Homeland Defense and Civil Support stated that "the global commons consist of international waters and airspace, space, and cyber space".[3]

[1] Daniel T Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (ed.), *Cyberpower and National Security*, Washington, DC: National Defense University Press.Kuehl, 2009, p. 28.

[2] David R Johnson and David Post, "Law and Borders – The Rise of Law in Cyberspace", *Stanford Law Review*, 1996, p. 48.

[3] Strategy for Homeland Defense and Civil Support, *Department of Defense*, USA, 2005, p. 12, at https://www.hsdl.org/?view&did=454976

In reality, cyber space is neither a new form of "outer space", nor a global common where no State exercises its jurisdiction. Indeed, cyber space relies on physical elements such as computers, routers, servers and cables that are territorially based. A cyber operation moves on a network that is generally physically located in one or several States, except when the cyber operation uses undersea cables or satellite transmissions. However, in that latter case, the cyber operation takes place on an owned facility where the owner is subject to a country and to its laws.

States do exercise their sovereign authority and territorial jurisdiction over physical infrastructure based in their territory that supports cyber activities – this encompasses the State's land area, its internal waters, its national airspace, when applicable its territorial sea and its archipelagic waters – or an area under their exclusive control – for example, a territorial area occupied by the State or a State warship on the high seas.[4] Thus, States exercise their sovereign authority over cyber conduct resident or transiting through their territory. States have, in fact, regularly asserted their sovereign authority and jurisdiction over cyber activities conducted on their territory, and thus the implementation of international norms deriving from the principle of sovereignty.[5] In its 2015 report, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security stated: '[S]tate sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT[Information and Communications Technology]-related activities and to their jurisdiction over ICT infrastructure within their territory".[6] The UNGGE was composed of 20 States' representatives, including the most important States in information technology: China, the USA, Russia, and Israel.[7]

If States exercise their sovereign authority over the cyber infrastructure based on their territory, they have only limited sovereign authority over other, non-physical layers of cyber space. They do not control the use of the cyber infrastructure located on their territorial base or

[4] Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace", in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, Tallinn, NATO CCD COE Publication, 2013, pp. 193–194.

[5] Wolff Heintschel Von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, 2013, p. 126

[6] UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, Report 2015 UN Doc. A/70/174, para. 27

[7] Australia, Botswana, Brazil, Canada, China, Cuba, Egypt, Estonia, Finland, France, Germany, India, Indonesia, Japan, Kazkhstan, Kenya, Mexico, Netherlands, Republic of Korea, Russia, Senegal, Serbia, Switzerland, United Kingdom, United States.

any other area under their exclusive control. This is true of poorly technologically developed States, yet also of technologically developed States like the United States - whose legal culture currently precludes the level of monitoring that would be necessary to completely monitor cyber communications. Furthermore, a high portion of the world cyber infrastructure is owned by private entities, which makes the control of cyber traffic by States even more difficult.[8] So, despite the will to exert sovereign authority over cyber space, no State is currently able to completely prevent, react to, or even detect cyber attacks on or emanating from the cyber infrastructure within its territorial borders. Cyber attacks are defined broadly in this paper and are understood as operations in cyber space that compromise or impair the confidentiality, availability, or integrity of electronic information, information systems, services, or networks, whatever the objective of the cyber attacker, economic, political or otherwise.

Under international law, States have to respect the international obligation to prevent harmful international cyber operations committed by non-State actors from their territory.[9] However, in practice, States lack the skills or staffing to protect the networks on their territory and to react to cyber attacks targeting entities based on their territory or elsewhere. It is particularly true of cyber attacks against the private sector. Indeed, much of the State cyber security capacity is consumed by the protection of cyber State assets and services as well as of critical national infrastructures, such as water distribution, health, energy, transportation, banking and finances' services.[9] Furthermore, State investigation could be slowed down or stopped if the cyber attack is traced back to a foreign computer. Indeed, the foreign State may not be willing to cooperate or may be hampered by resources' constraints. Thus, overall, States are slow in deterring and prosecuting cyber attackers targeting private companies. Worse, most of the cyber attacks are unresolved.[10] State law enforcement is overwhelmed both by the technical unfamiliarity of the crimes and the number of attacks occurring in the cyber world.

---

[8] Paul Rosenzweig, "Cybersecurity and Public Goods", Hoover Institution, Stanford University, 2012, p. 2, at http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf [9] Irène Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations", *International Review of Law, Computer & Technology*, 2018, pp. 37-57.

[9] Sean M Condron, "Getting It Right: Protecting American Critical Infrastructure in Cyberspace", *Harvard Journal of Law & Technology*, 2007, vol. 20, 416.

[10] Patrick Lin, "Forget About Law and Ethics - Is Hacking Back Even Effective?", *Forbes*, 26 September 2016, at https://www.forbes.com/sites/patricklin/2016/09/26/forget-about-law-and-ethics-is-hacking-backeveneffective/#7d0ccfe047d8.

Cyber attacks, such as the theft of intellectual property, the manipulation of banking data, or holding data hostage for ransomware generate high costs for the private sector.[11] Thus, in light of the ineffective action of States in securing cyber space, private actors, whether multinational information corporations (Google, Facebook, Yahoo, Microsoft etc.) or private cyber security companies (Novetta, CrowdStrike Mandiant, FireEye etc.) hired by other companies, have reacted to harmful cyber operations themselves, without any coordination with a State.[12] For instance, when Google became the victim of a widespread and sophisticated attack attempting to steal intellectual property and email accounts at the end of 2009, it hackedback immediately to stop the attack.[14] This paper will refer to "companies" as non-State actors whose conduct cannot be attributed to a State. Indeed, the behaviour of a State-owned company is in principle not attributable to the State unless the corporation exercised public power or the State used its ownership interest in order to achieve a particular result.[131415] The private sector's cyber response goes by the name of "active cyber defence". Active cyber defence activities may stay in the network of the defender or intrude into the network of the attacker. This second category of cyber defence operations are known as "hack-back activities". Cyber defence measures may stay within the territory of a State or cross an international border. Therefore, the question arises as to whether private cyber defence strategies are regulated under international law.

In its second section, this paper will analyse the lawfulness of hacking-back by private actors. After having specified the different categories of cyber defence measures, the paper will argue that, in principle, international law neither recognises the right of, nor prohibits, hackingback by private entities. A State, however, would violate its obligation of due diligence to prevent harmful international activities if it did not prevent damaging international cyber defence activities perpetrated from its territory. In its third section, this paper will show that hack-back activities create many legal and political difficulties, which raises the question of their regulation under international law. Finally, this article will conclude that non-State actors should not be allowed by States to respond to harmful cyber operations on their own. It will

[11] Wyatt Hoffman and Ariel E. Levite, *Private Sector Cyber Defense,* Washington, Carnegie Endowment for International Peace, 2017, p. 3.

[12] Jan E Messerschmidt, "Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm", *Columbia Journal of Transnational Law,* 2013, vol. 52, p. 277.

[14] David E. Sanger and John Markoffjan, "After Google's Stand on China, U.S. Treads Lightly", *New York Times,* 14 January 2010.

[13] Art. 8 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, pp.

[14] -

[15] , at http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

recommend cooperation between States and non-State actors in reacting to damageable international cyber operations, circumscribed by international standards, and will study how this might occur.

2. Hack-back Activities by non-State Actors under International Law

2.1. Defining and Categorising Active Cyber Defence Measures

First active cyber defence must be distinguished from passive cyber defence. Passive defence strategies are focused on preventing unauthorised cyber intrusions. They produce effects only within an actor's own network. They primarily concern the resort to perimeter-focused tools like firewalls, patch management procedures, internal traffic monitoring, and antivirus software. Passive defence measures are necessary for good cyber security. However, they may be insufficient to defend against advanced cyber attacks.[16]

Active cyber defence techniques allow to potentially interrupt cyber attackers at different stages of the attack. They capture a range of active cyber security activities to detect, analyse, mitigate, or stop malicious activity on one's network. They may cross the threshold of the actor's own network, and produce consequences on the network of another, which may involve a cross-border transit. Active cyber defence measures are either defensive or offensive.

Measures aimed at securing one's own system or preserving operational freedom can be characterised as defensive. These are, for instance: using a sandbox or tarpit that provides barriers that slow or halt and examine incoming traffic that may be suspicious; resorting to a honeypot that attracts a person who attempts to penetrate another computer without authorisation into an isolated system to identify him and prevent his access; deception that allows an adversary to steal documents containing false or misleading information and thus makes it difficult for the attacker to access the desired information; using a beacon that notifies the owner in case of data's theft; using a more impactful beacon designed to return to the victim information about the Internet protocol (IP) address and network configuration of the computer system that a stolen file is channelled through; various means of intelligence gathering that can collect information on cyber threats inside and outside of one's system.[17]

[16] Centre for Cyber & Homeland Security, "Into the Gray Zone", Project Report October 2016, p. 9, at https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf [17] Centre for Cyber & Homeland Security, *op. cit.* note 16, pp. 9-10.

Other active cyber defence measures occur outside the actor's network and are therefore offensive. They include in particular: taking down a botnet which uses networks of compromised computers to launch attacks; sinkholing, which redirects malicious traffic to a system under control of the defender; recovering information that has been stolen in the network of the intruder or, alternatively, altering or destroying this information; forward intelligence gathering, including in external networks, to collect evidence about the attacker (for instance, photographing him by using his own webcam). Active cyber defence activities also encompass aggressive operations committed with the intent to disrupt or destroy information or external networks.[17] Those operations are, for instance: the implantation of malwares in the network of the attacker to disrupt the computer or system of the attacker to impede his ability to attack, by, for example, locking down his computer; the upload of malwares to damage the computer or system of the attacker to stop or prevent further attacks.[19] Many companies are already using active cyber defence measures, including the most aggressive ones.[18] They do it themselves or they hire a cyber security company to provide for their cyber defence.

Active cyber defence measures that intrude into one's network are likely to lead to different levels of harm, from affecting the confidentiality of data to corrupting the integrity and availability of systems. The disruption of networks may even cause damage to the physical world, for instance when the system monitoring the traffic of planes in a State is disabled. Given the interconnected character of information and technology communications, aggressive cyber defence measures may cross an international border. This paper only addresses those cyber defence operations by non-State actors that commit an unauthorised intrusion into someone else's network, even if they do not produce harm per se, and that cross an international border. They are included into the category of "hack-back activities".

2.2. Absence of a Right to Hack-Back

Under international law, a State can react with acts of retorsion, countermeasures or even by self-defence to a damageable act, for instance a detrimental cyber operation, perpetrated by

[17] Centre for Cyber & Homeland Security, *op. cit.* note 16, p. 12.
[19] Wyatt Hoffman and Ariel E. Levite, *op. cit.* note 12, p. 8.
[18] Kristen E. Eichensehr, "Public-Private Cybersecurity", *Texas Law Review*, 2017, vol. 95, p. 499.

another State.[19] Furthermore, a State could also adopt acts of retorsion or countermeasures against a State that does not comply with its obligation of due diligence to prevent the commission of harmful international cyber operations by non-State actors from its territory. An act of retorsion is an unfriendly measure, lawful in itself, adopted by a State in reaction to the unfriendly conduct of another State, whether that conduct is lawful or not.[20] A typical example of an act of retorsion is the disruption of diplomatic relations or the withholding of economic assistance. An act of retorsion could also take a cyber form and be a hack-back act.

A countermeasure is a measure that would be unlawful if it were not taken by a State in response to an internationally wrongful act by another State.[21] An example of countermeasures is the temporary non-performance of an international treaty obligation towards the responsible State. The purpose of a countermeasure is only to induce the responsible State to comply with its obligation of cessation of its wrongful act or its obligation of reparation for the damage caused. A countermeasure cannot involve the use of armed force.[22] Thus, the reacting State cannot adopt hack-back measures that could be assimilated to a resort to force, because the effects of those measures would be equivalent to the effects of a resort to force, namely physical destruction, human injuries or human deaths.[2324] Furthermore, countermeasures cannot infringe obligations for the protection of fundamental rights, obligations of a humanitarian character prohibiting reprisals, and obligations arising from peremptory norms of general international law.[2526] Finally, countermeasures must be proportionate to the harm suffered.[27]

As they are also subjects of international law, international organisations are allowed to adopt acts of retorsion in reaction to a conduct of a State or another international organisation.

---

[19] A cyber operation attributed to a State whose consequences in another State are similar to those of a traditional armed attack, namely severe physical damage, important human injuries or numerous human deaths can be seen as an armed attack triggering the right to self-defence. Irène Couzigou, "The Challenges Posed by Cyber-Attacks to the Law in Self-Defence", in August Reinisch, Mary E Footer and Christina Binder (ed.), *International Law and …,* Oxford and Portland, Hart Publishing, 2016, pp. 250-253.

[20] Nigel White and Ademola Abass, "Countermeasures and Sactions", in Malcolm D. Evans (ed.), *International Law*, Oxford, OUP, 5th ed., 2018, pp. 527-529.

[21] Art. 49 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, p. 129, *op. cit.* note 15. See also Nigel White and Ademola Abass, *op. cit.* note 22, pp. 524-526.

[22] Art. 50 (1) Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, p. 131, *op. cit.* note 15.

[23] Irène Couzigou, "The Challenges Posed by Cyber-Attacks to the Law in Self-Defence", *op. cit.* note 21, pp.
[24] -251.

[25] Art. 50 (1) Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, p.
[26] , *op. cit.* note 15.

[27] Art. 51 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, p. 134, *op. cit.* note 15.

They could also adopt countermeasures in response to the breach of an international obligation by a State or another international organisation that affects one of their rights, under similar conditions than the ones for countermeasures by States.[28] The conclusion of this short analysis on international non-forcible reactions to internationally wrongful acts is that they can only be taken by a State or an international organisation and only in response to the violation of an international obligation by another State or international organisation. The rules related to nonforcible reactions to wrongful acts under international law concern only subjects of international law and do not give the right to respond to private actors, in a cyber or other way.

Similarly, non-State actors could not rely on the right to self-defence under international law to legally justify their action in cyber defence. In accordance with Article 51 of the UN Charter, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations". Only members of the United Nations, thus States, can resort to the right to self-defence in reaction to an armed attack. The right to self-defence in customary international law is also only a right of States. If it is now recognised that non-State actors (in particular terrorist organisations) can perpetrate an armed attack, it has not been acknowledged by States or the international legal doctrine that non-State actors can be the victims of armed attacks and do have the right to self-defence.[29] Thus, the international right to self-defence does not give the right to hack-back to private actors.

Yet if international law does not explicitly provide for a right for private companies to counter-hack, it may do so implicitly. Indeed, international rules of self-protection may, by analogy, give the right to private actors to hack-back. Resort to analogies is often the legal reasoning used in areas not yet regulated by law. The right of hot pursuit of pirates in the sea provides for the closest legal analogy with international hacking-back against the author of a harmful international cyber operation. Indeed, the sea constitutes a space where goods can be

[28] Art. 5 and Art. 51 to 57 Draft Articles on the Responsibility of International Organizations, p. 6 and pp. 12-14 respectively, at http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf

[29] See in particular SC Resolution 1373 that recognised the right to self-defence against the Al-Qaida organisation, although this organisation was a non-State actor, and thus implicitly acknowledged that Al-Qaida had committed an armed attack. UN Doc SC/1373/2001, preamble. See also the argument provided by most of the States that intervened in Syria from 2014 that they had a right to self-defence against the Islamic State. This implies that the Islamic State had perpetrated armed attacks. Irène Couzigou, "The Fight against the 'Islamic State' in Syria: Towards the Modification of the Right to Self-Defence?", *Geopolitics, History, and International Relations*, vol. 9, 2017, p. 87.

transported; similarly, cyber space is a space where communications are conveyed. Pirates steal physical property; similarly, cyber attackers may steal intellectual property.[30] The Convention on the Law of the Sea, as well as the older and less ratified Convention on the High Seas, both authorise a State party to engage in hot pursuit of a foreign ship if it has reasons to believe that the ship has violated the laws and regulations of that State. [31] In accordance with both conventions, the pursuit "must be commenced when the foreign ship or one of its boats is within the internal waters, the archipelagic waters, the territorial sea or the contiguous zone of the pursuing State".[32] The pursuit must cease "as soon as the ship pursued enters the territorial sea of its own State or of a third State".[33] Hack-back measures, in particular those taken to recover stolen data in the network of the intruder, could be assimilated to the hot pursuit of pirates. The Convention on the High Seas and the Convention on the Law of the Sea are codification conventions. Furthermore, the Convention on the Law of the Seas has been widely ratified.[34] Thus, it is here argued that the right of hot pursuit is customary. However, only the State has the right to hot pursuit, as is made clear: the "right of hot pursuit may be exercised only by warships or military aircraft, or other ships or aircraft clearly marked and identifiable as being on government service".[35] Thus, the law of piracy cannot be translated into cyber space so as to legally justify hacking-back perpetrated by non-State actors.

2.3. A Limited Prohibition to Hack-Back

The Statute of the International Criminal Court (ICC) imposes the international criminal responsibility to individuals who perpetrate certain behaviours, namely genocide, crimes against humanity, war crimes and crimes of aggression. A crime of aggression must be committed by a State – or "by a person in a position effectively to exercise control over or to

[30] Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures", *Stanford Journal of International Law*, 2014, vol. 50, p. 110.

[31] Art. 111 (1) Convention on the Law of the Sea of 10 December 1982, at http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf; Art. 23 (1) Convention on the High Seas of 29 April 1958, at https://www.gc.noaa.gov/documents/8_1_1958_high_seas.pdf

[32] Art. 111 (1) Convention on the Law of the Sea, *op cit.* note 32. See also Art. 23 (1) Convention on the High Seas, *op cit.* note 32.

[33] Art. 111 (3) Convention on the Law of the Sea, *op cit.* note 32. See also Art. 23 (2) Convention on the High Seas, *op cit.* note 32.

[34] The Convention on the Law of the Sea has 168 Parties as of 8 June 2019.

[35] Art. 111 (5) Convention on the Law of the Sea, *op cit.* note 32. See also Art. 23 (4) Convention on the High Seas, *op cit.* note 32.

direct the political or military action of a State"[36] – and does therefore not concern the situation of hack-back by a non-State actor. Private cyber hack-back measures could however, in exceptional circumstances, be assimilated to a genocide, to a crime against humanity or to a war crime. Article 6 of the Statute of the ICC reproduces Article II of the Convention on the Prevention and Punishment of the Crime of Genocide of 1948 and corresponds to customary international law.[37] For this provision, genocide is constituted by one of the following acts committed with the intention to destroy a national, ethnical, racial or religious groups: "[k]illing members of the group", "[c]ausing serious bodily or mental harm to members of the group"; "[d]eliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part", "[i]mposing measures intended to prevent births within the group", "[f]orcibly transferring children of the group to another group".[38] Thus, we could imagine the situation where the representative of a political organisation hostile to a particular ethnical group and in reaction to detrimental cyber conduct perpetrated by that group, shuts down computers controlling waterworks and dams in order to generate a flood in the region inhabited by the group with the purpose of killing it.

The definition given of crimes against humanity by Article 7 of the Statute of the ICC crystallises to a large extent customary international law.[39] A crime against humanity may be murder, extermination, enslavement, deportation, imprisonment, torture, sexual violence, persecution, enforced disappearance of persons, the crime of apartheid or other acts of a similar character, perpetrated as part of an attack directed against a civilian population and with knowledge of the attack.[40][41][42][39][40] To constitute a crime against humanity the offense must be extremely grave and be part of a pattern of misbehaviour against a population. It may be committed by an individual not acting on behalf of an official authority, provided he/she behaves in unison with a general State policy.[41][42] Here again, a private cyber hack-back operation could, in certain limited circumstances, be assimilated to a crime against humanity,

[36] Art. 2 (1) Amendments to the Rome Statute of the ICC, 11.6.2010, at https://asp.icccpi.int/iccdocs/asp_docs/RC2010/AMENDMENTS/CN.651.2010-ENG-CoA.pdf

[37] Antonio Cassese, Paola Gaeta, Laurel Baig, Mary Fan, Christopher Gosnell, Alex Whiting, *International Criminal Law*, Oxford, OUP, 2013, 129.

[38] Art. 6 Rome Statute of the ICC, 17.7.1998, at https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-
[36] a655eb30e16/0/rome_statute_english.pdf

[39] Antonio Cassese, Paola Gaeta, Laurel Baig, Mary Fan, Christopher Gosnell, Alex Whiting, *op. cit.* note 37, pp. 105-108.

[40] Art. 7 Rome Statute of the ICC, *op. cit.* note 38.

[41] Antonio Cassese, Paola Gaeta, Laurel Baig, Mary Fan, Christopher Gosnell, Alex Whiting, *op. cit.* note 37, p.

[42] .

entailing the international criminal responsibility of its author. Such would be the case of an individual, who, as a cyber hack-back measure and in support of the policy of a State, disables the systems that control the reactor of a nuclear power plant, with the intent to release radioactive materials and exterminate a civilian population.

War crimes are serious violations of customary or treaty rules belonging to the international law of armed conflict. The Rome Statute of the ICC gives a quite precise definition of war crime that can be seen as customary.[43] For its Article 8,[44] war crimes are grave breaches of the four Geneva Conventions of 1949 or other "serious violations of the laws and customs applicable in international armed conflict, within the established framework of international law".[45] Grave breaches are for instances "wilful killing" or "wilfully causing great suffering, or serious injury to body or health" "not justified by military necessity and carried out unlawfully and wantonly" against civilians.[46] An international armed conflict takes place whenever there is a resort to armed force between two or more States, or between a State and a national liberation movement, in conformity with the First Additional Protocol of 1977.[47] Thus, the leader of a national liberation movement engaged in a conflict against a State might be seen as perpetrating a war crime if, in reaction to harmful cyber operations perpetrated by the State, he/she cuts down the energy supply of hospitals and thereby wilfully caused the death of, or serious injury to, many civilians. For the Statute of the ICC, war crimes also consist in serious violations of Article 3 common to the four Geneva Conventions, against persons not taking part in the hostilities, in the case of a non-international armed conflict.[48] Conflicts not of an international character are large scale hostilities, other than simple internal tensions, riots or sporadic acts of armed violence, between the State and organised non-State entities, or between two or more organised groups within a State.[49] Common Article 3 of the Geneva Conventions prohibits for instance each party in an internal conflict from exercising violence against persons not taking part in the

[43] *Nils Melzer*, *International Humanitarian Law*, Geneva, International Committee of the Red Cross, 2016, p. 286.
[44] Art. 8 Rome Statute of the ICC, *op. cit.* note 38.
[45] Art. 8 2 a) and b) Rome Statute of the ICC, *op. cit.* note 38.
[46] Art. 147 Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12.8.1949, at https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=F8D322BF3C02 16B2C12 563CD0051C654. Other grave breaches are defined in the following provisions: Articles 50, 51, and 130of the First, Second, Third Geneva Conventions, respectively, as well as in Article 85 of the First Additional Protocol of 1977.
[47] Art. 1(4) Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8.6.1977, at https://ihl-databases.icrc.org/ihl/INTRO/470.
[48] Art. 8 2 c) Rome Statute of the ICC, *op. cit.* note 38.
[49] Gary D. Solis, *The Law of Armed Conflict*, New York, CUP, 2017, pp. 163-164.

hostilities, "in particular murder of all kinds, mutilation, cruel treatment and torture".[50] Thus, the leader of a terrorist organisation engaged in a conflict against the government of a State might commit a war crime if, in reaction to a harmful cyber operation by the State - for instance, an operation that closes the network the movement uses to communicate -, he/she disabled the electronically controlled water distribution of the State with the intent to create great human suffering.

The circumstances under which cyber hack-back operations by individual non-State actors would constitute a genocide, a crime against humanity or a war crime are rare. Indeed, they would have to occur in reaction to an initial harmful cyber operation. Furthermore, hack-back activities would have to fulfil strict requirements in order to correspond to a genocide, a crime against humanity or a war crime. It is also to be noted that authorities of political organisations, whether States or other political entities, tend to commit those crimes. They are unlikely to be perpetrated by representatives of companies.

The Convention on Cybercrime of the Council of Europe of 2002 is the only international treaty to date that addresses cyber behaviours of non-State actors. It has been ratified or acceded to by a majority of Council of Europe Members, as well as a number of non-Member States.[51] The Convention on Cybercrime requires the 63 State Parties to criminalize offences against the confidentiality, integrity and availability of computer systems (illegal access, illegal interception, data interference, system interference, misuse of devices), computer-related offences (forgery, fraud), content-related offences related to child pornography, and offences related to the infringements of copyrights and related rights.[52]

The Convention remains silent on a right to counter-hack in reaction to a harmful cyber conduct. The only reference to cyber-defence is made by the explanatory report.[53] It explains that the cyber operations referred to by the Convention on Cybercrime are "not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, *self-defence* or necessity, but where other principles or interests lead to the exclusion of criminal liability" (we underline). Thus, the explanatory report suggests

[50] Art. 3 1) a) Geneva Convention relative to the Treatment of Prisoners of War, 12.8.1949, at https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf
[51] Council of Europe, *ETS* No. 185, 23 November 2001.
[52] Number of States Parties as of 8 June 2019.
[53] Council of Europe, Art. 38 explanatory report to the Convention on Cybercrime, *ETS* No. 185, 23 November 2001.

that State Parties could exclude criminal responsibility for the offenses of the Convention on Cybercrime if they occur pursuant to self-defence or cyber-defence. The explanatory report is of significance because it constitutes a rare international recognition of a right to cyber-defence in reaction to a cyber conduct. It is however only meant to facilitate the implementation of the Convention, and not to provide its authoritative interpretation. Thus, hack-back operations are included into those cyber activities to be criminalised by the States party to the Convention on Cybercrime.

Here, it is worth mentioning the Active Cyber Defense Certainty (ACDC) Act, introduced to the American House of Representatives at the end of 2017. It provides for exceptions to the Computer Fraud and Abuse Act, which prohibits access to computers without authorisation. Under the proposed law, it would be legal for the victim of a "persistent unauthorised intrusion" to use "active cyber defense measures" to access the systems of the attacker to "establish attribution", to "disrupt continued unauthorized activity against the defender's own network" or to "monitor the behaviour of an attacker".[54]

In conclusion, hack-back activities are cyber offenses in all States party to the European Convention on Cybercrime. Here, private actors are not prohibited from hacking-back under international law, but under the domestic law of all States party to the Convention. Moreover, other States not party to the Convention may criminalise the unauthorised intrusion into a network and thus cyber counter-hack.[55] More generally, as illustrated in section 2 of this paper, international law neither provides a right to hack-back to private actors, nor imposes a general prohibition on them to do so. However, given the possible impact of private hacking-back on the international scene, international law should regulate counter-hack activities, as explained below.

3. Difficulties Raised by Hack-Back Activities by non-State Actors

3.1. Advantages of Hacking-Back

[54] H.R.4036 - Active Cyber Defense Certainty Act, at https://www.congress.gov/bill/115thcongress/housebill/4036/text

[55] For instance, all G8 countries criminalise unauthorised access to a computer to a greater or lesser extent. Amanda N Craig, Scott J Schackelford & Janine S Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis", *American Business Law Journal*, 2015, vol. 52, issue 4, pp. 18-20.

The main argument in favour of hacking-back by non-State actors is that States are not in a position to protect those actors from harmful cyber operations effectively. In practice, private actors may be more efficient than States to attribute, and respond to, cyber attacks. Indeed, attribution in cyber space is notoriously difficult. First, the cyber operation must be traced back to its source, that is, to a computer. It is true that devices connected to the Internet are assigned IP addresses that reveal the geographic location. Cyber perpetrators however can mask their IP address through the use of cost-free anonymization services such as the I2P Network and the Tor Project. They can also reroute their cyber conduct over hacked computers of innocent users which assigns it a different IP address. In addition, mobile phones are increasingly providing access to the Internet and the wide availability of non-registered SIM cards allow users to surf the Internet without any form of identification required. Finally, the collection of evidence in the cyber context is particularly difficult and slow. Indeed, since cyber attacks often transcend borders, different State normative frameworks need to apply. Furthermore, many cyber attacks are identified as such only after an average of 150-200 days. For instance, interruption of the provision of electricity could first been seen as a cyber incident although it may have been the initiative of a cyber attacker. [56] Meanwhile, the integrity of digital forensics is vanishing quickly. The second stage in the attribution's procedure is the identification of the person who sat behind the computer. In the third stage of the attribution's process, the affiliation of that person must be established. Depending on the legal nexus between that person and a State, his conduct may be attributable to a State. Problems of attribution at this stage are not peculiar to the cyber context. They are addressed by the Articles on State Responsibility for Internationally Wrongful Acts. Most of these are customary.[57] The more time elapses after a cyber attack, the harder the attribution becomes. Thus, the victim of a cyber attack may be in a better position to attribute a cyber attack than a State law enforcement authority, in particular when the cyber attacker is still online.

Countering imminent or ongoing cyber attacks necessitates quick responses. For instance, a virus spreads quickly, which requires immediate action in order to prevent or mitigate the damage it may cause. However, States are usually slow in reacting to cyber attacks and in

[56] Thomas Reinhold and Matthias Schulze, "Digitale Gegenangriffe", Arbeitspapier, 2017, pp. 9-10 at https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf.
[57] Chapter II Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, pp. 38-54, *op. cit.* note 15.

prosecuting cyber attackers.[58] Private victims may be able to respond more efficiently and more quickly than States to harmful cyber operations. It is especially true of leading digital companies such as Google, Microsoft or Apple that possess a better cyber expertise than most States. Google showed its ability for cyber defence in 2009, when it reacted to a significant and sophisticated cyber attack on its network and corporate infrastructure. Internal security teams avoided the theft and alteration of Google's source code, identified the cyber attackers, entered the attackers' server and stopped their attack.[58] Furthermore, private actors with less cyber ability can hire the services of private cyber security companies whose number is growing rapidly.[59]

The State is based on a "social contract" with its citizens. Those renounce their natural liberty to use force against each other and agree to transfer this power to the State. There is a traditional understanding that the State has a monopoly in providing national security. It is the State's responsibility to secure its borders and the people within those borders.[59] Thus, if the State is unable to protect its citizens in cyber space, the State's monopoly on violence in that area should be suppressed and the power to defence should be reverted back to the citizens themselves.[60] The argument runs that one should be allowed to "do justice to oneself".

Another argument in favour of hacking-back is its deterrent effect. A faster and stronger response to harmful cyber operations by the private actor would deter cyber attacks. Indeed, those would need to be more complicated and costly to succeed, reducing the benefits of cyber attacks. Private cyber defence may not deter ideological attackers who are not motivated by profit. However, it might dissuade cyber criminals by imposing higher costs on their attacks.[61]

Finally, companies may be reluctant to allow access to their computer systems to governmental authorities and may prefer to organise their own defence. Indeed, a resort to the State to ensure their security may make public their cyber security weaknesses and negatively impact their reputation. Competitors could use disclosed vulnerabilities to their advantage. Moreover, companies may not want to give the State access to their systems, their data or the

[58] Patrick Lin, "Ethics of Hacking Back", Policy paper on cybersecurity funded by US National Science Foundation, 2016, p. 13, at http://ethics.calpoly.edu/hackingback.pdf [58] Centre for Cyber & Homeland Security, *op. cit.* note 16, p. 14. [59] Wyatt Hoffman and Ariel E. Levite, *op. cit.* note 12, p. 15.

[59] Max Weber, "Politics as a Vocation", in Hans Heinrich Gerth & C Wright Mills (ed.), *From Max Weber: Essays in Sociology,* Oxford, OUP, 1946, p. 78.

[60] Patrick Lin, "Ethics of Hacking Back", *op. cit.* note 57, p. 8.

[61] Patrick Lin, "Ethics of Hacking Back", *op. cit.* note 57, p. 21.

data of their clients. They may fear that such information is used by State intelligent services or, in relation to foreign companies, for cyber espionage.[62]

3.2. Disadvantages of Hacking-Back

There is a general agreement that the graver the charge the more confidence there must be in the evidence.[63] This logical assumption can be translated into cyber space. In our opinion, hacking-back in reaction to a cyber attack requires a clear and convincing evidence of the cyber attacker. The standard of proof in the attribution of conduct should not be lower in cyber space than in the physical world only to accommodate the difficulty of attributing in the cyber context. Indeed, standards of proof exist not to disadvantage the victim, but to protect against false attribution. It is hoped, however, that with the improvement of technology it will become easier to trace back cyber conduct.[64] There is a risk that private actors do not respect strict standards of proof and attribute harmful cyber conduct too quickly and with a low degree of certainty, thus targeting an innocent third party and not the perpetrator of the cyber attack. It is even more so that companies may not have the financial means to get effective cyber defence tools or the skilled human resources to use them. A cyber attacker could use a compromised third party computer to, for instance, download stolen data or upload malware. The cyber defender could, when hacking-back, accidentally target this computer but not that of the cyber attacker. Harm could be severe if the hacked computer belongs for example to a hospital or a nuclear station. The action in cyber defence could then damage medical records or safety systems.[65] There is also a risk that private actors do not correctly assess the intent of the perpetrator of a harmful international cyber operation. A detrimental cyber conduct may not necessarily be the result of malicious intent but of a mistake in network configuration. In that latter case, a cyber defence reaction should be less offensive.

---

[62] Karine Bannelier and Théodore Christakis, *Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors*, 2017, pp. 63-64, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988.

[63] Separate Opinion of Judge Higgins in *Case Concerning Oil Platforms* (Islamic Republic of Iran v United States of America) ICJ *Rep*., 2003, para. 30-39.

[64] Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations*, 2014, Cambridge, CUP, pp. 146-147.

[65] Sean L Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management", *Richmond Journal of Law and Technology*, 2014, vol. 2, p. 27.

Like every action in self-defence in the physical world, active digital defence should be proportionate to the harm caused by a cyber attack.[66] There is however a concern that private actors react to a cyber attack in a disproportionate way. Such would be the case when the defender launches a counter-worm to react to a worm. This may cause massive damage to many third parties. More generally, private actors, influenced by private interests, may not act in a consistent and fair way. Their action is not circumscribed by the principles of political accountability, transparency and fairness as is the action of the public sector in democratic societies. Democratic governmental authorities may be held accountable through parliamentary oversight and elections either of themselves or of higher level authorities who are responsible for their actions. Government's conduct is also subject to public scrutiny. By contrast, private actors largely escape public accountability mechanisms. Furthermore, private actors are not constrained by human rights obligations, in particular by the right to privacy, unlike public authorities in most States.[67]

More generally, authorising hacking-back could put into question the role of the State. The legal order of the State is based on the idea of a substitution of institutional justice for private justice. Accepting that States are not able to guarantee security in cyber space and that the private sector should "take the law into his own hands" is likely to sow disorder.[68] To rely on the private sector to perform security functions may increase security in the short term, but negatively affect security in the long term by weakening the authority of the State, "which has long been the locus of national security in the international system".[70]

Hacking-back could interfere with State activities. Thus, it could jeopardise operations carried out against the same target by the intelligence services of a State. Furthermore, counterback measures could compromise evidence needed by State law enforcement agencies to prosecute the targeted cyber attacker, particularly if the attacker's computer system has been shut down or digital footprints have been wiped out or altered during the hack-back action.[69]

---

[66] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) ICJ *Rep.*, 1986, para. 176.

[67] Kristen E. Eichensehr, *op. cit.* note 20, p. 505-506.

[68] Karine Bannelier and Théodore Christakis, *op. cit.* note 63, pp. 65-66. [70]
Kristen E. Eichensehr, *op. cit.* note 20, p. 518.

[69] Patrick Lin, "Ethics of Hacking Back", *op. cit.* note 57, p. 21; Karine Bannelier and Théodore Christakis, *op. cit.* note 63, p. 66.

Allowing hack-back activities could lead to escalation. Indeed, counter-hacking by a company may be received as an invitation to react in return. [70] The diverse reactions of hackbacks by the attacker and the initial victim may escalate quickly. Furthermore, the practice of hacking-back might be abused. Private cyber security companies could attack small companies without cyber defence means and, once the attack is over, offer them their services. Worse, if someone wants a computer to be attacked, he could route attacks through that computer against several victims and wait for the victims to attack back at that computer in the belief that the computer is the source of the attack. In disguising the origin of the initial attack, a wrongdoer could get innocent parties to counter-attack a hacked computer.[71]

At a more international level, hack-back operations could have harmful consequences in another State, different from the State where the hack-back perpetrator is located. Every State has an obligation to prevent detrimental conduct for another State perpetrated from its territory. Thus, if a State allowed hack-back reactions, it would violate its obligation of due diligence to prevent detrimental international activities against another State, if the hack-back reactions constituted internationally wrongful acts if perpetrated by the authorising State and if they caused serious damage.[72] Companies that hack-back in crossing national boundaries would be seen as attacking servers in other countries. An international crisis may result from an escalating exchange of cyber attacks and counter-hacks between companies in two States. For instance, a series of increasingly destructive hack-back measures between an American company and a Chinese company could become an international incident and prompt intervention of both States. [73] Private hacking-back as a response to cyber attacks has to be agreed by the international community of States as a whole. Otherwise, private cyber defence authorised by a few States but not by other States would derail relationships between those two categories of States. If, however, hacking-back becomes legal in most, if not all, States, it would be extremely difficult to regulate cyber counter-attacks of all companies located in more than 190 States.

4. Conclusion and Recommendations

[70] Sean L. Harrington, *op. cit.* note 66, p. 28.

[71] Orin Kerr, "The Hackback Debate", November 2012, p. 13, at https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/

[72] Irène Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations", *op. cit.* note 9, pp. 9-10.

[73] Wyatt Hoffman and Ariel E. Levite, *op. cit.* note 12, p. 17.

As demonstrated, international law neither recognises the right of, nor prohibits, hacking-back by private entities, except when, in exceptional circumstances, hacking-back triggers the international criminal responsibility of its author. However, it is generally prohibited under national law. If States authorised private actors to engage in active cyber defence at their will, this would give rise to many legal and political issues. In particular, hacking-back might lead to an escalation of harmful cyber operations crossing international borders, and, in the long run, to a destabilisation of the word order. On the other hand, given the inefficiency of States in securing cyber space, totally preventing the private sector from hacking-back may not be realistic. Indeed, companies are already resorting to active cyber defence and will continue to do so to protect their economic interests. [74] Thus, it is necessary to analyse the different possibilities for cooperation between States and non-State actors in responding to cyber attacks targeting the private sector.

First, States and companies could collaborate more systematically in the investigation and prosecution of harmful cyber operations. Some are calling for States to work more closely with private companies to better manage cyber attacks.[77] The company could detect and attribute a cyber attack by using non offensive cyber defence techniques. It should then inform the State enforcement agency. Only the State would be allowed to pursue more aggressive cyber defence measures, possibly with the assistance of the company. The role of the company would be similar to that of private detectives of insurance fraud offenses in assisting in the investigation and prosecution of law enforcement authorities.[75] Practice already offers examples of such a scenario. Thus, firms like Crowdstrike, Mandiant, and FireEye have already informed the United States about detrimental cyber operations.[76] Given the absence of borders in information and communications technology, there is a need for an international harmonised understanding of which active defence techniques are considered acceptable when done by companies without the cooperation of States. Even if that agreement is reached, it is doubtful whether States could systematically rely on the intelligence gathering provided by private companies. Indeed, companies may not be as disinterested and fair as States in detecting and attributing cyber attacks. A solution to this would be for States to cooperate only with certain, licensed, companies as explained below.

---

[74] Patrick Lin, "Ethics of Hacking Back", *op. cit.* note 57, p. 4. [77] Scott J. Shackelford, *op. cit.* note 65, p. 256.

[75] Centre for Cyber & Homeland Security, *op. cit.* note 16, p. 29.

[76] Centre for Cyber & Homeland Security, *op. cit.* note 16, p. 30.

Second, a private actor could be allowed to react to a specific cyber attack under the control of a State, at least in relation to severe cyber attacks. It is here submitted that the State should then exercise a close, effective, control over the private entity so as to avoid any of the difficulties of active cyber defence described above. The action in cyber defence of the nonState actor would then be attributable to the State and the State would assume the responsibility for any unlawfulness that might occur.[77] Such a scenario might happen if a State asks a company to react to a cyber attack because it aims to respond to it in an efficient way. This might also exist if a company solicits the authorisation of the State before acting against a particular harmful cyber activity.

Third, a small number of companies could be allowed to pursue active cyber defence, not only on an *ad hoc* basis, but before, in anticipation of potential harmful cyber operations. States increasingly resorted to private maritime security companies (PMSCs) in the last two decades to perform tasks that the national armed forces could no longer meet or wished to meet. In particular, States authorised the presence of PMSCs on board of their national flag vessels transiting through the Gulf of Aden and Indian Ocean from 2009. The use of private armed contractors by States on private commercial vessels corresponded with a substantial decrease in piracy. The maritime private security experience suggests that delegating the competence of ensuring security to a few entities does not necessarily lead to an escalation of violence, and, on the contrary, can have a deterrent effect.[78] Similarly, States could grant licences to a small number of companies in securing cyber space.[82] Thus, a non-licensed private actor would only be allowed to hack-back through a licensed company which acts on its behalf. Licensed companies should be selected based on their cyber expertise - to be updated on a regular basis - and should report their hack-back activities to the States. Given their limited number, States could more easily retain a control over them. Liability for unnecessary or unproportioned harm caused by hacking-back would be assumed by the licensed company. The State would however

[77] Art. 8 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, *op. cit.* note 15.

[78] Wyatt Hoffman and Ariel E. Levite, *op. cit.* note 12, pp. 24-27. Outsourcing the function of ensuring security was also done in the form of letters of marque attributed by States to vessels. In times of armed conflict, a vessel with a letter of marque could attack the enemy's trade. In peacetime, the practice of reprisal represented the means to seek redress against the harm suffered by the ship of another State. A letter of marque allowed a merchant to attack any ship of the offending State in order to find something of equal value to its loss. The practice of letters of marque was abolished in 1856 by the Declaration Respecting Maritime Law. Florian Egloff, "Cybersecurity and the Age of Privateering", in George Perkovich and Ariel E. Levite (ed.), *Understanding Cyber Conflict: Fourteen Analogies*, Washington, Georgetown University Press, 2017, p. 231. [82] Karine Bannelier and Théodore Christakis, *op. cit.* note 63, p. 76.

engage its responsibility if it is proven that it did not respect certain criteria in granting a cyber security licence to the company. Considering that many cyber hack-back operations have an international character, the cyber security license attributed to a few companies has to be recognised at the international stage by States. Thus, States should agree on common criteria in licensing companies. Ideally, in the long run, licensed companies should pull their resources and create a security consortium. A common agreement among States on cyber security licences is however unlikely to happen in the near future, given the current difficulty of States in regulating the use of cyber space.[79]

Private active cyber defence should respect certain requirements so as to avoid any destabilisation of the cyber world and to respect the rights of third parties. First, attribution must be done with a high degree of confidence and there must be a high chance of hitting the cyber attacker. Second, the action in hacking-back should be circumscribed by principles extracted from the law on the use of force and the law of armed conflict. Thus, counter-hack measures should be necessary and conducted with a predetermined objective (gather intelligence on the cyber attacker, prevent the theft of electronic data or rescue stolen data, protect against a disruption of a network or damage to it). Hack-back activities should not be done for retaliation or commercial gain. Therefore, as with the implementation of the right to self-defence in the physical world, hacking-back should occur just before an imminent cyber attack, in reaction to an ongoing cyber attack or shortly thereafter.[80] Furthermore, the action in counter-hacking should be proportionate to the objective. Thus, active cyber defence should be conducted with the minimum scope required and cease upon achievement of the predetermined objective. Hack-back activities should have consequences that are localised and preferably temporary and/or reversible. Hacking-back should not result in greater harm for the attacker. Active cyber defence measures with extended duration would be lawful only against persistent imminent threats of cyber attacks. They should seek to avoid collateral damage for third party networks to the greatest extent possible.[81] This may not be possible when the attack has been routed

[79] Different visions of cyberspace, particularly with regard to issues of sovereign authority and information access, covert military actions, espionage, and competition for global influence create a difficult context for the development of cyber norms. James A Lewis, "Confidence-Building and International Agreement in Cybersecurity", *Disarmament Forum*, United Nations Institute for Disarmament Research, 2011, 58.

[80] Fiona Leverick, *Killing in Self-Defence*, Oxford, OUP, 2006, pp. 87-89. On the right to anticipatory self-defence in reaction to an imminent armed attack under International Law: Irène Couzigou, "The Fight against the 'Islamic State' in Syria: Towards the Modification of the Right to Self-Defence?", *op. cit.* note 29, p. 90.

[81] Dorothy E. Denning, "Framework and Principles for Active Cyber Defense", *Computers & Security*, 2014, vol. 40, pp. 111-112.

through a third party's network. In that case, the cyber defender should alert and cooperate with the third party before acting. If time-sensitive requirements preclude this, the third party should at least be alerted after the cyber response. Appropriate technology must be exerted in order to respond to a harmful cyber operation in conformity with the principles described above. Automatic active cyber defence should be prohibited because it has the potential to disrupt or harm a third party's network. The defender should be liable for damage to the data or network of an innocent party and should remedy to it.[82] The defender should also be liable for damage inflicted on the attacker if the active cyber defence activity proved to be excessive, retaliatory or pursued for commercial interest.[83] Active cyber defence should respect the human rights of all persons affected, in particular their rights to privacy and free speech.

The standards that determine how active cyber defence can be resorted by the private sector to could be included into a soft law instrument, prepared in collaboration between States and a broad set of major companies from all over the world. Considering the rapid development of information and communications technology, such standards should be updated on a regular basis. Basic guidelines with respect to active cyber defence could serve as a building block for the creation of international norms in the future. With the increasing dependence of our world on online activities, States and the private sector need to work together to establish common cyber security principles.

[82] Making companies liable for third party damage will cause them to internalise in their decision to hack-back the potential harm to a third party and thus react reasonably.

[83] Wyatt Hoffman and Ariel E. Levite, *op. cit.* note 12, 2017, pp. 34-36; Jay P. Kesan and Ruperto Majuca, "Optimal Hack Back", *Chicago Kent Law Review*, 2010, vol. 84, pp. 838-839.