Hacking-Back by Non-State Actors and the Rule of Law

Dr. Irene Couzigou

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

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

Hacking-Back by Non-State Actors and the Rule of Law

Abstract:

States exercise their sovereign authority over the cyber infrastructure based on their territory, but many of them have only limited sovereign authority over other, non-physical layers of cyber space. Those do not control the use of the cyber infrastructure located on their territorial base or any other area under their exclusive control. This is true of poorly technologically developed States, yet also of technologically developed States – whose political and legal culture currently precludes the level of monitoring that would be necessary to completely monitor cyber communications. So, despite the will to exert sovereign authority over cyber space, most States are not currently able to completely prevent, react to, or even detect cyber attacks on or emanating from the cyber infrastructure within their territorial borders. In particular, States are generally slow in deterring and prosecuting cyber attackers targeting private companies. In light of the ineffective action of many States in securing cyber space, private actors, whether multinational information corporations or private cyber security companies hired by other companies, have reacted to harmful cyber operations themselves. Cyber defence activities may stay in the network of the defender. Alternatively, they may intrude into the network of the cyber attacker and are then known as "hack-back" activities. International law does not recognise the right of hacking-back by private entities and, in principle, does not prohibit it. Hacking-back by non-State actors is however currently contrary to national legal systems and as such contrary to the content of the rule of law at municipal levels. States may be tempted to authorise the private sector to hack-back with the aim of improving cyber security. Hack-back measures, not overseen by States, would however contradict formal attributes of the rule of law, the ones of generality, predictability, clarity and constancy. More fundamentally, it would threaten the philosophical and theoretical characteristics of the rule of law. Indeed, the rule of law can be understood as based on a contract between the State and its citizens where the State rules over its subjects in exchange of ensuring their security. This paper argues that private entities should thus not be authorised to respond to harmful cyber operations on their own. It contends that only a minority of licensed non-State actors should be allowed to hack-back, under the supervision

of States. This limited and State-supervised private active cyber defence would be respectful of the rule of law.

Keywords: hacking-back, non-State actors, rule of law, law, order

The following article has not been published, submitted, or accepted elsewhere.

I. 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 self-regulation.[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]

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

[1] *D. T. Kuehl*, From Cyberspace to Cyberpower: Defining the Problem, in: *F. D. Kramer, S. H. Starr, and L. K. Wentz* (eds.), Cyberpower and National Security, 2009, 28.
[2] *D. R. Johnson and D, Post*, Law and Borders - The Rise of Law in Cyberspace, Stanford L. Rev. 48 (1996), 48.
[3] Strategy for Homeland Defense and Civil Support, Department of Defense, USA, 2005, 12, at <https://www.hsdl.org/?view&did=454976>.

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 State 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 national and 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, many have only limited sovereign authority over other, non-physical layers of cyber space. Those States do not control the use of the cyber infrastructure located on their territorial base or any other area under their exclusive control. This is true of poorly technologically developed States, yet also of technologically developed States – whose political and legal culture currently precludes the level of monitoring that would be necessary to completely monitor cyber communications. Indeed, fundamentally, the United States and its allies, particulary in Western Europe, do not want to subject cyber space to sovereign

[4] *B. Pirker*, Territorial Sovereignty and Integrity and the Challenges of Cyberspac, in: *K. Ziolkowski* (ed.), Peacetime Regime for State Activities in Cyberspace, 2013, 193–194.
[5] *W. H. Von Heinegg*, Territorial Sovereignty and Neutrality in Cyberspace, Int'l L. Stud. 89 (2013), 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.

control, whereas for China, Russia, along with other States of the former Soviet Union, that space should be controled by sovereigns.[8] Furthermore, a high portion of the world cyber infrastructure is owned and operated by private entities. This makes the control of cyber traffic more difficult because it first requires that States impose monitoring obligations on the private sector.[9] So, despite the will to exert sovereign authority over cyber space, States are not always able or willing to completely prevent, react to, or even detect cyber attacks on or emanating from the cyber infrastructure within their 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.

In practice, many States lack the skills and/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.[10] Furthermore, State investigation can 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, and most of the cyber attackers are not identified.[11] State law enforcement is often overwhelmed both by the technical unfamiliarity of the crimes and the number of attacks occurring in the cyber world. 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.[12] Thus, in light of the absence of effective action of most States in securing cyber space, private actors, whether multinational information corporations (Google, Facebook, Yahoo, Microsoft etc.) or private cyber security companies (Novetta, CrowdStrike Mandiant,

[8] *K.E. Eichensehr*, The Cyber-Law of Nations, The Geo. L. J. 103 (2015), 329-335.

[9] *P. Rosenzweig*, Cybersecurity and Public Goods, 2012, 2, at <http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf>.

[10] *S. M. Condron*, Getting It Right: Protecting American Critical Infrastructure in Cyberspace, Harv. J. of L. & Technology 20 (2007), 416.

[11] *P. Lin*, Forget About Law and Ethics - Is Hacking Back Even Effective?, Forbes, 26.9.2016, at <https://www.forbes.com/sites/patricklin/2016/09/26/forget-about-law-and-ethics-is-hacking-back-even-effective/#7d0ccfe047d8>.

[12] *W. Hoffman and A. E. Levite*, Private Sector Cyber Defense, 2017, 3 at ‹https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf›.

FireEye etc.) hired by other companies, have reacted to harmful cyber operations themselves, independently from a State.[13] 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 2019, it hacked-back immediately to stop the attack.[14] Similarly, in 2011, when the "Koobface" gang compromised Facebook servers and used its access to disseminate malware to consumers, Facebook technicians exfiltrated the available evidence from its servers and disabled the "Koobface" gang's primary command and control server.[15]

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 within the meaning of Article 5 of the Draft Articles on the Responsibility of States – meaning the State specifically delegated State powers to the company – or if it acts on the instructions of, or under the direction or control of the State in accordance with Article 8 of the Draft Articles – which requires that the company acts under the "effective control" of the State.[16] The criteria for attribution of the conduct of a company to a State are very strict and thus unlikely to be fulfilled. 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 latter category of cyber defence operations is known as "hack-back activities". Those activities may remain within a State's territory or cross an international State border, which raises international legal issues.

As law applies in cyber space, private actors must of course respect the law of the State to which they are attached, including international law applying in the State's legal order. Indeed, the rule of law, regarded as essential in almost all common law or civil law national systems and supported by the international legal system, requires that everyone, whether

[13] *J. E. Messerschmidt*, Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm, Colum. J. of Transnat'l L. 52 (2013), 277.
[14] David E. Sanger and John Markoffjan, "After Google's Stand on China, U.S. Treads Lightly", *New York Times*, 14 January 2010.
[15] *A. D. Glosson*, "Active Defense: An Overview of the Debate and a Way Forward", Mercatus Working Paper, 2015, 17-18 at <https://www.mercatus.org/publication/active-defense-overview-debate-and-way-forward-guardians-of-peace-hackers-cybersecurity>.
[16] Art. 5 Draft Articles on Responsibility of States for Internationally Wrongful Acts; Art. 8 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 47-48, at <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>. Also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro) ICJ Reports 2007, 204-205, para. 390-391 and *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) ICJ Reports 1986, 64-65, para. 115.

official or private, natural person or legal person, is subject to law.[17] The concept of the rule of law is premised on the position that subjects ought to obey the law.[18] The rule of law means "the rule by laws", in that "people should obey the law and be ruled by it".[19] The question thus arises whether cyber defence activities, including hacking-back, conform to national and international law. As will be explained later in this article, the rule of law is also defined by formal and theoretical attributes which are essentially the same for the rule of law at both the national and the international levels. The rule of law is indeed characterised by its generality, predictability, clarity and consistency of its norms. More fundamentally, the rule of law can be understood as a theoretical construct where the authority to guarantee security and protection is given to the State and not to a non-State actor.[20] Consequently, the question also arises as to whether the privatisation of cyber security would be consistent with those formal and theoretical characteristics of the rule of law.

In section II, after having specified the different categories of cyber defence measures (II. 1), the paper will analyse the compatibility of hacking-back by private actors with the content of the rule of law, at the international and national levels. It will argue that, in principle, international law neither recognises the right of, nor prohibits, hacking-back by private entities (II. 2). This paper will also show that there does not seem to be any national legal order explicitly authorising the right to hack-back (II. 3). Section III will outline attributes of the rule of law. It will then be contented that if States allowed the private sector to perform hack-back activities, this may guarantee law and order in the short term (III. 1) but would threaten formal and theoretical attributes of the rule of law in the long term (III. 2). Finally, in section IV, this article will conclude that private entities should not be allowed to respond to harmful cyber operations on their own. It will recommend regulated cooperation between States and certain non-State actors in the reaction to injurious cyber operations and thus an integration of the role of those non-State actors into the rule of law.

II. Hacking-Back by Non-State Actors and Content of the Rule of Law

1. Defining and Categorising Active Cyber Defence Measures

[17] Declaration of the High-Level Meeting of the General Assembly on the Rule of Law at the National and International Levels, 30 November 2012, UN Doc. A/RES/67/1.
[18] *A.V. Dicey*, Introduction to the Study of the Law of the Constitution, reprint of the 8th ed. of 1915, 1982, 114.
[19] *J Raz*, The Rule of Law and its Virtue, in *J Raz* (ed.), The Authority of Law: Essays on Law and Morality, 1979, 210.
[20] *H. Barnett*, Constitutional & Administrative Law, 2017, 57-58.

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.[21]

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/her and prevent his/her 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.[22]

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/her own webcam). Active cyber defence activities also encompass aggressive operations committed with the intent to disrupt or

[21] Centre for Cyber & Homeland Security, Into the Gray Zone, Project Report, October 2016, 9, at <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf>
[22] Centre for Cyber & Homeland Security (note 21) 9-10.

destroy external networks.[23] Those operations are, for instance: the disabling of hostile email accounts; the implantation of malwares in the network of the attacker to disrupt the computer or system of the attacker to impede his/her ability to attack, by, for example, locking down his/her computer; the upload of malwares to damage the computer or system of the attacker to stop or prevent further attacks.[24] Many companies are already using active cyber defence measures, including the most aggressive ones.[25] They do it themselves or they hire a cyber security company to provide for their cyber defence.

Active cyber defence activities can be adapted to the harmful cyber operations to which they respond and be taken manually. They could also be automatic and autonomous.[26] They could for instance remove malware automatically. To identify the existence of a detrimental cyber operation, to attribute it, and to adopt appropriate reaction to mitigate or stop the cyber harm is time consuming, thereby increasing the likelihood that harm is sustained. Thus, automatic active cyber defence improves the effectiveness of the cyber response.[27]

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. They are included into the category of "hack-back activities".

2. Hacking-Back by Non-State Actors under International Law

a) 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 an injurious act, for instance a detrimental cyber operation, perpetrated by another State. Furthermore, a State could also adopt acts of retorsion or countermeasures

[23] Centre for Cyber & Homeland Security (note 21) 12.
[24] *W. Hoffman and A. E. Levite* (note 12) 8.
[25] *K. E. Eichensehr*, Public-Private Cybersecurity, Tex. L. Rev. 95 (2017), 499.
[26] *W. Hoffman and A. E. Levite* (note 12) 9.
[27] *N. Tsagourias and R. Buchan*, "Automatic Cyber Defence and the Laws of War", GYIL, 2017, 206.

against another 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.[28] 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.[29] 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.[30] An example of countermeasure is the temporary non-performance of an international treaty obligation towards the responsible State. A countermeasure could also be a hack-back activity. 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.[31] 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.[32] 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.[33] Finally, countermeasures must be proportionate to the harm suffered.[34]

The right to self-defence allows a State to react with force to an armed attack, including to a detrimental cyber operation.[35] Indeed, a cyber conduct 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

[28] For the requirements for the implementation of the obligation of due diligence in cyber space, see: *I. Couzigou*, Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations, International Review of Law, Computer & Technology 1 (2018), 4-10.
[29] *N. White and A. Abass*, Countermeasures and Sanctions, in: *M. D. Evans* (ed.), International Law, 5th ed., 2018, 527-529.
[30] Art. 49 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (note 16) 129. See also *N. White and A. Abass* (note 29) 524-526.
[31] Art. 50 (1) Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (note 16) 131.
[32] *Couzigou*, The Challenges Posed by Cyber-Attacks to the Law in Self-Defence, in: *A. Reinisch, M. E. Footer* and *Ch. Binder* (eds.), International Law and *…,* 2016, 250-251.
[33] Art. 50 (1) Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (note 16) 131.
[34] Art. 51 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (note 16) 134.
[35] Art. 51 UN Charter.

triggering the right to self-defence.[36] Action in self-defence could be perpetrated in cyber space and take the form of cyber self-defence.

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. 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.[37] Similarly, they could react in self-defence to an armed attack.[38]

The international rules related to non-forcible or forcible reactions to internationally wrongful acts or simply international unfriendly acts concern only subjects of international law. 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 have the right to self-defence.[39] Thus, the international law on acts of retorsion, countermeasures or self-defence does not give the right to respond to private actors that are not subjects of international law, in a cyber or other way.

Yet if international law does not explicitly provide for a right for private companies to counter-hack, the question arises as to whether it does so implicitly. Indeed, international rules of self-protection might, 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 transported; similarly, cyber space is a space where communications are conveyed. Pirates steal physical property; similarly, cyber

[36] *Couzigou* (note 32) 250-253.

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

[38] The right to self-defence is customary. *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) ICJ Reports 1986, 94, para. 184-186. As such, it applies to international subjects of international law, whether States or international organisations. *A. Bleckmann*, Zur Verbindlichkeit des allgemeinen Völkerrechts für internationale Organisationen, ZaöRV 107 (1977), 113-114.

[39] 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. *I. Couzigou*, The Fight against the 'Islamic State' in Syria: Towards the Modification of the Right to Self-Defence?, Geo., Hist., and Int'l. Rel. 9 (2017), 87.

attackers may steal intellectual property.[40] 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.[41] 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".[42] The pursuit must cease "as soon as the ship pursued enters the territorial sea of its own State or of a third State".[43] 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.[44] 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".[45] Thus, the law of piracy cannot be translated into cyber space so as to legally justify hacking-back perpetrated by non-State actors.

b) 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 direct the political or military action of a State"[46] – and does therefore not concern the situation of hack-back by a non-State actor whose conduct cannot be attributed to a State.

---

[40] *P. Rosenzweig*, International Law and Private Actor Active Cyber Defensive Measures, Stanford J. of Int'l. L. 50 (2014), 110.

[41] Art. 111 (1) Convention on the Law of the Sea of 10.12.1982, 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>.

[42] Art. 111 (1) Convention on the Law of the Sea (note 41). See also Art. 23 (1) Convention on the High Seas (note 41).

[43] Art. 111 (3) Convention on the Law of the Sea (note 41). See also Art. 23 (2) Convention on the High Seas (note 41).

[44] The Convention on the Law of the Sea has 168 Parties as of 2.9.2019.

[45] Art. 111 (5) Convention on the Law of the Sea (note 41). See also Art. 23 (4) Convention on the High Seas (note 41).

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

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.[47] 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".[48] 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.[49] 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.[50] 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.[51] Here again, a private cyber hack-back operation could, in certain limited circumstances, be assimilated to a crime against humanity, 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.

[47] A. *Cassese, P. Gaeta, L. Baig, M. Fan, C. Gosnell, A. Whiting*, International Criminal Law, 2013, 129.
[48] Art. 6 Rome Statute of the ICC, 17.7.1998, at <https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf>.
[49] *A. Cassese, P. Gaeta, L. Baig, M. Fan, C. Gosnell*, A. Whiting (note 47) 105-108.
[50] Art. 7 Rome Statute of the ICC (note 48).
[51] *A. Cassese, P. Gaeta, L. Baig, M. Fan, C. Gosnell, A. Whiting* (note 47) 100.

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.[52] For its Article 8,[53] 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".[54] 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.[55] 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.[56] 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.[57] 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.[58] Common Article 3 of the Geneva Conventions prohibits for instance each party in an internal conflict from exercising violence against persons not participating in the hostilities, "in particular murder of all kinds, mutilation, cruel treatment and torture".[59] 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

[52] *N. Melzer*, International Humanitarian Law, 2016, 286.
[53] Art. 8 Rome Statute of the ICC (note 48).
[54] Art. 8 2 a) and b) Rome Statute of the ICC (note 48).
[55] Art. 147 Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12.8.1949, at <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=F8D322BF3C0216B2C12563CD0051C654>. Other grave breaches are defined in the following provisions: Articles 50, 51, and 130 of the First, Second, Third Geneva Conventions, respectively, as well as in Article 85 of the First Additional Protocol of 1977.
[56] 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>.
[57] Art. 8 2 c) Rome Statute of the ICC (note 48).
[58] *G. D. Solis*, The Law of Armed Conflict, 2017, 163-164.
[59] 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>.

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.

3. Hacking-Back by Non-State Actors under National Law

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.[60] The Convention on Cybercrime requires the 64 State Parties[61] to criminalize offences against the confidentiality, integrity and availability of computer systems (illegal access, illegal interception, data interference, system interference, misuse of devices),[62] computer-related offences (forgery, fraud),[63] content-related offences related to child pornography,[64] and offences related to the infringements of copyrights and related rights.[65] Thus, the Convention asks the State Parties to criminalise the unauthorised access into a network.

The Convention remains silent on a right to interfere, without authorisation, in a network in order to pursue cyber activity, as a response to a harmful cyber conduct. The only reference to active cyber-defence is made by the explanatory report.[66] 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

[60] Council of Europe, ETS No. 185, 23.11.2001.
[61] Number of Parties as of 2.9.2019.
[62] Articles 2, 3, 4, 5 and 6 Convention on Cybercrime.
[63] Articles 7 and 8 Convention on Cybercrime.
[64] Article 9 Convention on Cybercrime.
[65] Article 10 Convention on Cybercrime.
[66] Council of Europe, Art. 38 explanatory report to the Convention on Cybercrime, ETS No. 185, 23.11.2001.

to the exclusion of criminal liability" (we underline). Thus, the explanatory report suggests that State Parties could exclude criminal responsibility for the access into a network if it occurs pursuant to private self-defence or cyber-defence. The explanatory report is of significance because it constitutes a rare international recognition of a private right to cyber-defence. It is however only meant to facilitate the implementation of the Convention, not to provide for an authoritative interpretation. None of the 63 States party to the European Convention on Cybercrime has interpreted the Convention as authorising the right to hack-back. Thus, hack-back operations correspond to those cyber activities to be criminalised by the States party to the Convention on Cybercrime.

More generally, to our knowledge, other States than the ones party to the European Convention on Cybercrime, criminalise the unauthorised intrusion by a non-State actor into a network, without explicitly providing for an exception when the intrusion reacts to a harmful cyber activity. Thus, they do not authorise hacking-back.[67] For instance, all G8 countries criminalise unauthorised access to a computer to a greater or lesser extent without explicit exception.[68] It is however 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".[69] An amendment of 2013 of the Computer Misuse and Cyber Security Act of Singapore is also worth referring to. Without authorising offensive private active cyber defence, it created a mechanism for State-sanctioned active cyber defence. In accordance with that amendment, the government of Singapore could issue certificates to authorise individuals or organisations to adopt measures in order to prevent, detect or counter threats to national security or critical national infrastructures, while providing prosecutorial immunity for the concerned persons or organizations. The authorised measures included in particular access to "the operation in or

[67] *Th. Reinhold and M. Schulze*, Digitale Gegenangriffe, Arbeitspapier, 2017, pp. 9-10 at <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf>.
[68] *A. N. Craig, S. J. Shackelford & J. S. Hiller*, Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis, Am. B. L. J. 4 52 (2015) 18-20. Also see the discussion as to whether offensive active cyber defence could be seen as compatible with the American Computer Fraud and Abuse Act in *A. D. Glosson* (note 15) 9-14.
[69] H.R.4036 - Active Cyber Defense Certainty Act, at <https://www.congress.gov/bill/115th-congress/house-bill/4036/text>.

from Singapour of a computer" and use of any computer in or from Singapore "to search any data contained in or available to such computer".[70] This possibility has since been repealed.[71]

In conclusion, hacking-back by non-State actors is in most cases not contrary to the substance of the rule of law of the international legal order. For the moment, it is however not compatible with the content of the rule of law of national legal orders. This may change if States authorised hacking-back by private entities, as a means to improve the security in cyber space. Private cyber security would however threaten formal and theoretical attributes of the rule of law, as explained in section III.

III. Hacking-Back by Non-State Actors and Attributes of the Rule of Law

1. Attributes of the Rule of Law

The rule of law has received many different theoretical definitions. A basic definition that is acceptable across cultures and political systems is necessarily a formal one.[72] While there are considerable controversies about the substance of the rule of law, there is a relative consensus over its formal characteristics.[73] Law theorists have recognised different formal attributes of the rule of law.[74] The most accepted ones are: generality, meaning that everyone is subject to the same law; publicity, expecting that the law is public so that citizens or other subjects are aware of it and adapt their conduct accordingly; predictability, requiring that the law is laid down in advance; clarity, signifying the law should not be obscure or vague as to leave its subjects at the mercy of discretion; non-contradictory, meaning that contradictions in the law should be avoided; practicability which means that the law should not command the impossible; constancy, expecting that the law should not be changed too frequently; and congruence between official action and declared rule.[75] Those core characteristics of the rule

[70] Article 15A 1 and 2a, to read in conjunction with Article 39 (1) (a) and (b), (2) (a) and (b) and Article 40 (2) (a) and (b) of the Criminal Criminal Code. Version of the Computer Misuse and Cybersecurity Act of 2013 at ‹https://www.unodc.org/res/cld/document/computer-misuse-and-cybersecurity-act_html/2014_COMPUTER_MISUSE_AND_CYBERSECURITY_ACT.pdf›

[71] Current version of the Computer Misuse and Cybersecurity Act of Singapour at ‹https://sso.agc.gov.sg/Act/CMA1993?ProvIds=pr14-#pr14-›

[72] *S. Chesterman*, An International Rule of Law, AJIL 56 (2008), 342.

[73] *J. Moller*, The advantages of a thin view, in: *Ch. May and A. Winchester* (ed.), Handbook on the Rule of Law, 2018, 28-29.

[74] *E. N. Zalta* (ed.), Standford Encyclopedia of Philosophy, The Rule of Law, 2016, at <https://plato.stanford.edu/entries/rule-of-law/#FormAspe>.

[75] *L. L. Fuller*, The Morality of Law, revised ed 1964, 46-91. Also *J. Moller* (note 73) 28-29.

of law are essentially the same for a national or international rule of law.[76] They should apply to the norms that govern a community, including to the enforcement norms reacting to unlawful and/or injurious activities. They ensure that the legal order is a constraining framework of well-established norms rather than composed by norms established in a discretionary manner. As written by Bentham, "[t]he principle of security… requires that events, so far as they depend upon laws, should conform to the expectations which law itself has created".[77] In municipal law, the formal attributes of the rule of law have two aims. First, they guarantee that power is not arbitrary, is predictable, and personnel and thereby protects citizens against the State. [78] This objective, the more prominent one, has been essential in the emergence of the rule of law. Second, the formal characteristics of the rule of law prevent anarchy in relations between non-State actors – individuals and groups – and promotes social order. They protect citizens or other subjects from their fellow citizens or other subjects.[79] This second function, that limits the authority of municipal subjects, is equivalent to the function of the formal attributes of the rule of law as applied in the international legal order. Indeed, under international law, the role of the formal characteristics of the rule of law is to restrict the authority of international subjects, namely that of States and international organisations.[80] Thus, the rule of law aims to secure a peaceful coexistence of the subjects of municipal legal orders or of the international legal order.

More fundamentally, the rule of law is also defined by theoretical attributes. It can be conceived as a philosophical construct where citizens give up their freedom and accept to be ruled by a State providing it ensures their protection. The States and its citizens concluded a "social contract" where the citizens agree to be subjected to the rule of law attached to a State and the State consented to guarantee their security.[81] Consequently, there is an understanding that the State has a monopoly in providing national security to physical and, more broadly, legal persons over its territory. It is the State's responsibility to secure its borders and the

[76] *R. McCorquodale*, Business, the International Rule of Law and Human Rights, in: *R. McCorquodale* (ed.), The Rule of Law in International and Comparative Context, 2010, 32.
[77] *J. Bentham*, The Theory of Legislation, 1931, 111.
[78] *L. L. Fuller* (note 75).
[79] *A. Bedner*, The promise of a thick view, in: *Ch. May and A. Winchester* (ed.), Handbook on the Rule of Law, 2018, 35-36. Also *A. Bedner*, An Elementary Approach to the Rule of Law, Hague Journal on the Rule of Law, 2(1) (2010) 50-52.
[80] *A. Watts*, The International Rule of Law, GYIL 36 (1993), 23.
[81] *Th. Hobbes*, Leviathan, 1651, 103-106; *J.-J. Rousseau*, Du contrat social, 1966, 50-52; *B. Z. Tamanaha*, On the Rule of Law, 2004, 129-130.

people and legal entities within those borders.[82] On that point, international law increasingly recognises the responsibility of States to protect their population, whether through the resort to force or otherwise.[83]

2. Efficiency of Privatising Cyber Security

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 using 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. [84] 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. Meanwhile, the integrity of digital forensics is vanishing quickly.[85] 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.[86] Depending on the legal nexus between that person and a State, his/her 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 Draft Articles on State Responsibility for Internationally Wrongful Acts.

[82] In that sense: *M. Weber*, Essays in Sociology, 1948, 78. For Weber, the State has the monopoly of the use of legitimate force for a given territory. This security function of the State can be broadened up and include security activities not limited to physical force.
[83] Most States have recognised the responsibility of each individual State "to protect its population from genocide, war crimes, ethnic cleansing and crimes against humanity". General Assembly Resolution, 15 September 2005, UN Doc. A/60/4/1, para. 138 and 139. Furthermore, the UN Security Council has referred to this primary responsibility to protect in a multitude of resolutions. See <http://www.globalr2p.org/resources/335>.
[84] *R. Buchan*, Cyberspace, Non-state Actors and the Obligation to Prevent Transboundary Harm, Journal of Conflict and Security Law 21 3 (2016), 430.
[85] *S. W. Brenner*, At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare, Journal of Criminal Law and Criminology 97 (2007), 420.
[86] *R. Buchan* (note 84) 431.

Most of these are customary.[87] 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, especially when the cyber attacker is still online.[88]

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. Or if data has been illegally exfiltrated from the network of a company, the data must be recovered quickly before it is copied or distributed. However, States are usually slow in reacting to cyber attacks and in prosecuting cyber attackers.[89] 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.[90] Furthermore, private actors with less cyber ability can hire the services of private cyber security companies whose number is growing rapidly.[91]

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. Offensive active 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.[92]

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

[87] Chapter II Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (note 16) 38-54.
[88] *A. D. Glosson* (note 15) 14-15.
[89] *P. Lin*, Ethics of Hacking Back, Policy paper on cybersecurity funded by US National Science Foundation, 2016, 13, at <http://ethics.calpoly.edu/hackingback.pdf>.
[90] Centre for Cyber & Homeland Security (note 21) 14.
[91] *W. Hoffman and A. E. Levite* (note 12) 15.
[92] *P. Lin* (note 89) 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.[93] Although authorising the private sector the power to hack-back may ensure a more efficient cyber security, it also entails risks of inconsistency and escalation that threaten the rule of law.

3. Risks of Privatising Cyber Security for the Rule of Law

a) Inconsistency of Private Cyber Security

Private companies have different cyber defence tools or skilled human resources to use them. Thus, allowing hack-back activities to the private sector will lead to inconsistent reactions to cyber attacks. Some companies will be able to defend themselves, others not or not to the same level. Furthermore, private cyber reactions may not be accurate. There is a general agreement that the graver the charge the more confidence there must be in the evidence.[94] This logical assumption can be translated into cyber space. In our opinion, hacking-back in reaction to a cyber attack requires a high threshold of proof, a clear and convincing evidence about the identity of the cyber attacker. It should be substantially more likely than not that a specific person is the author of the cyber attack. 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.[95] 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. 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

[93] *K. Bannelier and Th. Christakis*, Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors, 2017, 63-64, at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988>.
[94] Separate Opinion of Judge Higgins in *Case Concerning Oil Platforms* (Islamic Republic of Iran v United States of America) ICJ Reports 2003, 233-235, para. 30-39.
[95] *S. J. Shackelford*, Managing Cyber Attacks in International Law, Business, and Relations, 2014, 146-147.

hospital or a nuclear station. The action in cyber defence could then damage medical records or safety systems.[96]

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.

Like private self-defence in the physical world, active digital defence should be proportionate to the harm caused by a cyber attack.[97] There is however a concern that not all private actors will have the technical means to react to a cyber attack in a proportionate way. For instance, a company could launch a counter-worm to react to a worm and thereby cause massive damage to many third parties.

Approximations or mistakes in attribution, in the assessment of the intention of the cyber attacker and in the proportionality of the cyber response may be even worse in the case of automatic hacking-back. If offensive active cyber defence is programmed, a computer may be able to trail back the real source of a malicious cyber operation. The computer will however not be able to identify the real perpetrator of the cyber conduct, his/her status – whether he/she is a non-State actor or a State actor – and his/her intention – hostile or not. The absence of identification of the cyber perpetrator may have political, legal and practical effects. If programmed consequently, a computer can recognise a detrimental cyber conduct and assess the scale of the harm caused, at least when the harm remains online.[98] The computer could then automatically disable the zombie email account or server responsible for the harmful cyber conduct. Automatic hacking-back is however suitable only in strictly predetermined situations, not in case of unforeseen or complex harmful cyber activities. Indeed, in such scenarios, the computer could not identify the various cyber reactions that are available, assess their potential efficacy, and choose the most appropriate response. For doing so, the computer would need to possess some form of artificial intelligence, able to translate mimic human reasoning. This technology that does not exist yet.[99] Hence, the absence of adaptability in automatic active cyber defence may give rise to unproportionate cyber reactions. It could also result in harming third parties, for instance when an active cyber

[96] *S. L Harrington*, Cyber Security Active Defense: Playing with Fire or Sound Risk Management, Richmond J. of L. and Tech. 2 (2014), 27.
[97] *S. Uniacke*, "Proportionality and Self-Defense", Law and Philosophy 30 (3) 2011, 253-255.
[98] *N. Tsagourias and R. Buchan* (note 27) 209.
[99] *Human Rights Watch*, Losing Humanity, 2012, 8 at <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>.

defence measure forces offline a website that is used for both malicious and legitimate objectives. [100]

Overall, independently on their cyber capacity and on whether it is activated manually or automatically, private actors may be motivated by their business interests and may not act as consistently and fairly as State actors. At least in democratic societies, the action of public actors is circumscribed by the principles of transparency and fairness. By contrast, private actors largely escape public accountability mechanisms; private companies are influenced by changeable profit-driven interests.[101] For instance, some private cyber security companies may have incentive to cut costs in order to compete. They may then offer cheaper cyber defence action, but of a lower quality than others.

In consequence, recognising the power to the private sector to defend itself against cyber attacks may lead to inconsistencies in the content and/or degree of cyber defence activities. Thus, authorising private hacking-back would contradict the rule of law as characterised by the attributes of generality, publicity, predictability, clarity, and constancy. This conclusion could however be different if the State controlled how active cyber-defence by the private sector should be perpetrated, as will be explained in section IV.

b) Escalation of Private Cyber Security

Another downside of hacking-back by non-State actors is the risk of escalation. Indeed, counter-hacking by a company may be received as an invitation to react in return.[102] The diverse reactions of hack-backs 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/she 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.[103]

[100] *N. Tsagourias and R. Buchan* (note 27) 214 and 217.
[101] *K. E. Eichensehr* (note 25) 505-506.
[102] *Sean L. Harrington* (note 96) 28.
[103] *O. Kerr*, The Hackback Debate, 11.2012, 13, at <https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate>.

At a more international level, hack-back operations could have detrimental 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.[104] This obligation also applies to the prevention of harmful cyber conduct under several requirements. The territorial State must know or should have known of the harmful cyber conduct; the cyber conduct would amount to an internationally wrongful act if it were committed by that State; the conduct causes prospective or current significant harm and not only a simple inconvenience. [105] Thus, if a State allows hack-back reactions, it would violate its obligation of due diligence to prevent detrimental international activities against another State in relation to the hack-back reactions that would constitute internationally wrongful acts if they were perpetrated by the authorising State and that would inflict serious damage in another State. 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, in particular if the Chinese company is owned by the Chinese State, and prompt intervention of both the United-States and China.[106] 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 perpetrated from the States authorising it with international effects in States that do not approve this practice could be seen as harmful conduct by these latter States and 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.

Hence, 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. To allow hack-back activities by private companies may lead to the "wild west" in cyber space. 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. At the same time, this will threaten the very basis of the rule of law. Indeed, as explained above, the rule of law can be seen as based on a contract where the State governs over individuals in exchange of ensuring their protection. If

[104] *The Corfu Channel Case* (United Kingdom v. Albania) ICJ Reports 1949, 22.
[105] *I. Couzigou* (note 28) 4-10.
[106] *W. Hoffman and A. E. Levite* (note 12) 17.

the State becomes unable to protect the people or legal persons based on its territory – or any other area under its effective control – from the harmful effects of cyber conduct on its territory – or any other space under its jurisdiction –, the "social contract" it entered with its citizens will be breached. Authorising hacking-back may, in the long run, put into question the role of the State and of the rule of law.

IV. Conclusion and Recommendations

As demonstrated, hacking-back by non-State actors is not incompatible with the content of the rule of law under international law, except when, in exceptional circumstances, it triggers the international criminal responsibility of its authors. However, hacking-back would be contrary with the substance of the rule of law in national legal systems. States may be tempted to authorise hacking-back by non-State actors as an attempt to improve the security of cyber space. If they do so however, this would have a negative impact on the formal attributes of generality, publicity, predictability, clarity, and constancy of the rule of law. Furthermore, if States gave up their monopoly in pursuing offensive active cyber defence and attributed the power to non-State actors to ensure their own cyber-security, including through offensive active cyber-defence, they would threaten an essential theoretical characteristic of the rule of law. Indeed, the rule of law can be understood as based on a contract between the State and its citizens where the State rules over the individuals and legal persons based on its territory – or any other area under its exclusive control – in exchange for ensuring their security. Private cyber security would contravene the terms of this contract. On the other hand, totally preventing the private sector from hacking-back may not be realistic, so long as not all States are willing or able to ensure an efficient cyber security. Companies are already resorting to active cyber defence and will continue to do so to protect their economic interests.[107] Thus, it is necessary to take into account the role of non-State actors in securing cyber space. They should however act under the supervision of States so that their action in hacking-back conform with formal attributes of the rule of law and does not affect the monopoly of the State in guaranteeing the protection of its territory. How this could be done is explained below.

States and companies could collaborate more systematically in the investigation and prosecution of detrimental cyber operations. Some are calling for States to work more closely

[107] P. Lin (note 89) 4.

with private companies to better manage harmful cyber activities.[108] The company could detect and attribute a cyber conduct 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, including hack-back activities, 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.[109] Practice already offers examples of such a scenario. Thus, firms like Crowdstrike, Mandiant, and FireEye have already informed the United States about cyber attacks.[110] 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 operations. A solution to this would be to work with only a small number of companies, with excellent cyber expertise and under the close oversight of States.

Those companies could even be authorised to pursue offensive active cyber defence, encompassing hacking-back, not on an ad hoc basis but in general. Indeed, time is crucial for the efficiency of a cyber response to a detrimental cyber operation. Instead of having to wait for authorisation for action after the occurrence of a detrimental cyber operation, a company could be authorised to pursue active cyber defence ahead of harmful cyber activities.[111] States increasingly resorted to private maritime security companies (PMSCs) – commercial firms providing military services ranging from the use of lethal force to training and advice to militaries – in the last two decades to perform tasks that the national armed forces could no longer meet or wished to meet.[112] 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 security contractors by States on private commercial vessels corresponded with a substantial decrease in piracy. The private maritime security experience

[108] *S. J. Shackelford* (note 96) 256.
[109] Centre for Cyber & Homeland Security (note 21) 29.
[110] Centre for Cyber & Homeland Security (note 21) 30.
[111] Under the amendment of 13.3.2013 of the Computer Misuse and Cybersecurity Act of Singapore, private actors could be authorised by the State to access computer data in response to cyber threats. See *infra*. A verifier.
[112] *S. Chesterman and Ch. Lehnardt*, Introduction, in: *S. Chesterman and Ch. Lehnardt* (eds.), From Mercenaries to Market: The Rise and Regulation of Private Military Companies, 2007, 3.

suggests that delegating the competence of ensuring security in the sea to a few private entities does not necessarily lead to an escalation of violence, and, on the contrary, can have a deterrent effect.[113] Similarly, States could grant licences to a small number of companies in securing cyber space.[114] 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 and should publicly report their hack-back activities to States. Licences should be valid for a limited time period to ensure that the licenced companies continue to fulfil criteria for licences (e.g., competence, respect for the law). Given their limited number, States could more easily retain a control over licenced companies. Those companies would however keep a certain freedom for action. They would not be de facto organs of a State in accordance with Article 4 of the Draft Articles on Responsibility for Internationally Wrongful Acts, empowered to exercise governmental authority within the meaning of Article 5 of the Draft Articles or would not act on the instructions of, or under the under the direction or control of a State in conformity with Article 8 of that Draft Articles.[115] Thus, liability for unnecessary or disproportional harm caused by hacking-back would be assumed by the licensed company. Potential tort liability would give firms incentive to hack-back accurately and proportionally.[116] States would however engage their responsibility if it is proven that they did not respect certain criteria in granting a cyber security licence to the company.

Licensed companies make take active cyber defense action against companies located in other States. Thus, in order to avoid tension between States, the cyber security license attributed to a few companies has to be recognised at the international stage. States should agree on common criteria in licensing companies. [117] Ideally, in the long run, an independent

[113] *W. Hoffman and A. E. Levite* (note 12) 24-27. Outsourcing the function of ensuring security was also done in the form of letters of marque attributed by States to privateers, privately owned and operated ships. In times of armed conflict, a privateer with a letter of marque could attack and seize the trade of the State's enemy. In peacetime, a letter of marque provided for limited authorisation for a privateer to hunt down a pirate after being attacked. The practice of letters of marque was abolished in 1856 by the Declaration Respecting Maritime Law. *F. Egloff*, Cybersecurity and the Age of Privateering, in: *G. Perkovich and A. E. Levite* (eds.), Understanding Cyber Conflict: Fourteen Analogies, 2017, 231.

[114] *K. Bannelier and Th. Christakis* (note 93) 76.

[115] Art. 4, 5 and 8 Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (note 16) 40, 42 and 47 respectively.

[116] *Jay P. Kesan and Carol M. Hayes*, Thinking Through Active Defense in Cyberspace, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010), 329.

[117] As some did in the Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations for Private Military and Security Companies (PMSCs) During Armed Conflict of 17 September 2008, the fruit of a discussion between States, industry representatives, academic experts and non-governmental organizations. The Montreux Document set forth voluntary guidelines for how States should manage their relationships with PMSCs to ensure their respect for international law, international humanitarian

international oversight mechanism for licensing companies and monitoring their activities should be created. Furthermore, licensed companies should with time pull their resources and create a security consortium. For the moment however, a common agreement among States on cyber security licences is unlikely to happen, given the current difficulty of States in regulating the use of cyber space.[118]

Hacking-back by non-State actors should respect certain rules so as to avoid any destabilisation of the cyber word and to respect the attributes of generality, predictability, clarity and constancy of the rule of law. 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 necessity and proportionality principles 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 private right to self-defence in the physical world, hacking-back should occur just before an imminent detrimental cyber operation, in reaction to an ongoing harmful cyber operation or shortly thereafter.[119] Furthermore, the action in counter-hacking should be proportionate to the objective. Thus, offensive 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. Offensive active cyber defence with extended duration would be lawful only against persistent imminent threats of detrimental cyber conduct. It should not encompass activities that pose a risk to human safety; those activities should be exclusively within the remit of State actors.[120] Hacking-back should seek to avoid collateral damage for third party networks to the greatest extent possible.[121] This may not be possible when the cyber operation has been routed

---

law and human rights law, and limit the risks of detrimental consequences from their conduct. It thus contains PMSC selection criteria. <https://www.icrc.org/en/doc/assets/files/other/icrc_002_0996.pdf >

[118] 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. *J. A. Lewis*, Confidence-Building and International Agreement in Cybersecurity, Disarmament Forum 4 (2011), 58.

[119] *F. Leverick*, Killing in Self-Defence, 2006, 87-89.

[120] *W. Hoffman and S. Nyikos*, Governing Private Sector Self-Help in Cyberspace: Analogies from the Physical World, 2018, 59 at ‹https://carnegieendowment.org/2018/12/06/governing-private-sector-self-help-in-cyberspace-analogies-from-physical-world-pub-77832›.

[121] *D. E. Denning*, Framework and Principles for Active Cyber Defense, Computers & Security 40 (2014), 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. For the time being, until computers acquire a form of conscious through artificial intelligence, automatic hacking-back should be prohibited because it has the potential to be disproportional and to harm third parties. The defender should be liable for damage to an innocent party. 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.[122] 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 hacking-back can be resorted to could be included into a soft law instrument, prepared in collaboration between States and a few companies with developed cyber expertise.[123] Considering the rapid development of information and communications technology, such standards should be updated on a regular basis. Those guidelines could serve as a building block for the creation of international norms in the future. In view of the overall pre-eminence of the private sector in cyber space, there is a need to recognise its role in the establishment and implementation of cyber security standards. This should however be done in conformity with the rule of law. Therefore, only a few non-State actors with advanced cyber knowledge should be allowed to hack-back under the close supervision of States.

[122] *W. Hoffman and A. E. Levite* (note 12) 34-36; *J. P. Kesan and R. Majuca*, Optimal Hack Back, Chicago Kent L. Rev. 84 (2010), 838-839.

[123] Similar to the Montreux Document (see note 117) or the International Code of Conduct for Private Security Providers of 9 November 2010. This Code, signed by 58 companies at the time of its drafting and by more than 700 today, negotiated by companies, civil society organisations and States, expands upon the principles of the Montreux Document. It is addressed to PMSCs and guides their conduct. <https://www.icoca.ch>. See also *W. Hoffman and S. Nyikos* (note 120) 42-46.