Cyber-Attacks
Prevention-Reactions : The Role of States and Private Actors

Karine Bannelier
Associate Professor, University Grenoble Alpes

Théodore Christakis
Professor, University Grenoble Alpes/Institut Universitaire de France

Preparatory Study for the International Conference

« Building international peace and security in a digital society »

Public actors, Private actors: duties and responsabilities

Maison de l'UNESCO, Paris, April 6th - 7th 2017

Association loi 1901 fondée en 1939

Les Cahiers de la Revue Défense Nationale

SGDSN

Agence nationale de la sécurité des systèmes d'information · ANSSI ·

SPEAK UP FOR YOUR RIGHT TO PEACE AND SECURITY IN THE DIGITAL WORLD

LEGAL EXPERTS

USER OF DIGITAL TECHNOLOGIES

Karine BANNELIER

Karine Bannelier is Associate Professor of International Law at the University Grenoble Alpes and Director of the Master 2 Programme in International Security and Defense at the same University and at the Paris School of International Relations (ILERI). Researcher at the Center for International Security and European Studies (CESICE), she founded the Cyber-Nano-Bio Research Group: Challenges of new technologies for international security, and co-founded AMNECYS (Alpine Multidisciplinary Network on Cyber Security studies) which unites dozens of experts of different disciplines working in the field of cyber security. Member of the executive board of the Grenoble Alpes Data Institute, she is in charge of WorkPackage5 Data Governance, Data Protection and Privacy with C. Castelluccia. Her research focuses on international law, international security law, cyber security, data governance and data protection. She participates in various international research networks in these fields, such as the Cyber-Terrorism Project led by the University of Swansea. She has been invited to present papers or seminars on these issues in some twenty countries and has published or co-edited 7 books and about 40 articles. [Karine.Bannelier@univ-grenoble-alpes.fr].

Théodore CHRISTAKIS

Theodore Christakis is Professor of international law at the University Grenoble Alpes and a Senior Member of the Institut Universitaire de France (IUF), where he conducts a research project on National Security and International Law, an important part of which is devoted to the law of cyber security. He is Director of the Center for International Security and European Studies (CESICE) and Deputy Director of the Grenoble Alpes Data Institute. He is founder and co-chairman of the European Society for International Law's Interest Group on Peace and Security, a member of the International Law Association's International Committee on Use of Force, a member of the editorial board of the Leiden Journal of International Law (Cambridge University Press) and the Scientific Council of the Revue Belge de droit international. He was also a member of the Executive Council and the Board of the French Society for International Law (SFDI) for 12 years. Over the recent years he has been a Visiting Professor at Australian National University, College of Law; at the Università degli Studi di Napoli Federico II; Chuo University, Tokyo; Kobe University, Graduate School of International Cooperation Studies; and the Hague Academy of International Law. Since 2005, he also teaches international law at the Paris School of International Affairs (Sciences-Po Paris). He has been invited to present his work in conferences, symposia and seminars in 25 countries, published or co-edited 9 books and is the author or co-author of more than 60 scientific articles and book chapters that focus on public international law, international security law, international and European protection of human rights, cyber security law and data protection. [Theodore.christakis@univ-grenoble-alpes.fr].

Contribute !
https://jesuisinternet.today

Cyber-Attacks
Prevention-Reactions: The Role of States and Private Actors

Karine BANNELIER,
Associate Professor of International Law, University Grenoble Alpes.
Théodore CHRISTAKIS,
Professor, University Grenoble Alpes, Institut Universitaire de France.

Foreword by Guillaume POUPARD,
Director General of the National Cybersecurity Agency of France (ANSSI).

Revue Défense Nationale is published by the Committee for National Defence Studies,
an association governed by the law of 1901, residing in the
Ecole Militaire, 1 place Joffre, Paris VII.
Postal address: BP 8607, 75325 Paris cedex 07
Fax: +33 (0)1 44 42 31 89 - www.defnat.com - redac@defnat.com

Director: Alain Coldefy - Tel: +33 (0)1 44 42 31 92
Editor-in-chief: Jérôme Pellistrandi - Tel: +33 (0)1 44 42 31 90
Secretary general and *Web site manager*: Paul Laporte - Tel: +33 (0)1 44 42 31 91
Editing secretary-general: Pascal Lecardonnel - Tel: +33 (0)1 44 42 31 90
Assistant to the Director: Marie-Hélène Mounet - Tél: 01 44 42 31 92
Editorial secretariat: Marie-Hélène Mounet and Jérôme Dollé
Subscriptions: Eliane Lecardonnel - Tel: +33 (0)1 44 42 38 23

Publicity managed by: Karim Belguedour - Tél: +33 (0)1 49 60 58 56
ISSN: 2105-7508 - CP N° 1014 G 85493 of 9 September 2010
Printed in France by Bialec, 23 Allée des Grands Pâquis, 54180 Heillecourt

Suggested citation:

Karine BANNELIER and Théodore CHRISTAKIS, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, Les Cahiers de la Revue Défense Nationale, Paris, 2017.

Foreword
What digital society do we want?

The world agrees on the idea that cyberspace constitutes an opportunity for sharing knowledge or increasing economic development. It profoundly modifies the functioning of our societies, our businesses and even our lifestyles. While trade, energy, transport and industry are transforming themselves by leveraging electronic communications as well as increasingly efficient data collection and processing capacities, some are working towards the advent of an "increased humanity", connected in depth and permanently, a world where Man and technology would merge.

The community of States is directly concerned. Cyberspace is a new environment that introduces major issues regarding State's sovereignty. It constitutes a place where it is important to be present and to preserve autonomy of action, despite the fact that cybernetic operations are increasingly used in a manner that could generate conflicts. However cyber developments also have other effects on our societies because, although the manipulation of public opinion is not a new phenomenon, the new opportunities offered by the digital and its "social networks" expose more the citizens as well as their political leaders to a low cost but high impact destabilization.

The Agency in charge of the security and defense of the information systems that I lead notes year after year an increasing number of computer attacks, whose sophistication is also increasing. The main motivation remains espionage and the destabilization of precise targets—government authorities, parliamentarians, public services, industries, the media, etc. Also, numerous aggressive cyber-attacks aiming businesses or individuals, mainly for financial purpose through scam, theft or blackmail, have become more common. Finally, the prospect of terrorist groups resorting to the use of cyber-attacks in order to provoke industrial or ecological disasters and to destroy human lives is unfortunately no longer merely the result of long-term anticipation.

Preparing for and protecting against these attacks, and countering them when they occur, is already sufficient to occupy a large part of the public and private resources of security and defense of information systems. Protecting critical national infrastructures and essential operators to the functioning of society and economy is now a priority for nations that must at the same time succeed in their digital transition, starting with that of their administrations.

Each international organization works according to its field of competence for the adoption of best practices, rules of conduct or the establishment of cooperation mechanisms, which should enable States to combat cybercrime, ensure a certain resilience and avoid escalation during a cyber-confrontation that could be destructive for all Parties involved. For several years there has been an agreement on the applicability of international law and its principles to cyberspace.

What remains is to harmonize the proposals and to confront some of them with the technical reality of cyberspace. Recognized and lawful, regulated practices or valid reasoning, applied in the material world can find their limits in an intangible mode and even more in the hybrid world into which we enter.

The initiative taken by the Secretary General of the French National Defense and Security through the digital platform "jesuisinternet.today", accessible in 11 languages; the seminars linking legal and technical expertise; and the international Conference to be held at UNESCO on 6 and 7 April 2017, aim to contribute to the sharing of ideas and points of view at an international level.

The remarkable study led by Karine Bannelier and Theodore Christakis both precedes and accompanies these ideas and opinions to be shared. Certain major players could be tempted to take measures that may seriously destabilize cyberspace and the hopes it carries. At a time when a market of IT vulnerabilities has emerged, whose analogy in the material world would be viewed as completely unacceptable by public opinion, this study provides the basis and prospects for a debate that can be but international.

I thank the authors of this study as well as the *Revue Défense Nationale*, which made it possible to publish it and, of course, UNESCO whose motto, "Building peace in the minds of men and women" perfectly matches the objectives of our initiative.

Guillaume POUPARD,
Director General of the National Cybersecurity Agency of France (ANSSI)

Preface

The present study aims to conceptualize and present, in a concise manner, the main questions raised in the field of international law regarding the role of the States and private actors in the prevention and the reaction to cyber-attacks.

The study is the result of research carried out by its authors on issues relating to cyber-security, data protection and privacy. It aims to contribute to the reflection of an informed reader (expert in law or cyber-security) while also remaining accessible to non-specialists and the general public, in order to dispel certain confusions or errors of perception that might exist about the fundamental role that international law must have in this field. The security of the digital space, the fight against cyber-crime and data protection are major challenges both for international and national security. While international organizations, States and the private sector are mobilizing to adopt new standards and codes of conduct in this field, existing international law already provides a large number of responses to ensure the peaceful coexistence and cooperation of nations in the digital age.

The authors would like to thank Katerina Pitsoli, Ph.D. Candidate student in cybersecurity, co-supervised by the University of Swansea and the University Grenoble Alpes, for her research assistance and for contributing in the translation and editing of the English version. They also wish to thank Claude Castelluccia and Cédric Lauradoux from *INRIA* (the French Institute for Research in Computer Science and Automation) for their advice and, more generally, all their colleagues from different disciplines who have nourished their reflection in AMNECYS (Alpine Multidisciplinary Network on Cyber security Studies) and the Grenoble Alpes Data Institute. Any error is of course our own. Finally, the authors would like to thank the editorial committee of the National Defense Journal, which has honored them with accepting this study for publication in the *Cahiers de la RDN* collection.

The present study strictly expresses the personal opinions of its authors in the framework of their academic research.

Introduction:
Cyber-Security and International Law

Cybersecurity is terrible, and will get worse.
Adi Shamir (February 2016)

The dramatic rise of cyber-attacks involving States and non-State actors constitutes a real threat to international peace and security. In its 2015 report, the United Nations Governmental Expert Group on Cyber Security (GGE)[1] expressed its concern at "worrying trends" marked by a dramatic increase in the number of malicious acts directed against, *inter alia*, vital infrastructure of States.[2] This alarming fact is now shared by all digital and cyber security actors, regardless of whether they are States, international organizations or private actors.[3] Not only do these attacks threaten critical infrastructures, but they are also a major source of tensions between States.

Over a small number of years, the digital universe has become a space for confrontation not only between States but also between States and certain non-State actors whose destabilizing activities are a major concern for the international community as a whole. As the Secretary-General of the United Nations pointed out, "Among the complex issues that have emerged is the growing malicious use of ICTs by extremists, terrorists and organized criminal groups".[4] The phenomenon is all the more complicated because some States have more or less close ties with these non-State groups and use them as 'intermediaries', 'proxies', to develop malicious activities against the interests of other States.[5]

Yet, besides this important and worrying phenomenon for international peace and security, private actors also play a leading role in the security of digital technology. Private sector activity in this respect is developing in virtually all areas,

(1) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Henceforth "GGE".

(2) "There are, however, disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States, and the misuse of ICTs may harm international peace and security. 4. A number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely. 5. The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious", Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 2015, *Note by the Secretary-General*, A/70/174, 22 July 2015 (henceforth *GGE 2015*).

(3) In February 2017, participants in the OSCE Conference on Critical Infrastructure Protection further emphasized the crucial importance of protecting vital infrastructure against cyber-attacks for international peace and security. *Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE*, Vienna, 15 February 2017.

(4) *GGE 2015*, *supra* note 2, p. 4.

(5) For these questions, see *infra*, Part 1 (Introduction).

from preventing cyber-attacks and securing digital infrastructures to "active cyber defense" measures, including the use of offensive techniques like "hacking back",[6] passing through activities such as the attribution of cyber-attacks.[7] Private sector activities in the area of cyber-security, however, raise several issues and controversies, of political, ethical, technical and legal nature.

The purpose of this study is to contribute to the reflection on these issues by shedding light on an important aspect which will undoubtedly be at the center of the international community's concerns in the years to come, namely the respective roles of public and private actors regarding the safeguarding of peace and security of digital space, within the framework of international law.

In 2013, the members of the GGE recognized the application of international law, including the Charter of the United Nations, in the cyberspace. This recognition was an important milestone for the GGE, as well as for digital peace and security. The cyberspace is not a "No Law's Land"; rather, it can be regulated by international law, as are virtually all international activities. But the task in this field is infinitely more complex. More specifically, determining how international law applies in the digital space inevitably brings us back to the problem of the identification and interpretation of existing rules, but also to the question of their relevance and their limitations in the cyberspace.

It is clear that there are very few legal instruments in international law specifically dedicated to cyber security. Not only are international conventions in this field scarce, but their impact is often limited, either due to the small number of participants or the restricted nature of their subject matter;[8] the Budapest Convention on Cybercrime being, arguably, the most effective for the time being.[9] In this context, conventional and customary rules should be applied, despite their not having been specifically designed to regulate cyberspace. Such a practice of applying rules to areas outside their original scope of application is not unusual in international law; however, it does require some caution. The limited number of binding international rules designed specifically for the regulation of cyberspace seems to be proof of the reluctance of many States to act decisively for the development of new conventional rules on cyber security.

This situation has left the field open to different private initiatives ranging from the refusal of any regulation ("leave the Internet alone!"), to the promotion of a self-regulation of cyberspace by the private actors themselves. Some major players in the digital industry have also embarked on a new path of proposing

(6) A term which designates, as we shall see, a digital counter-attack capable of using methods as varied as "hacking" itself. See Part III.

(7) For all these questions see Part III.

(8) The African Union Convention on Cyber Security and Protection of Personal Data of 2014, for example, has not yet been ratified by any State.

(9) Council of Europe, *Convention on Cybercrime*, 2001, Budapest, currently ratified by 52 States.

norms to regulate not only their own behavior in a self-regulation-like logic, but the behavior of the States too. The most notable initiative in this respect is undoubtedly that of Microsoft, which in 2015 proposed to States a series of cyber security standards,(10) followed by the publication in 2016 of a document on their implementation and, in February 2017, a call for the adoption of a new Geneva Convention to protect civilians from State attacks on the Internet.(11) Numerous academic initiatives have also taken up the question of the identification and interpretation of international law in cyber space, the most well-known achievement in cyber security being the publication of the *Tallinn Manuals 1* and *2.0*.(12)

This major role of private actors in cyberspace constitutes a radical disruption of the landscape of international law and the relations between public and private actors.

Traditionally, international law is called upon to intervene so as to **protect** certain specific categories of non-State actors, either against the actions of foreign States (protection of foreigners, protection of investments, etc.) or against the actions of States under the jurisdiction of which the private actors find themselves (e.g. in the field of human rights, minority protection or indigenous peoples). It may also intervene in order to **impose obligations** directly on both non-State actors and States, as in the fight against piracy or on the prevention and repression of certain international crimes such as genocide, crimes against humanity, war crimes, organized crime and terrorism. Since 11 September 2001, the fight against terrorism has indeed brought to the forefront the question of the role of non-State actors in international law and the rights and obligations of States in relation to them.

Whatever the challenges posed by these questions to international law, generally, relations between States and non-State actors have remained affected by a clear disequilibrium in favor of States, linked not only to the difference in legal status between the former (holders of sovereignty and important powers) and the latter ("subjects" to the States), but also because of the *de facto* diversity of power, resources and capacities of each. Indeed, the State has almost always emerged as possessing an unparalleled power conferring upon it unquestionable pre-eminence on private actors, which are both dependent on its protection

(10) Microsoft, *Reducing Conflict in an Internet-Dependent World*, 2015, followed in 2016 by a document concerning the implementation of these standards by States, Microsoft, *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, 2016 (https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf).

(11) Brad Smith, "The need for a Digital Geneva Convention", RSA Conference, San Francisco, 14 February 2017 (https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention).

(12) Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013 (henceforth *Tallinn Manual 1*) and M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017 (henceforth *Tallinn Manual 2.0*). This manual has just been published and the authors of this study relied only on an electronic edition for consultation.

(individuals, minorities, investors, etc.) and confronted with its powers of regulation, jurisdiction, enforcement.(13)

This traditional model is disrupted profoundly by the paradigm of cyber security. And this disruption takes place while cyberspace constitutes a major challenge in terms of national security, as highlighted by many States that have published over recent years their "Strategies of National Cyber Security".

The top tech companies appear to be as powerful as States, and sometimes even more so, to prevent cyber-attacks, attribute them and to respond to malicious acts. As Michael N. Schmitt and Sean Watts noted:

> "Classically, states and non-state actors were differentiated not only by disparities in legal status, but also by significant imbalances in resources and capabilities. Not surprisingly, international law developed a state-centric bias to account for these imbalances. Cyberspace and cyber operations, however, have closed a number of formerly significant gaps between states' and non-state actors' abilities to compromise international peace and security. In fact, some non-state actors now match, if not exceed, the cyber capabilities of many states in this respect".(14)

The technical capabilities of the digital giants and their economic strength are not commensurate with those of many States, especially the less technologically advanced ones. The very architecture of the Internet seems to reinforce this situation, by constituting a challenge for the traditional mode of a "centralized" governance of the States, seemingly favoring the role of the private actors that are active in cyberspace.(15) Private companies are increasingly involved in cyber security, either autonomously or in conjunction with States, in multi-faceted "public/private" relations that go far beyond traditional patterns. The structure of these relations and the complex partnerships between States and private actors in the fields of cyber-defense and cyber-attack, as well as their legal and political consequences, remain largely to be identified and theorized. The key role of private actors in these areas is promised to last, firstly because these actors are directly affected by cybercrime and cyber-attacks and, consequently, consider that they must protect themselves; and then, because the Internet, data, artificial intelligence, Internet of Things (IoT), cloud and a number of other digital wonders that appear day after day, have a huge potential for growth that companies are determined to defend and exploit. The cyber security market itself is all the more booming as threats to digital security continue to grow over time.

In this context, there is an urgent need for in-depth reflection on the respective roles of States and private actors regarding peace and security in cyberspace.

---

(13) This phenomenon of legal and *de facto* inequality between States and non-State actors was particularly evident in the so-called "regal" areas which lie at the heart of quintessentially governmental functions: the protection of national security; the fight against organized crime; and the conduct of foreign policy.

(14) M.N. Schmitt and Sean Watts, "Beyond State-Centrism: International Law and Non-state Actors in Cyberspace", *Journal of Conflict & Security Law*, Vol. 21, No. 3, 2016, p. 1.

(15) This does not mean that the governance of cyber security must follow exactly the same pattern as the governance of the Internet.

This reflection must take into account the extreme complexity of the problem, marked by the great diversity of the actors involved: potential perpetrators of cyber-attacks (States, 'proxies', private actors supported or tolerated by States, terrorists, cybercriminals, companies conducting espionage or wanting to gain a competitive advantage, individual hackers, patriotic hacker groups, etc.); potential victims of attacks (States, administrations and communities, companies, media, individuals, etc.); those involved in these attacks (e.g. the States through which cyber-attacks transit, companies and individuals whose systems are used by the attackers without the knowledge of the owners); and, finally, those to be potentially involved in a response to a cyber-attack (States, private companies acting for their own benefits, private companies undertaking a response on behalf of another company, etc.). This situation creates an impressive number of combinations, which in their respective turns affect the type and appropriateness of a response.

This reflection must also take into account the frequent international or transnational character of cyber-attacks which makes this problematic almost naturally a problematic relating to international law.

The object of our study is, precisely, to present the main answers that international law brings today to these questions. We will voluntarily adopt here a broad definition of the term "cyber-attack"(16) to examine the roles of states and private actors in preventing and responding to cyber-attacks.

In the first part, we will focus on the issue of prevention and show that the concept of "cyber-diligence", which we have forged on the basis of existing international law and the obligation of any State not to allow knowingly its territory to be used for acts contrary to the rights of other States , provides a satisfactory answer to the question of vigilance that States should exercise with regard to cyber-operations developed from their territory by private actors (I).

In the second part, we will examine those responses to cyber-attacks which can be developed in accordance with international law. This will be done by classifying the possible reactions to cyber-attacks, and by proposing a kind of "user's manual" for victim States that wish to react within the limits of international legality (II).

In the third part, we will present a detailed study of the issues related to "hack-back" and "active cyber defense". After analyzing the advantages, disadvantages and risks of hack-back, we will answer to the question of whether private actors can unilaterally undertake cyber-offensive measures in accordance with the law, and examine to what extent States can authorize a hack-back operation and/or rely on private actors to conduct counter-attacks (III).

(16) See in detail *infra*, Part II (Introduction).

PART I. Cyber-diligence: a key concept in dealing with transnational malicious acts

I. Cyber-diligence: a key concept in dealing with transnational malicious acts

Introduction

The acknowledgement of the growing development of cyber-attacks and hack-back measures by private actors is often associated with the idea that States do not assume any international obligation or responsibility *vis-à-vis* such 'private' acts. The idea is largely erroneous and seems to be based on a double misunderstanding concerning both cyberspace and the international law that applies to it.

The first source of misunderstanding comes from a representation of cyberspace as including neither territories, nor defined boundaries. In fact, the physical infrastructure that supports the Internet, the cyber activities developed under its auspices and the data produced are largely located within the territory of sovereign States or are under their control.(17) The territoriality of cyberspace has been clearly recognized by the members of UN GGE in their 2015 Report, where it was highlighted that: "States have jurisdiction over the ICT infrastructure located within their territory".(18) It is thus recognized that the territorial jurisdiction of States is exercised whatever the nature and origin of the activities, whether physical or digital, public or private, national or foreign.

The second source of misunderstanding derives from the assumption that international law is silent when activities are of private origin, since it is supposed to regulate only inter-State relations. International law is nonetheless very clear in this respect: States, by virtue of their sovereignty, have obligations with regard to private activities which take place on their territory, under their jurisdiction or under their control, and may in certain circumstances be held responsible for such activities.

There are mainly two hypotheses according to which a State may be held responsible for the conduct of private persons. The first concerns the case where the acts of private persons are to be considered as acts of the State itself (A). This hypothesis has been examined in detail by the United Nations International Law Commission (ILC) in its *Articles on the Responsibility of States for Internationally*

(17) As highlighted, in fact, by Harold H. Koh, "The Physical infrastructure that supports the internet and cyberactivities is generally located in sovereign territory and subject to the jurisdiction of the territorial State", *in* H.H. Koh, "International Law in Cyberspace", United States Cyber Command Inter-Agency Legal Conference, Fort Meade, MD, 18 September 2012, *Harvard International Law Journal Online*, Vol. 54, 2012, p. 6 (www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf).

(18) *GGE 2015*, *supra* note 2, §28 (a).

Wrongful Acts adopted by UN General Assembly in 2001.[19] The second hypothesis concerns a situation where a State has violated its obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other States"[20] (B).

A) The act of a private person as the act of the State

The act of a private person may, under certain conditions, be assimilated to that of a State and, thus, engage its responsibility. Two situations must concern us in particular regarding this question: first, the situation in which private persons (natural or legal) may be "acting on the instructions of, or under the direction or control of, that State";[21] and, second, the situation where a State "acknowledges and adopts the conduct in question as its own".[22] In both cases, damage caused to third States as a result of the activities of such private persons, is considered to be a violation of international law by the State itself.[23]

In cyber space, the use of private persons in the form of 'intermediaries' or 'proxies' is a widespread practice among States which seek to develop different operations in a clandestine way.[24] In 2013, the GGE Report echoed the concerns of the international community in this regard by stating that "States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs".[25] In its 2015 Report, the GGE strongly reiterated this affirmation by highlighting that "States must meet their international obligations regarding internationally wrongful acts attributable to them under international law"[26] and that they "must not use proxies to commit internationally wrongful acts using ICTs".[27]

The attribution of the acts of private persons to the States remains nevertheless a sensitive and delicate operation. It is rare that a State recognizes and

(19) International Law Commission, "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", *Yearbook of the International Law Commission 2001*, Vol. II. Part. 2 (henceforth: *YILC 2001*).

(20) *Corfu Channel Case*, Judgment of 4 April 1949, *ICJ Reports 1949*, p. 22.

(21) Article 8. Conduct directed or controlled by a State: "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct", *YILC 2001*, *supra* note 19, p. 47.

(22) Article 11. Conduct acknowledged and adopted by a State as its own: "Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own", *ibid*., p. 52.

(23) See in this regard our analyses *infra* Part III.

(24) Numerous studies have been dedicated to this phenomenon; among the most recent ones, see for example, Tim Maurer, "'Proxies' and Cyberspace", *Journal of Conflict & Security Law*, Vol. 21, No. 3, 2016, 383-403.

(25) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Note of Secretary-General*, A/68/98, 24 June 2013, §23. (henceforth: *GGE 2013*).

(26) *GGE 2015*, *supra* note 2, §28 (f), emphasis added.

(27) *Ibid*. §28 (e).

adopts as its own the behavior of these persons. Moreover, the number and diversity of private persons who are developing activities in cyberspace and the varying intensity of their links with States, render the attribution of their conduct to the State by virtue of instructions, directives or control, particularly difficult to establish.(28) This operation is all the more difficult in relation with malicious transnational cyber-operations, since locating the origin of an act in a given territory is not sufficient to attribute the act in question to the State. As pointed out by the GGE in its 2015 Report, "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State".(29) The degree of certainty required to establish the attribution of a cyber-attack to a State is also obviously a crucial issue, as the GGE 2015 Report observes: "the accusations of organizing and implementing wrongful acts brought against States should be substantiated".(30) In the second part of this analysis we will examine what evidence must be provided by a State prior to reacting to a cyber-attack, and what degree of certainty is required by international law (*infra* Part II, 2A). In any case, attribution of a malicious cyber act of a private person to a State may sometimes be a particularly difficult operation.

B) The obligation of every State "not to allow knowingly its territory to be used for acts contrary to the rights of other States"

States may be held responsible for the acts of private actors by virtue of "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".(31) This obligation refers directly to the responsibility of States for the acts of private persons, regardless of the relations between them and irrespective of the precise nature of the acts in question, whether cyber-attacks, hack-back measures or any other activity. This obligation generates a duty of 'vigilance', **due diligence** which stems directly from the sovereignty of States.

The concept of cyber-diligence,(32) expressing this duty in the cyberspace, can play a central role in building international peace and security in the digital era (1). In fact, it indicates a standard of reasonable and responsible behavior of

(28) See especially, on this question, M.N. Schmitt and Liis Vihul, "Proxy Wars in Cyber Space: The Evolving International Law of Attribution", *Fletcher Security Review*, Vol. I., No. 2, 2014, 55-73 (https://ccdcoe.org/sites/default/files/multimedia/pdf/c28a64_2fdf4e7945e9455cb8f8548c9d328ebe.pdf) ;

Kubo Macak, "Decoding Article 8 of the International Law Commission's Article on State Responsibility: Attribution of Cyber Operations by Non-State Actors", *Journal of Conflict & Security Law*, Vol. 21 No. 3, 2016, 405-428.

(29) *GGE 2015*, *supra* note 2, §28 (f).

(30) *Ibid*.

(31) *Corfu Channel Case*, *op. cit.*, p. 22.

(32) This term was first used in Karine Bannelier, "Cyber-Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber-Operations?", *Baltic Yearbook of International Law*, Vol. 14, No. 1, 2014, 23-39. This legal concept, in conjunction with the development of voluntary tools, namely confidence building measures and capacity building initiatives, could efficiently strengthen international peace and security in the cyberspace.

States (2) to prevent and put an end to cyber-attacks launched by private actors from their territory against the territory or infrastructures of other States (3).

1. « He who can and does not prevent, sins»: the concept of cyber-diligence

"*Qui peut et n'empêche, pèche*": "He who can and does not prevent, sins";(33) the saying by Antoine Loysel, a French lawyer of the seventeenth century, famous for having collected the customary rules of the Kingdom of France, reflects well what the concept of cyber-diligence expresses in the 21st century towards sovereign States in cyber space: to intervene, when they know and they may, in order to prevent acts infringing the rights of third States.

A) State sovereignty at the heart of the concept of cyber-diligence

In cyberspace, the responsibility of States to intervene, wherever they can, originates directly from their sovereignty over infrastructure within their territory. As the GGE members pointed out in their 2015 Report: "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory".(34) The "norms and principles" which derive from State sovereignty are in fact associated with rights for the benefit of States but also, as a corollary, with duties for States. This close correlation between the rights and duties of sovereign States has been famously expressed by the Arbitral Award rendered in 1928 in the *Island of Palmas Case*. According to it: "Territorial sovereignty […] involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war".(35)

Sovereign States have the **right** to have their territorial integrity respected, but they also have the **duty** not to use or allow their territory to be used in such a way as to undermine the territorial integrity of another State: *sic utere tuo ut alienum non laedas*.(36) As pointed out in the 1925 Arbitral Award in the *Spanish Zone of Morocco Claims*: "[t]he responsibility for events which may affect international law and which occur in a given territory goes hand in hand with the

(33) Antoine Loysel, *Institutes coustumieres, ou manuel de plusieurs et diverses reigles, sentences, et prouerbes, tant anciens que modernes, du droict coustumier et plus ordinaire de la France*, A. L'Angelier, Paris, 1607 (https://archive.org/details/1607LoiselInstitutesCoutumieres).

(34) *GGE 2015*, *supra* note 2, §27. Already in 2013, the GGE report supported that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory", *GGE 2013*, A/68/98, 24 June 2013, §20.

(35) Permanent Court of Arbitration, *Island of Palmpas case*, *USA v. The Netherlands*, Arbitral Award of 4 April 1928, *RIAA*, Vol. II, p. 839.

(36) "Make use of your property so as not to infringe on that of another".

right to exercise, to the exclusion of other States, the prerogatives of sovereignty".(37)

The duty of using one's territory so as not to injure the rights of others has been repeatedly reaffirmed by international jurisprudence, starting with the famous *dictum* of the International Court of Justice in the Corfu Channel Judgment, concerning "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".(38)

By virtue of their sovereignty, States have an obligation of vigilance, of **due diligence**, with regard to the activities taking place in their territory or under their control and, in the event of a breach of this obligation they may, under certain conditions, be considered responsible for infringements of the rights of third States.

B) The responsibility of States for transnational attacks and damage to third States

In the Corfu Channel Judgment, the International Court of Justice condemned Albania for breaching its duty of vigilance as mines laid in its territorial waters had caused damage to British ships. In the Judgment, the Court did not condemn Albania for having laid down the mines, but rather, asserted that Albania was liable for the damage caused to the United Kingdom insofar as, having undoubtedly knowledge of the existence of the minefield, Albania had not taken reasonable measures within its power to prevent the incident and the damage.

This obligation of vigilance, which derives from the sovereignty of States, is thus binding on States irrespective of the identity of the authors of such activities. In this respect, it is important to emphasize that, historically, this obligation of vigilance was first developed in relation to the responsibility of States for private activities.(39) The first known application of this obligation by international jurisprudence concerned the responsibility of a State, the United Kingdom, for acts of private companies. In the Alabama case, the United Kingdom was convicted for violating its due diligence obligation by allowing private companies to build and arm, within its territory, the Alabama vessel which was to serve in the Confederate army against the Union during the war of secession in the United States.(40)

Since then, the principle of **due diligence** has been applied by international jurisprudence in relation to very different activities and in very diverse fields,

(37) *Spanish Zone of Morocco Claims*, *UK v. Spain*, Arbitral Award of 1 May 1925, *RIAA*, Vol. II, p. 649. English translation in 'Report of the International Law Commission on its 31st Session', *ILC Yearbook 1979*, Vol. II, Part Two, p. 98, note 505.

(38) *Corfu Channel Case*, *op. cit.*, p. 22.

(39) See Timo Koivurova, "Due diligence", *Max Planck Encyclopedia of Public International Law* (www.mpepil.com).

(40) Alabama *claims of the United States of America against Great Britain*, Award rendered on 14 September 1872 by the Tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, *RIAA*, Vol. XXIX, p. 130.

such as the law of the sea,[41] human rights,[42] the protection of the environment[43] and the protection of individuals, diplomats and foreign States against insurgencies and cross-border attacks by non-State groups.[44] For example, in the *Case concerning armed activities on the territory of the Congo* between DRC and Uganda, the latter asserted, on the basis of the Corfu Channel Judgment, that the DRC had violated its due diligence obligation by not preventing armed groups from launching attacks against Uganda from within DRC's territory.[45] Although the International Court of Justice finally refused to consider that the DRC's inability to put an end to these attacks constituted, in the factual circumstances of that case, a breach of its due diligence obligation, it admitted, like the DRC, that such an obligation existed for States in the context of cross-border attacks by non-State actors.[46]

C) The usefulness of the concept of cyber diligence in the face of cyber-attacks

The obligation not to allow one's territory to be used for acts contrary to the rights of other States is binding on States irrespective not only of the perpetrator of the activity but also of the precise nature of the act in question. Such act can consist of a physical or digital activity, it can be high or low-tech. Already in 2001, the ILC in its "Draft articles on Prevention of Transboundary Harm from Hazardous Activities",[47] had insisted that the States' duty of care with regard to so-called hazardous activities was necessary for **all activities** from the moment that they entailed a risk of causing significant transboundary harm.[48] In its commentary to Article 1, the Commission explained that it refused to draw up a list of such activities because such a list would be immediately outdated by the rapidly changing technologies.[49]

The activities developed in cyberspace do not escape this rule. In its 2015 Report, the GGE, without expressly naming the concept of cyber-diligence, expressed this idea in several places. It mentioned in particular that the States

(41) See, for example, ITLOS, *Responsibilities and obligations of States with respect to activities in the Area*, Advisory Opinon, 1 February 2011, *ITLOS Reports 2011*, p. 10.

(42) See, for example, ECtHR, *Osman v. UK Case*, Judgment of 28 October 1998, *ECtHR 1998*, Vol. VIII.

(43) See, for example, *Trail Smelter Arbitration* (*United States v. Canada*), Arbitral Award of 11 March 1941, *RIAA*, Vol. III, p. 907; or the *Pulp Mills on the River Uruguay Case* (*Argentina v. Uruguay*), Judgment of 20 April 2010, *ICJ Reports 2010*, p. 14.

(44) See, for example, *Thomas H. Youmans (USA) v. United Mexican State*, 23 November 1926, United Nations, *RIAA*, Vol. IV. See, also *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, *ICJ Reports 1980*, p. 3.

(45) *Case concerning armed activities on the territory of the Congo (DRC v. Uganda)*, Judgment of 19 December 2005, *ICJ Reports 2005*, §277.

(46) *Ibid*. §283 et 300-303.

(47) ILC, "Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries", *2001 Yearbook of the ILC*, Vol. II, No. 2, p. 148f.

(48) *Ibid.*, Article 1, p. 149.

(49) *Ibid*. In this regard, see also the judgment of the ICJ in the Pulp Mills case, according to which due diligence must be exercise "in respect of all activities which take place under the jurisdiction and control of each party", *Pulp Mills on the River Uruguay Case*, *op. cit.*, §197.

"should seek to ensure that their territory is not used by non-State actors to commit such acts"(50) and that they "should not knowingly allow their territory to be used for internationally wrongful acts using ICTs".(51)

Therefore, the question is not whether States have an obligation not to knowingly allow their territory and infrastructures to be used by private actors so as to launch cyber-attacks against other States, as it is clear that such an obligation exists. Rather, the question is how far and in what ways can this obligation be imposed on States in cyberspace, and when we could consider that a State "knew", "could" but did nothing to prevent.

2. Cyber-diligence as a responsible and reasonable standard of behavior

The due diligence standard in relation with the duty to use one's territory in a manner that does not injure the right of other States, designates an obligation of **conduct** and not an obligation of result. This is a fundamental characteristic of this obligation which is unanimously accepted and which has never been questioned. It requires States to be reasonably vigilant with respect to the activities that are developped within their territories, according to their respective capacities.

A) An obligation of conduct and not of result

The exercise of territorial sovereignty by States does not mean that they must necessarily be aware of everything that is happening within their territory, or that they are in a position to be able to prevent everything. The degree of vigilance expected is that "of a good Government".(52) All international courts, tribunals and other bodies that have had to interpret and apply the principle of **due diligence** assert that the test of "reasonableness" must guide its application and that it "does not impose an impossible or disproportionate burden on the authorities".(53) This means, first of all, that the knowledge by a State of a cyber-attack launched by private persons from its territory against a third State cannot be presumed. As reiterated by the ICJ in the *Corfu Channel Case*, "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known, the authors".(54) On the other hand, it goes without saying that sovereign States

(50) *GGE 2015*, *supra* note 2, §28 (e).

(51) *Ibid.*, §13 (c).

(52) ILC, "Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries", *op. cit.*, §17, p. 155. For an extensive analysis of the concept of due diligence, see Riccardo Pisillo Mazzeschi, *"Due diligence" e responsibilita internatzionale degli Stati*, Milano, Dott. A. Giuffré editore, 1989, 418 p ; and also R. Pisillo Mazzeschi, "The Due Diligence Rule and the Nature of the International Responsibility of States", *German Yearbook of International Law*, Vol. 35, 1992, 9-51.

(53) ECtHR, *Osman v. UK Case*, Judgment of 28 October 1998, §116.

(54) *Corfu Channel Case*, *op. cit.*, p. 18.

cannot reasonably disregard everything that happens on their territory. As pointed out by the Court in the same case, "a State on whose territory or in whose waters an act contrary to international law has occurred, may be called upon to give an explanation. It is also true that that State cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and of its authors. The State may, up to a certain point, be bound to supply particulars of the use made by it of the means of information and inquiry at its disposal".(55)

A sensitive issue, which is particularly acute in cyberspace, is to determine the extent to which a sovereign State 'must know', 'ought to have known' or 'ought to seek to know', notably by monitoring activities which take place on its territory. This issue has already been widely discussed by international jurisprudence, particularly in the field of human rights, within the framework of the "positive obligations" of States,(56) or in the field of the protection of the environment.(57)

It seems that States should exercise control over the activities developed on their territory. However, this does not mean that they are allowed to use such a pretext in order to develop mass surveillance and, thus, erode essential freedoms, starting with the right to privacy and protection of data and correspondence. As underlined by the International Court of Justice in the *Case concerning the application of the Convention on the Prevention and Punishment of the Crime of Genocide*, "it is clear that every State may only act within the limits permitted by international law".(58)

In this regard, the members of the GGE recalled in their 2013 Report the need for States to respect the fundamental rights of persons: "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments".(59) In 2015, the GGE members returned to this fundamental issue by emphasizing the "central importance" of the respect of human rigths and fundamental freedoms by States, as well as the fact that "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166

(55) *Ibid*.

(56) As the ECtHR said in the Osman v. UK case, "where there is an allegation that the authorities have violated their positive obligation […] it must be established to its satisfaction that the authorities knew or ought to have known at the time of the existence of a real and immediate risk to the life of an identified individual or individuals from the criminal acts of a third party and that they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk", ECtHR, *Osman v. UK Case*, *op. cit.*, §116.

(57) In the Pulp Mills on the River Uruguay Case, the ICJ considered that the obligation to prevent implied "the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party", *Pulp Mills on the River Uruguay Case*, *op. cit.*, §197.

(58) *Case concerning the application of the Convention on the Prevention and Punishment of the Crime of Genocide, Bosnia-Herzegovina v. Serbia and Montenegro*, Judgment of 26 February 2007, *ICJ Reports 2007*, §430.

(59) *GGE 2013*, A/68/98, 24 June 2013, §21.

on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression".(60)

The criterion of reasonableness not only assesses the extent to which States are or should be aware of the activities taking place on their territory, it also makes it possible to determine whether a State has applied the "best efforts" at its disposal in order to prevent or preclude the infringement of the rights of a third State. The fact that a State ultimately fails and, consequently, does not manage to prevent such an infringement does not in itself constitute a breach of the duty of care. As stated by the ICJ in the *Case concerning the application of the Convention on the Prevention and Punishment of the Crime of Genocide*, "a State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment in concreto, is of critical importance".(61)

Given the complexity of the cyberspace and the instantaneous deployment and effects of cyber-attacks, the due diligence standard obviously does not require States to prevent all cyber-attacks. An evaluation of the circumstances and the capacities of each one is, among other things, necessary.

B) An obligation based on the principle of common but differentiated responsibility?

In practice, several criteria can determine the capacity of a State to fulfill its obligations of due diligence in cyberspace. These criteria concern both the circumstances of each case and the capacity of each State which, as international jurisprudence recognizes "varies greatly from one State to another".(62) In its work on the prevention of transboundary harm, the ILC empasized that: "The economic level of States is one of the factors to be taken into account in determining whether a State has complied with its obligation of due diligence".(63)

Alongside this economic criterion, it is clear that in cyberspace, the obligation of States to take all reasonable measures must also be assessed according to the level and technological capabilities of each. Not all States have the same capacities

(60) *GGE 2015*, *supra* note 2, §13 (e).

(61) *Case concerning the application of the Convention on the Prevention and Punishment of the Crime of Genocide*, *op. cit.*, §430. As stated by the International Law Commission: "[o]bligations of prevention are usually construed as best efforts obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur", *YILC 2001*, *supra* note 19, p. 62.

(62) *Ibid*. Also, in the *Alabama* Arbitration, the USA already defined due diligence as "in proportion to the magnitude of the object, dignity and strength of the power which is to exercise it" (Alabama *claims of the United States of America against Great Britain*), *in* John B. Moore, *International Arbitrations to which the United States has been a Party*, Vol. 1, 572–573.

(63) ILC, "Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries", *op. cit.*, Article 3, commentary §13, p. 155. The Commission explains that "It is, however, understood that the degree of care expected of a State with a well-developed economy and human and material resources and with highly evolved systems and structures of governance is different from States which are not so well placed", article 3, commentary §13, p. 155.

to protect their computer networks from malicious use. The concept of cyber-diligence therefore implies the principle of common but differentiated responsibility between States. This responsibility is **differentiated** because States are unequal on an economic and technological level, but it is also **common** as due to the interconnection that characterizes the digital world, the vulnerabilities of the essential infrastructures of a State can have serious consequences on others. As pointed out by the GGE in 2013, "Different levels of capacity for ICT security among different States can increase vulnerability in an interconnected world".(64) Nevertheless, it should be recalled that, whatever these inequalities, States cannot disengage altogether from their sovereign duties. As the ILC has highlighted, "vigilance, employment of infrastructure and monitoring of hazardous activities in the territory of the State, which is a natural attribute of any Government, are expected".(65)

3. A duty to prevent and respond to cyber-attacks

In the *Case Concerning United States Diplomatic and Consular Staff in Tehran* the ICJ engaged Iran's international responsibility for taking diplomatic and consular personnel as hostages, due to the fact that the Iranian authorities had taken no steps to prevent or react to this act. According to the Court, the Iranian authorities"(b) were fully aware, as a result of the appeals for help made by the United States Embassy, of the urgent need for action on their part; (c) had the means at their disposa1 to perform their obligations; (d) completely failed to comply with these obligations".(66)

However, it is necessary to examine the concrete measures that States should or could reasonably take to prevent the use of their digital infrastructures by private individuals to launch cyber-attacks (A) and to react to these attacks (B).

A) Preventing cyber-attacks and protecting critical digital infrastructures

In the *Alabama Case*, the Tribunal considered that "the British government failed to use due diligence in the performance of its neutral obligation; and especially that it omitted, notwithstanding the warnings and official representations made by the diplomatic agents of the United States during the construction of the said number '290', to take in due time any effective **measures of prevention**, and that those orders which it did give at last, for the detention of the vessel, were issued so late that their execution was not practicable".(67) This obligation of

(64) *GGE 2015*, *supra* note 2, §10.

(65) ILC, "Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries", *op. cit.*, article 3, commentary §17, p. 155.

(66) *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, *ICJ Reports 1980*, §68.

(67) *Alabama claims of the United States of America against Great Britain*, Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, *RIAA*, Vol. XXIX p. 130. Emphasis added.

prevention was subsequently reaffirmed on several occasions by international courts in various cases. In the *Corfu Channel Case*, the International Court of Justice held that Albania was responsible because it had done nothing to prevent the disaster: "In fact, nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania".(68) Similarly, in the *Case of Armed Activities on the Territory of the Congo*, the Court found Uganda responsible for the "lack of vigilance in preventing violations of human rights and international humanitarian law by other actors present in the occupied territory, including rebel groups acting on their own account".(69)

In cyberspace, it could be inquried whether this preventive obligation should lead States to take concrete legislative and technical measures to prevent unauthorized use of their digital infrastructures by private persons for malicious purposes against other States.

The protection of critical infrastructure is an essential aspect of digital security, as reflected in the work of the UN General Assembly on cybersecurity and critical infrastructure protection. In its resolution 64/211 of 21 December 2009 entitled *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, the General Assembly proposes that States adopt a "voluntary self-assessment tool for national efforts",(70) which would encourage them to develop measures in order to protect their critical digital infrastructures. Many other international organizations, such as the OSCE as part of its confidence-building measures,(71) the OECD,(72) the EU,(73) the African Union,(74) and the Shanghai Cooperation Organization(75) have developed important reflections and proposals in this field. As summarized well in the 2015 Report of the GGE, "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions".(76)

(68) *Corfu Channel Case*, *op. cit.*, p. 23.

(69) *Case concerning armed activities on the territory of the Congo (DRC v. Uganda)*, Judgment of 19 December 2005, *ICJ Reports 2005*, *op. cit.*, §179.

(70) A/Res/64/211, 21 December 2009, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*.

(71) See, for example, OSCE, *Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, Decision No. 1201, 10 March 2016.

(72) OECD, *Recommendation of The Council on The Protection of Critical Information Infrastructures*, OECD Ministerial Meeting on the future of the Internet Economy, Seoul, 17-18 June 2008.

(73) See especially, in this regard, the Directive (UE) 2016/1148 of the European Parliament and Council of 6 July 2016 *concerning measures for a high common level of security of network and information systems across the Union*.

(74) African Union Convention on Cyber Security and Personal Data Protection of 27 June 2014.

(75) Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on *Cooperation in the Field of international Information Security*, 16 June 2009.

(76) *GGE 2015*, *supra* note 2, §13 (g).

It goes without saying that the obligation of prevention is an obligation of behavior which varies according to the capacity of each State. In this respect, it may be considered that the ability to legislate so as to prohibit the malicious use of IT infrastructure is a common capability for all sovereign States. On the other hand, as we have already pointed out, technical capacities vary greatly between States. In order to effectively prevent malicious use, it is probably necessary to develop technical co-operation between States. Private sector participation is essential in this regard as many digital infrastructures around the world are private.

In light of all the jurisprudence and the work carried out in different *fora* and international organizations, it seems that a State which is manifestly failing and does not protect its digital infrastructures, allowing private actors to use them in order to launch cyber attacks against other States, could see its responsibility triggered. As the International Court of Justice had pointed out in the *Case concerning the application of the Convention on the Prevention and Punishment of the Crime of Genocide*, "violation of the obligation to prevent results from omission".(77)

A delicate issue, however, concerns the obligations of States with regard to the development and acquisition by private actors of cyber-weapons or cyber-offensive techniques that could be used to conduct cross-border cyber-attacks. Does the obligation of prevention imply a regulation on the part of the States on this topic?

Could the mere acquisition by some private actors of techniques intended for launching cyber-attacks constitute a sufficiently serious risk obliging the States to act and prevent? The answer is particularly sensitive as, since the techniques used to conduct cyber-attacks can be the same as those developed to secure and defend computer systems, it may ultimately depend on their use. The question of the commercialization of so-called dual-use goods and technologies is widely discussed in the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*.(78) Despite the interest it presents, the Wasenaar Arrangement remains a legally non-binding instrument. However, the development in recent years of the trade in zero-day vulnerabilities (*i.e.* uncorrected vulnerabilities) is undoubtedly worthy of a thorough analysis from the point of view of international law. It would be important to analyze to what extent trade by private actors of zero-day vulnerabilities could be considered as constitutive of

(77) *Case concerning the application of the Convention on the Prevention and Punishment of the Crime of Genocide*, *op. cit.* According to the Court, "[…] a State's obligation to prevent, and the corresponding duty to act, arise at the instant that the State learns of, or should normally have learned of, the existence of a serious risk that genocide will be committed. From that moment onwards, if the State has available to it means likely to have a deterrent effect on those suspected of preparing genocide, or reasonably suspected of harbouring specific intent (dolus specialis), it is under a duty to make such use of these means as the circumstances permit", §431.

(78) *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (www.wassenaar.org). See especially, in this regard Trey Herr, "Malware Counter-Proliferation and the Wassenaar Arrangement", *in* Nikolaos Pissandis, Henry Roigas and Matthijs Veenendaal (eds.), *Cyber Power, 2016 8th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2016, 175-190.

serious risks of cyber-attacks, in which case States, according to their duty of vigilance, should act by regulating or even prohibiting their marketing and proliferation.(79)

B) Notification and cessation of cyber-attacks

It is well established by international jurisprudence that States of origin have an obligation to notify States affected by harmful activities. This obligation of notification has been clearly affirmed by the International Court of Justice in the *Corfu Channel Case* as a general principle of international law.(80) This means that in cyberspace, States that know that cyber-attacks are launched from their territory and their infrastructures against other States must inform the latter without delay. In this regard, the development of an international notification procedure and international cooperation between CERT/CSIRT(81) could play an essential role in the implementation of this obligation. Such cooperation could also facilitate the notification by the victim States of cyber-attacks towards the States from which these cyber attacks emanated, in order to ensure that the States of origin are aware of the situation and can, thus, take the necessary measures to stop these attacks and to prevent new ones.

Beyond this obligation to notify, it is also self-evident that the States must take all measures in their power to put an end to these cyber-attacks. The obligation of cessation of the unlawful act incumbent on States is a classical obligation of international law which has been repeatedly recalled by international jurisprudence. Thus, in its 2015 Report, the GGE mentioned that "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty".(82)

Finally, along with the technical measures that could be taken by States to put an end to these attacks, they should also investigate and seek to identify, prosecute and condemn the perpetrators of the attacks. In the *Corfu Channel Case*, the Court criticized Albania as "whereas the Greek Government immediately appointed a Commission to inquire into the events of October 22nd, the Albanian

(79) See, for example, M. Fidler, "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis", *I/S: A Journal of Law and Policy for the Information Society*, Vol. 11, No. 2, 2015, 405-482.

(80) The ICJ, thus, held that "The obligations incumbent upon the Albanian authorities consisted in notifying, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in warning the approaching British warships of the imminent danger to which the minefield exposed them. Such obligations are based […] on every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States", *Corfu Channel Case*, *op. cit.*, p. 22.

(81) Computer Emergency Response Team/Computer Security Incident Response Team.

(82) *GGE 2015*, *supra* note 2 §13 (h).

Govemment took no decision of such a nature, nor did it proceed to the judicial investigation incumbent, in such a case, on the territorial sovereign".(83)

The obligation of prevention constitutes, therefore, an obligation of reasonable conduct, which means that States cannot be held automatically liable in the event that they fail to do so. In all the above-mentioned cases, the Court engaged the international responsibility of a State only when it considered that the State in question had not taken all reasonable measures in its power, while it had, or ought to have, knowledge of the risks, in order to avoid damage. As already mentioned, the obligation is proportionate to the capacity of each State. It is also clear that a failure by a State, particularly in the protection of its digital infrastructure, will entail its international responsibility only if it is actually exploited by non-State actors to launch cyber-attacks. As 14§3 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts" states: "The breach of an international obligation requiring a State to prevent a given event occurs when the event occurs".(84)

(83) *Corfu Channel Case*, *op. cit.*, 19-20.

(84) *YILC 2001*, *supra* note 19, p. 391. According to Roberto Ago, "[t]o our knowledge, decisions of international tribunals have never affirmed, even indirectly or incidentally, that failure to adopt measures to prevent the occurrence of a possible event sufficed in itself—*i.e.*, without the actual occurrence of such an event—to constitute a breach of the obligation incumbent on the State", "Seventh report in State Responsibility", *YILC 1978*, §11, p. 34. See also Sarah HEATHCOTE, "State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility", *in* K. BANNELIER, T. CHRISTAKIS and S. HEATHCOTE (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case*, London-New York, Routledge, 2012, p. 311.

PART II. The General Framework of International Law to Respond to Cyber-Attacks

Introduction: looking for a classification of reactions to cyber-attacks

A) The definition of cyber-attacks

B) In search of a criterion for the classification of admissible reactions

1. Reactions in the absence of a violation of international law by another State

A) Mechanisms for international cooperation and dispute settlement

B) Acts of retorsion

C) Exceptional mechanisms of self-protection (state of necessity, distress,* force majeure*)

2. Reactions to violations of international law by another State

A) Peaceful countermeasures

B) Self-defense in case of "armed attack"

II. The General Framework of International Law to Respond to Cyber-Attacks

Introduction: Looking for a classification of reactions to cyber-attacks

In this second part, the different reactions proposed by international law to States that consider they have been victims of cyber-attacks will be analyzed. A **classification** of these reactions will be suggested, revolving around the criterion of the existence or not of an "internationally wrongful act" according to the rules of public international law.

Our analysis will, thus, focus on the general framework of international law providing for the reaction to cyber-attacks. This framework applies in principle to inter-State relations, but we will see here (as well as in Part III) how non-State actors, such as private firms, may fit into the equation of authorized responses against cyber-attacks, as well as the most appropriate responses for such actors (prosecutions, criminal cooperation, arrest warrants, extraditions…).

A) The definition of cyber-attacks

International law does not provide for a unanimously accepted definition of the term "cyber-attack", while States propose very different definitions of this term.(85) In spite of this diversity, it can be observed that the existing definitions seem to converge towards a broad approach to the term "cyber-attack". For example, according to Canada:

> "Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber-attack determines the appropriate level of response and/or mitigation measures: *i.e.*, cyber security".(86)

For the International Committee of the Red Cross (ICRC):

> "Cyber operations can be broadly described as operations against or via a computer or a computer system through a data stream. Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system. By these means, a variety of 'targets' in the real world can be destroyed, altered or disrupted, such as industries, infrastructures, telecommunications, or financial systems".(87)

(85) Please see for example a compilation of different national definitions of "cyber-attack", proposed by the NATO Cooperative Cyber Defence Centre of Excellence (https://ccdcoe.org/cyber-definitions.html).

(86) *Cyber Security Strategy of Canada*, 2010, p. 3 (www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf).

(87) ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflict*, Geneva, October 2011, p. 36. (www.icrc.org/eng/).

According to the *Technopedia dictionary*:

"A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft".(88)

Therefore, for the purposes of our analysis, the term could be defined broadly enough to include a wide variety of techniques and purposes. As the United Kingdom has pointed out:

"The term cyber-attack can refer to anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as: gaining unauthorized access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)".(89)

B) In search of a criterion for the classification of admissible reactions

In light of positive international law, the challenge is to identify the reactions available to States given the wide range of "cyber-attacks" targeting both them and their legal and natural persons.(90) It seems quite obvious that the reaction of States would depend on the severity of the damage caused by cyber-attacks: a more serious attack would logically allow for a more severe reaction. However, the gravity of the damage can be neither the only, nor the decisive criterion for identifying and classifying the relevant answers that could be accepted by international law. Therefore, one can imagine situations where, despite the seriousness of the damage caused by a cyber-attack, it would have been not possible for a State to respond in a vigorous way such as, for example, through the adoption of countermeasures (*infra*). Such could be the case where a cyber-attack has been launched solely by a private actor, and either the act cannot be attributed directly to a State, or the State from where the private actor operated cannot be reproached for having breached its due diligence obligation. Conversely, in other cases, States could respond to a cyber-attack by the adoption of countermeasures even if the attack may have caused limited damage or even none at all, since, as we shall see, damage is not a condition for the exercise of countermeasures (however, it may influence the assessment regarding the proportionality of the reaction).

(88) According to the same source: "Cyberattack is also known as a computer network attack (CNA). Cyber-attacks may include the following consequences: Identity theft, fraud, extortion; Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses; Stolen hardware, such as laptops or mobile devices; Denial-of-service and distributed denial-of-service attacks; Breach of access; Password sniffing; System infiltration; Website defacement; Private and public Web browser exploits; Instant messaging abuse; Intellectual property (IP) theft or unauthorized access" (www.techopedia.com/definition/24748/cyberattack).

(89) Please refer to NATO Cooperative Cyber Defence Centre of Excellence (https://ccdcoe.org/cyber-definitions.html).

(90) International law accepts both the concept of "immediate" (or "direct") injury (resulting from the infringement of a legally protected right of the State itself as a subject of international law) and the concept of "indirect" injury, where the harm to the interests of private persons will be considered as an injury indirectly suffered by their national State itself. Thus, under the so-called "diplomatic protection" mechanism, a State has the right to bring an international claim against another State where one of its nationals has suffered damage as a result of an illegal act of another State. It is then said that the State "takes up the case" for its natural or legal persons by asserting its own right to ensure, in the person of its subjects, respect for the rules of international law.

From the point of view of international law it is, therefore, preferable to adopt another criterion for classifying the reactions which are permissible in the case of a cyber-attack: that of the internationally wrongful act. The expression "**internationally wrongful act**" means an **action or omission attributable to a State, which must constitute a violation of international law**.(91)

We will see that certain reactions to cyber-attacks are always allowed, even in cases where it is impossible to demonstrate that a State has committed a violation of international law (1). Other reactions, on the other hand, are admissible only if it can be established that a State has committed an internationally wrongful act, by an action or omission (2).

1. Reactions in the absence of a violation of international law by another State

The measures to be presented here are available to States (sometimes under certain conditions) whenever they wish to react to a cyber-attack of which they find, either themselves to be victims, or the natural and legal persons within their territory. In other words, to resort to these reactions:

- It is irrelevant whether the cyber-attack was initiated by a State, a non-State actor acting in connection with a State (e.g. a proxy) or a non-State actor acting without any relation to a State;
- It is irrelevant whether or not the cyber-attack can be attributed to a State;
- It is irrelevant whether or not this cyber-attack can be considered to be a violation of international law.

In other words, the reactions described below are admitted whether or not there is an "internationally wrongful act" of a State. There are three types of reactions.

A) Mechanisms for international cooperation and dispute settlement

The development of international cooperation lies at the heart of the mechanisms regarding the reactions of States to cyber-attacks, as reflected in the 2015 report of the GGE, which devotes a lot on this subject in Part V, entitled I*nternational cooperation and assistance in the field of computer security and capacity building*.(92) Such co-operation may be carried out between the States concerned (a), but also with the assistance of the relevant international organizations (b).

(91) For an analysis of these terms see *infra* Part II (2A).
(92) *GGE 2015*, *supra* note 2.

a) Cooperation between the concerned States

Whether or not the cyber-attack of which a State is a victim constitutes an "internationally wrongful act", the first reaction for the victim State is, undoubtedly, to address the State (or States) from where the attack was launched (or transits), in order to ask for their intervention and cooperation.

Non-State actors could, in fact, launch malicious transnational cyber-operations from the territory of certain States without their knowledge. It is therefore natural that the victim State informs the States concerned and requests that they act as soon as possible, in order to put an end to these cyber operations. As we have seen in Part I, States have as a corollary to their sovereignty, the duty to not allow their territory to be used in such a way as to undermine the right to respect for the territorial integrity of another State: *sic utere tuo ut alienum no laedas*. The GGE has also stressed, as we have seen, that "States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory".(93)

A notification to the States from which non-State actors have launched cyber-attacks, followed by a refusal by the non-State actors to cease them, could be considered a breach of due diligence, allowing the victim State to adopt countermeasures. Thus, recourse to the traditional diplomatic mechanisms of cooperation is not just the safest and probably the most effective path to follow, but it is also often necessary to establish that the State **is aware** of the fact that private actors have launched cyber-attacks from within its territory—and that it has done nothing to prevent them.

Inter-State cooperation to end a cyber-attack can take several forms, of course. If the State, from which the cyber-attacks have been initiated, does not have the technical means to act, the victim State or even third States could offer their technical assistance. This is particularly emphasized in the GGE report, according to which "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts taking into account due regard for sovereignty".(94)

"Hack-back" operations (*infra* Part III) could also be developed to neutralize non-State actors, with the consent and under the control of both the victim State and the State of origin of the attack. Of course, the search for effective inter-State co-operation does not prevent the victim State of a cyber-attack from unilaterally taking the necessary technical measures to neutralize the effects of that attack in compliance with its obligations under international law.

(93) *Ibid.*, §13 (h).
(94) *Ibid.*, §13 (h).

Constructive dialogue and cooperation between States should, therefore, be the first reactions to cyber-attacks launched by non-State actors. If such cooperation does not produce the desired results, States may also adopt the traditional methods of peaceful settlement of disputes(95) such as negotiation, mediation, inquiry or resort to mechanisms for the conciliation or adjudication of disputes.

b) Resort to competent international organisations

As the 2015 GGE report notes, mutual assistance between States in dealing with an IT incident could be enhanced "by the competent international organizations, including the United Nations and its agencies".(96)

The best known example is for a State that is the victim of a cyber-attack, to appeal to the UN Security Council if the situation is serious enough to be considered as a threat to peace and international security. Depending on the situation, the Security Council could then act within the framework of Chapter VI of the Charter (peaceful settlement of disputes) or Chapter VII (action with respect to threats to the peace, breaches of the peace, and acts of aggression). In the first case, the Council could, for example, on the basis of Article 34 of the Charter, "investigate any dispute or situation which might lead to international friction or give rise to a dispute, in order to determine whether the continuance of the dispute or situation is likely to endanger the maintenance of international peace and security". It could also, on the basis of Article 37, "recommend such terms of settlement as it may consider appropriate". In the second case, if the Council considers that the situation is serious enough to constitute a "threat to the peace" within the meaning of Article 39, it may resort to the provisional measures provided for in Article 40 of the Charter, or to non-military (Article 41) or even military (Article 42) measures of coercion. Never, however, until now, has the UN Security Council had to adopt such measures in the case of a cyber-attack.

Another option, perhaps more accessible to the States concerned, would be to approach regional cooperation mechanisms. One example is the European Union Agency for Network and Information Security (ENISA),(97) which is responsible for ensuring a high level of network and information security in collaboration with national authorities and European institutions, and which is working to develop a culture of information network security throughout the Union.

Another example is the Asia Pacific Computer Emergency Response Team (APCERT) which, among other things, has the task of enhancing Asia Pacific regional and international cooperation on information security, jointly developing

(95) See for example article 2 §3 of the Charter of the United Nations ("All Members shall settle their international disputes by peaceful means") and Chapter VI of the Charter entitled "pacific settlement of disputes".

(96) *GGE 2015*, *supra* note 2, §23.

(97) See ENISA's website (www.enisa.europa.eu/).

measures to deal with large-scale or regional network security incidents and assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency responses.(98) A final example is NATO's Rapid Reaction Team (RRT), developed within the NATO Computer Incident Response Capability (NCIRC), and composed of experts in cyber defense. This force is responsible for "assisting member states which ask for help in the event on an attack of national significance".(99) As it has been pointed out, "With the RRTs, NATO will be able to offer, upon request, professional and well-organized assistance to its members and partners, but principally to those countries which do not yet have the resources to set up cyber defense capabilities of this kind".(100)

B) Acts of retorsion

If cooperation and negotiation do not produce the desired effects, the victim State may also resort to acts of retorsion. Such an act is:

> "An unfriendly measure, lawful in itself, taken by a State in response to the unfriendly conduct of another subject of international law, regardless of whether or not that conduct is lawful".(101)

As explained above, there are no conditions laid down by international law for the initiation of acts of retorsion: the adopting State does not need to demonstrate that an "internationally wrongful act" has been committed by another State, nor does it have to "attribute" the cyber-attack to another State—even if, on a political level, establishing the origin of the attack would be very useful to legitimize the act of retorsion before the international community.

The international legal order does not impose any conditions for the exercise of acts of retorsion; other, of course, than their conformity with international law. More specifically, from a legal point of view, there is no need to respect any principle of "necessity" or "proportionality". Therefore, the act of retorsion could be of a magnitude great enough to send a strong message to another State which would have to either cease the cyber-attack itself, if it is conducted by its own agents, or take the necessary measures in the context of its due diligence obligation, if the attack is launched by private actors within its territory or under its jurisdiction. Such acts of retorsion could, of course, be poorly perceived by the State concerned, and inappropriate or even counterproductive in certain situations. These, however, are political and strategic considerations: on a legal level, whatever the extent or the "disproportionate" nature (compared to the effects of a

(98) See APCERT's website (www.apcert.org/).

(99) See "NATO Rapid Reaction Team to fight cyber attack", 13 March 2012 (www.nato.int/cps/en/natohq/news_85161.htm?selectedLocale=en).

(100) *Ibid.*.

(101) J. Salmon (ed.), *Dictionnaire de droit international public*, Bruxelles, Bruyant/AUF, 2001 p. 1007. Our translation. The definition provided by the UN International Law Commission is very similar. In its view, a retaliatory measure is an "'unfriendly' conduct which is not inconsistent with any international obligation of the State engaging in it even though it may be a response to an internationally wrongful act". *YILC 2001*, *supra* note 19, p. 128.

cyber-attack) of the act of retorsion may be, there is no violation of international law. From a strategic point of view, it could be considered that States may be tempted to undertake powerful acts of retorsion, as it could help "appease" the shocked public opinion in the aftermath of a cyber-attack, by showing that the injured State reacts "strongly". Arguably, such strong acts could, perhaps, also be more effective in obtaining the cooperation of the State concerned—avoiding resort to more "serious" measures such as the countermeasures analyzed *infra*. That being said, diplomatic practice shows that if the receiving State considers the measures to be unfriendly and inappropriate, it could respond in its respective turn by retorsion measures on the basis of the principle of reciprocity.

Several examples of acts of retorsion can be given.

First of all, there are **diplomatic measures**, which may range from the simple convocation of an Ambassador to the complete disruption of diplomatic relations through the temporary recall of the Head of the diplomatic mission or other diplomats; the reduction of diplomatic representation; or the declaration, on behalf of the receiving State, of certain members of the diplomatic staff of the sending State as "*personae non gratae*", accompanied by a summon to leave the country rapidly.

Another measure could be the so-called "**naming and shaming**". The publication, by the highest authorities of the victim State, of a report convincingly establishing that the cyber-attack was committed by agents of another State or by private actors located on the latter's territory or acting under its control, could not only send a strong message about the determination of the victim State, but also legitimize upcoming, more significant reactions.

A third set of measures could relate to the suspension of benefits granted without legal obligation to the other State (e.g. economic or military aid); the suspension of investments in progress or already undertaken in the other State; the suspension of negotiations; the cancellation of official visits; the refusal to participate in political or cultural activities, etc.

A fourth round of acts of retorsion could be the adoption of embargoes against products from the other State, or some of its enterprises considered to be involved in the cyber-attack, or the adoption of sanctions against certain entities or individuals presumed to be involved in the cyber-attack. For such sanctions to be considered acts or retorsion, however, it should be ensured that no rule of international law, such as any arising from commitments undertaken in the context of the international protection of human rights, is violated.

Generally, any measure that does not cross the "threshold of wrongfulness" in international law can be adopted as part of a strategy of recourse to acts of retorsion. This also concerns, of course, certain "cyber-operations" against another State

which would be considered as lawful[102] according to the current criteria of international law.

C) Exceptional mechanisms of self-protection (state of necessity, distress, force majeure*)*

International law recognizes three exceptional mechanisms of self-protection that allow a State to respond to certain situations, if necessary, by measures that under other circumstances would be considered to be unlawful. The common feature of these three mechanisms is that none of them presupposes the existence of a violation of international law on behalf of the State against whose rights they are directed. They also provide the States which invoke them "a shield against an otherwise well-founded claim for the breach of an international obligation".[103]

The United Nations International Law Commission has classified these three mechanisms as "circumstances precluding wrongfulness". According to the Commission's logic, the "circumstances" in question constitute justifying facts which abolish the illegality of an act, or, to put it more simply, exceptionally erase the illegality of an act.[104]

However, it is advisable not to try to generalize the invocation of these mechanisms in reaction to a cyber-attack. The fact that these mechanisms are admitted only as "exceptional" has been emphasized both by the UN International Law Commission[105] and the International Court of Justice.[106] In fact, international courts rarely accept their invocation—so rarely in fact that some authors have gone so far as to question the very existence of some of them.[107] While we consider that these three mechanisms are accepted by positive international law, we believe that for various reasons, especially due to the very strict conditions under which they apply, these mechanisms can only be accepted on an exceptional basis—thus diminishing their role in the palette of acceptable reactions to cyber-attacks.

---

(102) Regarding the "threshold of wrongfulness" see also *infra* Part II (2A).

(103) According to the terms of the ILC in the Draft Articles and Commentary 2001, *supra* note 19, p. 71.

(104) In several studies, however, we have tried to demonstrate that the two most important "circumstances" in question (necessity and distress) should rather be seen as "circumstances excluding or mitigating the responsibility" of States, and not precluding the wrongfulness of their acts. In other words, violations of international law committed under the excuse of necessity or distress remain unlawful acts, but the responsibility of the perpetrators may be, depending on the circumstances, either excluded or, at least, mitigated. See, among other studies: T. CHRISTAKIS, "Les 'circonstances excluant l'illicéité' : une illusion optique ?", in *Droit du pouvoir, pouvoir du droit, Mélanges offerts à Jean Salmon*, Bruxelles, Bruylant, 2007, p. 201-248 ; T. CHRISTAKIS, "'Nécessité n'a pas de Loi' ? Rapport introductif sur la nécessité en droit international" *in* T. CHRISTAKIS and K. BANNELIER (eds), *La nécessité en droit international*, Colloque de la Société française pour le droit international, Pedone, Paris, 2007, p. 9-62 ; T. CHRISTAKIS, "Quel remède à l'éclatement de la jurisprudence CIRDI sur les investissements en Argentine ? La décision du Comité ad hoc dans l'affaire CMS c. Argentine", *Revue Générale de Droit International Public*, No. 4, 2007, 879-896.

(105) *YILC 2001*, *supra* note 19, p. 80 §6 for distress and p. 80 (§§1 et 2) and 83 (§14) for state of necessity.

(106) *Gabcikovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, ICJ Reports 1997, §51.

(107) See particularly S. HEATHCOTE, *State of Necessity and International Law*, Thesis No. 772, University of Geneva, Geneva, 2005 and S. HEATHCOTE, "Est-ce que l'État de nécessité est un principe de droit international coutumier ?", *RBDI*, No. 1, 2007, 53-90.

a) Force majeure

According to article 23 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts":

> "1. The wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the act is due to *force majeure*, that is the occurrence of an irresistible force or of an unforeseen event, beyond the control of the State, making it materially impossible in the circumstances to perform the obligation.
>
> 2. Paragraph 1 does not apply if: (a) the situation of *force majeure* is due, either alone or in combination with other factors, to the conduct of the State invoking it; or (b) the State has assumed the risk of that situation occurring".

Therefore, *force majeure* refers to a situation in which the State is **obliged to act** in a manner which is not in conformity with an international obligation imposed on it. It differs from distress and necessity in the sense that the conduct of the State "is involuntary or at least involves no element of free choice".(108) As explained by the Commission, the material impossibility of complying with the obligation giving rise to a situation of *force majeure* "may be due to a natural or physical event (e.g. stress of weather which may divert State aircraft into the territory of another State, earthquakes, floods or drought) or to human intervention (e.g. loss of control over a portion of the State's territory as a result of an insurrection or devastation of an area by military operations carried out by a third State), or some combination of the two".(109) This exception is nevertheless regulated. In particular, it is required that "the situation must be irresistible, so that the State concerned has no real possibility of escaping its effects".(110) *Force majeure* does not, however, extend to the circumstances in which the performance of an obligation has been made difficult but is still possible. It is thus hard to imagine in what circumstances "*force majeure*" could justify a cyber-attack (or a reaction to it by a practice of hack-back).

b) Distress

According to article 24 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts":

> "1. The wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the author of the act in question has no other reasonable way, in a situation of distress, of saving the author's life or the lives of other persons entrusted to the author's care.
>
> 2. Paragraph 1 does not apply if: (a) the situation of distress is due, either alone or in combination with other factors, to the conduct of the State invoking it; or (b) the act in question is likely to create a comparable or greater peril".

(108) *YILC 2001, supra* note 19, p. 76 §1.
(109) *Ibid*., p. 76 §3.
(110) *Ibid*.

Distress, therefore, concerns a situation in which the agent of a State (an individual whose actions are attributable to the State) finds himself in a perilous situation, either personally or through persons he is in charge of protecting, and has, reasonably, no other means of saving the lives in question than through violating international law. Unlike a situation of *force majeure*, the agent of the State does not act unintentionally, but rather chooses to violate international law in order to save lives, even if this choice is almost imperative by the situation of peril. In practice, distress has been invoked primarily to justify unauthorized incursions into the aerial or maritime territory of other States by ships or aircraft in distress, as a result of stress of weather, mechanical failures or navigational problems.(111) Even if one could imagine a situation of an unauthorized intrusion into the cyberspace of another State as the only way to save lives, such a hypothesis should remain exceptional in the context of a response to cyber-attacks.

c) The state of necessity

According to article 25 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts":

> "1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act: (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.
>
> 2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if: (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the State has contributed to the situation of necessity".

Unlike *force majeure*, the state of necessity does not concern involuntary or constrained behavior. Unlike distress, necessity lies not in a peril for the lives of persons whom an agent of the State has the burden of protecting, but in a grave peril threatening the essential interests of the State.

This circumstance is probably among the three most likely to be invoked by States that react to cyber-attacks, or even initiate them, by claiming that there is "a grave and imminent peril" for their "essential interests". In fact, the *Tallinn Manual 2.0* has devoted extensive developments to this topic. It should be noted, however, that there is a great difference between the UN International Law Commission and the *Tallinn Manual*. In fact, the Commission had formulated article 25 in a negative way ("Necessity may not be invoked by a State […] unless the act […]"), in order to "emphasize the exceptional nature of necessity and concerns about its possible abuse".(112) The *Tallinn Manual* seems to want to distinguish itself from this cautious phrasing, by formulating its own rule ("rule 26")

(111) See *ibid*. §§3-6, the examples provided by the ILC.

(112) According to the terms by ICL itself in *ibid.*, p. 83§14.

on necessity in a positive way: "A State may act pursuant to the plea of necessity […]".(113) This is surprising, since the Commission had emphasized that the state of necessity, given a series of "special features", "will only rarely be available to excuse non-performance of an obligation and that it is subject to strict limitations to safeguard against possible abuse".(114) The examples provided for by the Commission, as well as the very limited acceptance of this mechanism by international jurisdictions,(115) appear to confirm the validity of the cautious approach adopted by the Commission and to warn against any attempt to rely heavily on the state of necessity as a general mechanism of justification for cyber-attacks.

It would take too long to enter into a detailed analysis of the very restrictive conditions of invoking a state of necessity in international law(116) and their relevance in the domain of reaction to cyber-attacks. However, the main conditions are:

• **The existence of a grave and imminent peril.** A state of necessity may be invoked only to protect an essential interest of the State against a grave and imminent peril. It goes without saying that a State cannot agitate ghosts to justify a breach of international law and that there can be no state of necessity without a particularly important, immediate and duly proven "peril" at the relevant time: *vani timoris justa excusatio non est*.(117) The Commission also considerably limited the margin of appreciation left to States by stressing that "the danger must be objectively established".(118)

• **This peril must adversely affect "an essential interest" of the State.** This interest may, thus, be linked to the protection of cyberspace and vital infrastructure or other areas of State activity.

• **The exclusivity of the means used.** The requirement that the incriminated act must constitute "the only means of protecting an essential interest against a grave and imminent peril" sets the bar too high. Consequently, state of necessity cannot be equated to *force majeure*: the State voluntarily chooses to violate the law to protect its own interests and, from this point of view, the condition of exclusivity of the means seeks to limit, as far as possible, any violations. Of course, this criterion has been criticized by some authors who emphasized that States will not be able to bypass it easily.(119) However, the Commission has not offered any

(113) Here is the entire text: "A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber or non-cyber in nature, to its essential interests when doing so is the sole means of protecting them", *Tallinn Manual 2.0*, *supra* note 12.

(114) *YILC 2001*, *supra* note 19, p. 80 §2.

(115) See, among others, the studies cited *supra*, notes 104 et 107.

(116) For this, see *ibid*.

(117) J. Salmon, "Faut-il codifier l'état de nécessité en droit international ?", *in* Jery Makarczyk, (éd.), *Études de droit international en l'honneur du Juge Manfred Lachs*, The Hague/Boston, M. Nijhoff, 1984, 251-254.

(118) Commentary of article 25 in *YILC 2001*, *supra* note 19, §15.

(119) According to J. Salmon, for example: "*Le caractère exclusif du moyen n'est pas très convaincant […] car de deux choses l'une : ou bien on doit épuiser sérieusement les moyens les plus onéreux d'écarter ce péril et alors peu de cas d'état de nécessité*

leniency in this matter, insisting in its commentary of article 25 that "The plea is excluded if there are other (otherwise lawful) means available, even if they may be more costly or less convenient".(120)

• **The quality of the injured right.** A state of necessity can never be invoked to justify an act which "seriously impair[s] an essential interest of the other State or States concerned, or of the international community as a whole". According to the Commission, "the interest relied on must outweigh all other considerations, not merely from the point of view of the acting State but on a reasonable assessment of the competing interests, whether these are individual or collective".(121) It is therefore a kind of control of proportionality between the two "essential interests" in question. This criterion establishes a strict hierarchy: the interest sacrificed must be inferior to the interest safeguarded.

• **"Clean hands".** The State committing the wrongful act "must not have contributed to the occurrence of the state of necessity".

• **The barrier of *jus cogens*.** A state of necessity can never justify a breach of an "obligation arising under a peremptory norm of general international law", as emphasized in article 26 of the Commission's Draft Articles. Thus, the state of necessity could not be invoked, for example, in order to commit an act of aggression against another State.

2. Reactions to violations of international law by another State

The reactions that we are going to study here are legally possible only if a State has violated international law in one way or another during the conduct of a cyber-attack. The existence of an "internationally wrongful act" is therefore indispensable in this case. Of course, there is no obligation of the victim State to resort to the reactions that will be analyzing here: it is upon a State's discretion to use the mechanisms analyzed above [II.1 and especially (A) and (B)], which are always available to it and which could be considered more appropriate by the victim State in some situations. It must also be emphasized that, according to a founding rule of international law, "every internationally wrongful act of the State entails its international responsibility"(122). This means that a State injured by such an act, may enforce the mechanisms for international responsibility by resorting where possible, for example, to an arbitral tribunal or the International Court of Justice and request that the State responsible terminate the unlawful act, refrain from repeating it and offer full reparation for the injury caused by its internationally

répondront aux conditions requises ; ou bien – ce qui est le plus à craindre – celui qui invoque le péril imminent tirera argument de l'imminence même du péril pour ne pas épuiser d'autres moyens" (*supra* note 117, p. 263).

(120) *YILC 2001*, *supra* note 19, p. 88 §15.

(121) *Ibid*, p. 83 §17.

(122) Rule codified by article 1 of the Commission's work on responsibility. *YILC 2001*, *supra* note 19.

wrongful act. Setting aside the question regarding the international responsibility of the State having launched a cyber-attack, we shall focus on the two reactions at the disposal of States as a response to the unlawfulness of a cyber-attack, namely non-forcible countermeasures (A) and self-defense in case of armed aggression (B).

A) Peaceful countermeasures

Countermeasures can be defined as:

> "Measures that would otherwise be contrary to the international obligations of an injured State *vis-à-vis* the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation".(123)

Countermeasures result from the use of "private justice" processes that are largely inconceivable in domestic legal systems that are based on the principle of "no one can do justice on oneself" and where the State is, by virtue of its sovereignty, the guarantor of the enforcement of the law.(124) In the international legal order, countermeasures "are a feature of a decentralized system by which injured States may seek to vindicate their rights".(125) In the absence of an authority superior to States, capable of imposing a solution, in the absence also of an impartial third party having always and automatically jurisdiction over disputes between States, the latter are authorized to "do justice on themselves", by resorting to acts which are in principle unlawful. It is, in a way, the tribute that the vice pays to virtue: injured States may resort to violations of international law against States responsible for such violations, but only in order to oblige the latter to comply with their international obligations, by ceasing the violation and remedying the consequences thereof. In such a case, the wrongfulness of the countermeasures exercised by the injured State is "erased", "excluded", because it is a justified response to a wrongful act starting from another State, and its function is to bring that State back into the path of legality. Contrary to the state of necessity or distress which should, in our view, be regarded as "excluding or mitigating the responsibility" of States(126), countermeasures are clearly circumstances "precluding wrongfulness". International jurisprudence seems to confirm this view of countermeasures as "justifying" an unlawful act.(127) This is also established by the fact that, to the best of our knowledge, there has never been any consideration in the practice of States and

(123) *Ibid*, p. 128 §1.

(124) However, domestic legal systems envisage certain situations where the victim of a violation of the law may resort to certain mechanisms of self-protection without recourse to the courts: this is particularly true of the exception of non-performance (*exceptio non adimpleti contractus*) in civil law or self-defense in criminal law. But these mechanisms, which have their equivalents in international law, differ greatly from the widespread authorization of countermeasures in international law.

(125) *YILC 2001*, *supra* note 19, p. 128 §1.

(126) *Supra* note 104.

(127) In the Cysne Case, for example, the arbitral tribunal highlighted that "An act contrary to international law may be justified, as a reprisal, if a similar act had provided the reason", Arbitral award of 30 June 1930, *RSA*, Vol. II, p. 1056. See also p. 1057.

international jurisdictions, of the existence of any obligation to compensate for losses incurred as a result of the adoption of justified countermeasures.(128)

Thus, in the event of a cyber-attack constituting an "internationally wrongful act", the victim State has the right if it so wishes, and under certain conditions, to react by resorting to measures which are normally violations of international law, against the attacking State. These countermeasures do not have to be of the same nature as the original wrongful act. As a result, the State may conduct in the course of countermeasures a hack-back or "cyber-attack in return" action, but it may also adopt any other peaceful measure contrary to law: suspension of the execution of an international agreement; economic sanctions contrary to international rules; or other violations of its obligations undertaken towards the attacking State. Should these countermeasures comply with the conditions of triggering (a) and exercise (b) that will be analysed, they will be considered justified, and will not entail the responsibility of their author.

a) Conditions of triggering: the existence of an internationally wrongful act of a State

Countermeasures are permitted only against the State that is responsible for an internationally wrongful act, and must be directed exclusively against it. Article 2 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts" clarifies that:

> "There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State".

Thus, in principle, the occurrence of pecuniary damage is not necessarily required in order to lawfully resort to countermeasures; mere moral or legal damage may suffice(129). On the other hand, in order for an "internationally wrongful act" to exist, two cumulative conditions must be met: the breach of an international obligation, and the attribution of said breach to a State.

I. VIOLATION OF AN INTERNATIONAL OBLIGATION

The breach of an international obligation is a *conditio sine qua non* for the adoption of countermeasures which, by definition, constitute the response to an original wrongful act of another State and are a means of enforcement of that State's international obligations. Depending on the nature and effects of a cyber-attack, several rules of international law could have been violated, ranging from

(128) Completely different is the question whether a legal system could provide for mechanisms for the compensation of private individuals, whether natural or legal, who had suffered damage as a result of countermeasures against States.

(129) The nature of the "harm" suffered by the "injured State" thus depens on the requirements of the primary rule violated by the responsible State. As stressed by the Commission: "It is sometimes said that international responsibility is not engaged by conduct of a State in disregard of its obligations unless some further element exists, in particular, 'damage' to another State. But whether such elements are required depends on the content of the primary obligation, and there is no general rule in this respect". *YILC 2001*, *supra* note 19, p. 36, §9.

breaches of *jus contra bellum* or *jus in bello* to less serious abuse of the sovereignty of a State, through the violation of principles such as that of non-intervention or the right of peoples to self-determination.(130) Due to the limited space provided here, it is impossible to enter into a detailed analysis of all scenarios and standards that could be violated by a cyber-attack. We shall therefore limit ourselves to three observations.

First, an examination of the texts and theory of international law reveals the uncertainties in the distinction between the principle of non-intervention and the principle of non-interference in the internal affairs of a country. It could be considered that the former refers to the protection of the territory of the State, of its *dominium*, and that its violation would therefore involve the carrying out of material operations in foreign territory; while the latter would refer to interference, without the authorization of the State, in the sphere of the exercise of its national sovereign powers and would, therefore, affect the *imperium* of the State.(131) Yet, this distinction often becomes blunted in practice. Thus, for example, the famous *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the UN*, adopted by the General Assembly of the United Nations in 1970 states that:

> "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law"(132)

The International Court of Justice emphasized in its 1986 Judgment in the *Case of Military Activities in Nicaragua* that:

> "A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State"(133).

---

(130) Serious interference in the electoral process of a State, resulting in a distorted result could, for example, be considered a violation of this principle. It should be recalled that according to the codification of this principle by the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the UN, adopted by the General Assembly of the United Nations in 1970: "By virtue of the principle of equal rights and self-determination of peoples enshrined in the Charter of the United Nations, all peoples have the right freely to determine, without external interference, their political status […]". A/RES 2625 (XXV) of 24 October 1970.

(131) See, in this regard, Jean Combacau and Serge Sur, *Droit international public*, Paris, Montchrestien, 5th edition, 2001, p. 260 and Pierre-Marie Dupuy and Yann Kerbrat, *Droit international public*, Paris, Dalloz, 12th edition, 2014, p. 130.

(132) According to the text of "The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter" of the A/RES 2625 (XXV) of 24 October 1970.

(133) *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. USA)*, Judgment of 27 June 1986, *ICJ Reports 1986*, p. 108, §205.

More detailed studies should probably be carried out, so as to better define the distinction between the two principles and their content and to identify when they could be considered to have been violated in the case of a cyber-attack. Thus, for example, there is no doubt that a cyber-attack that manipulates electoral results in a country could constitute a violation of the principle of non-interference.(134) It is more complicated, however, to define from what point onwards, would the mere hacking of electronic messages from certain political figures and their distribution in the media or their publication on the Internet, be considered as a violation of the same principle.(135)

Secondly, it is interesting to note the position of the *Tallinn Manual 2.0* which tried to determine under what circumstances a cyber-attack could constitute a violation of the sovereignty of a State. According to the experts invited to participate in this book:

> "The precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law. […] First, most of the Experts agreed that cyber operations constitute a violation of sovereignty in the event they result in physical damage or injury […]. Second, the Experts agreed that, in addition to physical damage, the remote causation of loss of functionality of cyber infrastructure located in another State sometimes constitutes a violation of sovereignty, although no consensus could be achieved as to the precise threshold at which this is so […].There was full agreement that a cyber operation necessitating repair or replacement of physical components of cyber infrastructure amounts to a violation because such consequences are akin to physical damage or injury. […] Third, no consensus could be achieved as to whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty".(136)

Tallinn Manual 2.0 considered also that "Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so".(137) On the other hand, other authors have considered that cyber-espionage constitutes a violation of the principle of non-interference within the internal affairs of States.(138)

Our third and final observation concerns the breach of the due diligence obligation, which is particularly relevant to the issue arising from cyber-attacks being carried out by private actors. As we have seen in the first part, by virtue of their sovereignty, States have an obligation to not allow knowingly their territory to be used for acts contrary to the rights of other States. If a State is aware of (or should have been aware of) a cyber-attack being initiated by private actors from

(134) See in this regard the address by Brian Egan (US State Department Legal Adviser), "International Law and Stability in Cyberspace", 10 November 2016 (www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf).

(135) In the aforementioned address, B. Egan concluded that "For increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States' activities in cyberspace".

(136) *Tallinn Manual 2.0*, *supra* note 12, analysis under "Rule 4 – Violation of sovereignty", §§ 10-14.

(137) *Ibid.*, Rule 32.

(138) See Russell Buchan, "Cyber espionage and international law" *in* Nicholas Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2015, 168-189.

its territory, and still did nothing to prevent and cease it, then it could be violating its duty of **due diligence**, thus, allowing the injured State to undertake countermeasures, including hack-back measures, against it and against the private actors operating on its territory, until the responsible State adopts the necessary measures to end the cyber-attack.

II. Attributable to a State

In order for a State to adopt countermeasures, the violation of international law by action (e.g. cyber-attack) or omission (e.g. breach of due diligence), must be attributable to the State against which the countermeasures are adopted. Therefore, attribution appears to be a fundamental condition for the adoption of countermeasures that are justified on the basis of international law. This brings us back to three observations.

The first concerns the **mechanisms of attribution**. It is necessary to distinguish among the the identification of the attackers as a technical operation linked to forensics ("cyber forensics"), and the attribution as a legal operation, despite the fact that the two of them are closely linked. In fact, international law provides for very precise mechanisms, which allow for the conduct of private actors to be attributed, under certain strict conditions, to States. These mechanisms are discussed below in Part III (3C).

The second observation concerns the **difficulties in the subject of attribution** from the standpoint of cyber forensics. Until recently, the attribution of attacks in cyberspace was considered particularly difficult. Despite the progress made and the efforts of some to present the attribution as a problem now solved, daunting difficulties remain. These difficulties exist due to a multitude of factors including, in particular, the lack of sufficient technical capacity (the problem of "forensic capacity") in several countries; the use of particularly sophisticated concealment techniques ("spoofing") by hackers in order to suggest that the attack was initiated by someone else; and, usually, the lack of sufficient time to establish with certainty the origin of the attack prior to adopting countermeasures that frequently take the form of hack-back. The complexity and limitations of attribution are often expressed by several States. Most recently, the US President himself spoke of the subject, noting that "unless you catch 'hackers' in the act, it is very hard to determine who was doing the hacking", or even that "hacking is a very hard thing to prove".(139)

In order to solve the problem of attribution at an international level, some States proposed the creation of an international centralized mechanism that would possess the necessary technical expertise to carry out reliable and independent

(139) See K. Eichensehr, "Trump's Dangerous Attribution Message on Russian Hacking—and How to Counter It", *Just Security*, 10 January 2017 (www.justsecurity.org/36161/trumps-dangerous-attribution-message-and-counter/).

operations of attribution. Nevertheless, other States opposed this idea, considering that the process of attribution includes not only technical and legal but also political considerations, which are part of the very DNA of the national security of States and essential governmental functions. Furthermore, these countries expressed doubts about the ability of an international body to effectively fulfill this role, since its mere creation could even be counterproductive. In conclusion, they considered that the attribution process, both from a technical and a legal point of view, should remain the prerogative of the States themselves.

The third and final remark concerns the question of the **necessary evidence regarding attribution** before the adoption of countermeasures. This is a crucial issue that has given rise to much exchange between States both within and outside the GGE, including in relation to certain accusations of cyber-attacks.

Positive international law, however, seems fairly clear in this respect: it does not require that States prove their allegations regarding the existence of a violation of international law by another State, prior to the adoption of countermeasures against it. This is an area where the old saying *nemo iudex in causa sua*(140) does not apply. In the absence of a centralized authority in the international legal system, automatically competent to assess the facts and to interpret the rules applicable to States, this power , including countermeasures,(141) is often left to States to decide and undertake.

As it was pointed out in 1978 by an Arbitral Tribunal regarding a flagship case concerning countermeasures between the United States and France:

> "Under the rules of present-day international law, and unless the contrary results from special obligations arising under particular treaties, notably from mechanisms created within the framework of international organisations, each State establishes for itself its legal situation vis-à-vis other States".(142)

The UN International Law Commission codified this rule in the "Articles on the Responsibility of States for Internationally Wrongful Acts". According to the Commission:

> "A State taking countermeasures acts at its peril, if its view of the question of wrongfulness turns out not to be well founded. A State which resorts to countermeasures based on its unilateral assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment".(143)

This means that a State does not have a legal obligation to produce evidence relating to the attribution of a cyber-attack before adopting countermeasures against the State accused of being the source of it. If, on the other hand, it is

(140) "No-one should be a judge in his own cause".

(141) *Cf.* Linos A. Sicilianos, *Les réactions décentralisées à l'illicite*, Paris, LGDJ, 1990, p. 31.

(142) *Case concerning the Air Service Agreement of 27 March 1946 between the United States of America and France*, Decision of 9 December 1978, *RIAA*, Vol. XVIII, §81.

(143) *YILC 2001*, *supra* note 19, p. 139 §3.

proved at a later stage that the injured State was mistaken in the matter of the attribution, the countermeasures adopted will no longer be justified on the basis of international law, and its international responsibility will be triggered, along with an obligation of reparation of the damage suffered by the State that was unjustly accused of being the perpetrator of the cyber-attack. In this regard, it must be added that, given the circumstances, the existence of a reasonable belief or the good faith of the State undertaking the countermeasures, would still not be sufficient to preclude its responsibility if, in spite of everything, it was wrong in the matter of attribution.

However, even if positive law in its present form does not seem to **require** States to prove their allegations of cyber-attacks, it could be in the best interest of States to submit certain evidence for political purposes and in order to defend the **legitimacy** of countermeasures in the eyes of the public opinion. The quantity and quality of such evidence should, moreover, be in accordance with the scale and severity of the countermeasures adopted. It is in this sense that the UN GGE stressed in its 2015 Report that "accusations of organizing and implementing wrongful acts brought against States should be substantiated".(144)

b) Conditions of exercise

While international law permits the use of countermeasures and "private justice" mechanisms under the aforementioned conditions, under no circumstances can such a practice be viewed as a return to the law of the jungle. The international legal order strictly governs the exercise of countermeasures by imposing a series of conditions which show that these "executive powers" available to States must be used in a prudent manner so as to avoid abuses and endangering international stability and security. Without going into the details of these conditions which are analyzed in other studies,(145) we will briefly highlight some of them for the purposes of our analysis.

• **Conditions relating to the objective of countermeasures.** The injured State may take countermeasures against the State responsible for the internationally wrongful act only in order to induce that State to comply with its obligations of cessation or reparation under international law. Countermeasures therefore do not have a punitive function and should not be considered as an expression of the law of retaliation ("*lex talionis*"). On the contrary, they are a means of enforcement the sole aim of which is to ensure respect for international law by the State which first violated it. Countermeasures must therefore be reversible(146) and cease "as

(144) *GGE 2015*, *supra* note 2, §28 (f).

(145) See, among others, the commentary of the ILC, 2001, *supra* note 19, pp. 75-76 and 128-139, and the studies by Denis ALLAND, Justice privée et ordre juridique international, Paris, Pedone, 1994, p. 503, and L.A. Sicilianos (*supra* note 141). See also *Tallinn Manual 2.0*, *supra* note 12, rules 20-25.

(146) According to article 49 §3 of the ILC draft articles and commentary, "Countermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question".

soon as the responsible State has complied with its obligations" under international law.(147)

• **Countermeasures must always be non-forcible.** The United Nations International Law Commission has codified the rule that countermeasures "shall not affect the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations".(148) This rule, which is also codified in other important international law instruments,(149) excludes the possibility of resorting to military countermeasures or of reacting by hack-back measures which could be considered as a violation of the prohibition of the threat or the use of force in international law.(150) This, of course, raises a question as to when can a specific action be considered to have crossed the "threshold" of the existence of a prohibited use of force. This is a great debate on *jus ad bellum* and the subject of long analyses in theory(151) which we cannot, unfortunately, analyze here. Nevertheless, a recent study by Marco Roscini proposes a broad definition of cyber operations which could be characterized as a violation of Article 2 §4 of the Charter on the prohibition of the threat and use of force. According to the author's conclusion: "Those worried that, by qualifying seriously disruptive cyber operations as a use of force, the risk of inter-State conflicts will increase should be reassured: indeed, a use of force, in itself, is not sufficient to entitle the victim State to react in self-defence, unless it is serious enough to amount to an 'armed attack'. Apart from the stigma attached to it, then, the only consequence of qualifying seriously disruptive cyber operations as a use of force is that they could not be undertaken in countermeasure, which certainly is a welcome result, considering the severe negative impact that they might have on the public order of today's digitally reliant societies".(152)

• **Countermeasures shall not violate certain other important obligations of States.** Under the rule codified by article 50 of the ILC "Articles on State responsibility", countermeasures shall not violate obligations relating to the protection of fundamental human rights, obligations of a humanitarian character prohibiting reprisals, and obligations arising from peremptory norms of general international law. This rule is particularly important because it prohibits the use of countermeasures that could affect, directly or indirectly, the obligations of States relating to human rights, which are not, in principle, subject to the principle of reciprocity under international law.

(147) *Ibid*., article 53.

(148) *Ibid*., article 50.

(149) See for example the 1970 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the UN, according to which "States have a duty to refrain from acts of reprisal involving the use of force", *op. cit.*

(150) The case of self-defense is naturally distinct and will be examined *infra*, Part II (2B).

(151) See especially Olivier CORTEN, *The Law Against War*, Hart, Oxford & Portland, 2010, 50-125.

(152) M. ROSCINI, "Cyber operations as a use of force", *in* N. TSAGOURIAS and R. BUCHAN (eds), *Research Handbook on International Law and Cyberspace*, *op. cit.*, p. 250.

• **Countermeasures must respect the principle of proportionality.** According to article 51 of the ILC Articles, "Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question". Unlike acts of retorsion where, as we have seen, the principle of proportionality is irrelevant, in the case of countermeasures it plays a fundamental role. The general idea is that the adoption of countermeasures, which are authorized under the motive of "correcting" an imbalance created by the original wrongful act of another State and for the sole purpose to push the latter back to the "path of international legality", must not create a new imbalance or lead to unfair results. Compliance with the principle of proportionality must be assessed on a case-by-case basis, bearing into consideration "not only the purely 'quantitative' element of the injury suffered, but also 'qualitative' factors such as the importance of the interest protected by the rule infringed and the seriousness of the breach".(153) On the other hand, the principle of proportionality does not require the injured State to reply "in kind" by adopting countermeasures in the same field as the original measures. On the contrary, States have a wide discretion in this respect for as long as their reply does not prove to be excessive and out of proportion with the act that motivated it.

• **Procedural conditions ("summons", notification, judicial proceedings pending).** International law also imposes a series of procedural requirements codified by article 52 of the ILC Articles. Before taking countermeasures, the injured State must, first, request of the responsible State to fulfill its obligations under international law and, then, to notify it of any decision to take countermeasures and to offer to negotiate. Urgent countermeasures may be exceptionally taken by the injured State if they are necessary to safeguard its rights. However, in accordance with the judicial mechanisms for the settlement of disputes, countermeasures cannot be taken and if they have been already taken they must be suspended without undue delay, if the dispute is pending before a court or tribunal whose judgment will be binding upon the Parties. In other words, where the "decentralized" character of the international system is shaded by the existence of a compulsory and impartial mechanism of dispute settlement through due process of law, the unilateral logic of countermeasures has no longer any justification or a *raison d'être*.

B) Self-defense in case of armed attack

Unlike countermeasures which, as we have seen, cannot involve the use of armed force, self-defense gives States the possibility of resorting to force in order to respond to an armed attack against them. The prospect of invoking self-defense in response to a cyber-attack has largely mobilized international scholarship and several studies have been published in this regard to examine the issue from the

(153) *YILC 2001*, *supra* note 19, p. 135 §6.

standpoint of *jus ad bellum* and *jus in bello*(154). However, it is clear that for the time being, the debate on these issues mainly has a theoretical dimension: never has a State officially accused, as far as we know, another State of having carried out an "armed attack" using cyber means; never has a State referred such a matter to the Security Council; and never has a State invoked Article 51 of the Charter in order to respond to a cyber-attack of which it considered itself to be the victim.

The debate, therefore, is largely forward-looking in nature and there may be a sharp contrast between the great academic interest for *jus ad bellum* and *jus in bello* in the cyber domain, and the practice of States, which shows that the reactions to cyber-attacks are almost exclusively linked to the "Law of Peace" and the categories we have examined in the rest of this study. However, given the "dire predictions" of many that cyber space could rapidly become a place of armed confrontation between States and, thus, give rise to "cyber Pearl Harbor" situations,(155) one can only understand the anticipation of the academic community. This also explains why several States or international organizations(156) have addressed these issues by developing national cyber defense strategies or international policies to contemplate on different possible hypotheses.

Taking into account these considerations as well as the amplitude of published studies on the topic of "cyber warfare", we shall limit ourselves here to a few brief observations, by examining the triggering conditions (a) and the conditions of exercise (b) of self-defense in response to a cyber-attack.

a) Trigger condition: the existence of an armed attack

For a State to invoke self-defense in order to respond by military (or assimilated) means to a cyber-attack, it must be the victim of an "armed attack". According to the terms of Article 51 of the Charter of the United Nations:

> "Nothing 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, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security".

(154) See particularly: M. Roscini, *Cyber Operations and the Use of Force in International Law*, New York, Oxford University Press, 2014; M. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York, Cambridge University Press, 2013; and several chapters *in* N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2015.

(155) According to the famous phrase of the former US Secretary of Defense, Leon Panetta. See Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack", *N.Y. Times*, 12 October 2012.

(156) See, for example, the NATO Wales Summit Declaration adopted in September 2014 where NATO member States adopted their "Enhanced Cyber Defence Policy", affirmed "therefore that cyber defense is part of NATO's core task of collective defence" and emphasized that "a decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis" (§72) (www.nato.int/cps/en/natohq/official_texts_112964.htm).

It should be noted, in this regard, that the Charter of the United Nations presents self-defense as a "natural right". Self-defense should be understood, nonetheless, as an **exception** to the general principle of the prohibition of the use of force.(157) The legal consequence is that it depends on the State invoking this exceptional "right", to prove the existence of the conditions necessary for its existence. The burden of proof therefore lies with those who invoke a situation of legitimate defense.

In order for a State to be able to invoke self-defense, it must be the victim of **"armed" attack** which, of course, can take various forms. Beyond classical cases, such as the invasion or bombardment of a State's territory, there are other possibilities, such as the attack by the navy or the air force of a State, the sending of paramilitary forces, mercenaries, etc. It should be emphasized that the nature of the weapons used does not matter as much: attack can be exercised by conventional weapons, weapons of mass destruction or even elements transformed to weapons because of their devastating effects, such as the use of the forces of nature (diversion of a river, induced eruption of a volcano, etc.) for hostile purposes. From this point of view, there is no doubt that armed attack can be exercised by using digital means, provided that the effects of such a "cyber-attack" are similar to those resulting from the use of conventional weapons.

This brings us to another criterion which is that of **gravity**: in order to qualify as "attack", and thus allow an action in self-defense, an attack must have a certain level of gravity. Thererfore, a limited use of force such as a border incident (a military patrol which draws on another patrol), constitutes a violation of Article 2 §4 of the Charter, which entails the international responsibility of its perpetrator, but does not necessarily constitute an "armed attack" and, consequently, does not allow for the other State to invoke a right of self-defense. The International Court of Justice has had the occasion to emphasize this point on several occasions, for example in the *Case of Military Activities in Nicaragua* (1986), where it was pointed out that it is "necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms". The idea behind this criterion is to avoid the risk of escalation that would take place should States undertake military actions in self-defense too easily so as to respond to minor incidents. In conclusion, a cyber-attack with limited effects on the territory of the victim State could constitute a violation of international law without, however, being considered as an "armed attack" giving the victim State the opportunity to invoke self-defense.

Another fundamental question relates to **who can commit** an attack. Traditionally, it has been accepted in international law that only a State can commit an attack against another **State**. However, since the 9/11 attacks of 2001,

(157) For an analysis see T. Christakis and K. Bannelier, "La légitime défense en tant que 'circonstance excluant l'illicéité'" in Rahim Kherad (ed.), *Légitimes défenses*, Paris, LGDJ, 2007, 233-256.

several authors have argued that sub-State groups may also commit an "armed attack" within the meaning of article 51 and that this notion should cover any person likely to launch an attack of a certain gravity. According to this theory, self-defense could be exercised not only against other States, but also against sub-State groups such as terrorist groups, including Al-Qaeda or ISIS. The acceptance of such a theory does not come without problems. The major problem, of course, is the fact that these groups do not possess their own territorial base and are located within the territories of States which are sometimes unable of removing them from it. Yet, any military action against these groups without the consent of the State within whose territory they are located, could be regarded as a violation of the sovereignty of that State or even as an armed attack. This debate takes on a new dimension in the context of a reaction to cyber-attacks possibly launched by an impressive multitude of private actors. Could we accept, for example, that the fact that non-State actors have launched an important cyber-attack against the territory of State A from within the territory of State B, gives State A the right to undertake military action on the territory of State B as an exercise of its right to "self-defense"? What could be the possibilities of State B to react in such a case against State A, especially if it ignored the presence of terrorists on its territory, or did not have the means to neutralize them? It is for this reason among others, that the International Court of Justice has taken a cautious approach in refusing the application of self-defense outside inter-State relations. Consequently, in its Advisory Opinion of 9 July 2004 on the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, the Court emphasized that: "Article 51 of the Charter recognizes […] the existence of an inherent right of self-defence in the case of armed attack by one State against another State". Despite this position of the Court and the strong support of a large number of States, including the Non-Aligned Movement of 117 States which has repeatedly emphasized in recent years that Article 51 of the Charter should "not be re-written or re-interpreted", the debate continues to rage in international law. Nevertheless, all agree that positive law accepts the hypothesis of an "indirect attack" in cases where an armed attack by a non-State group is considered as an "attack" committed indirectly by a State, thus authorizing the victim State to invoke its right to self-defense in order to trigger a military response against the State which committed the indirect "attack".(158)

Last but not least, another legal debate has been raging over the past few years: it concerns the question of whether a State could, despite the clear requirement of an "armed attack" in Article 51 of the UN Charter, invoke a right to self-defense without the actual presence of such an attack. More specifically, some authors consider that international law recognizes now the theory of "pre-emptive self-defense", according to which a State may respond to an imminent threat of attack; while others, have gone so far as to support the "preventive self-defense",

(158) In order to identify in which cases the action of a non-State actor could be attributed to a State, see, among others, *infra* Part III (3C).

according to which a State could react to what it considers to be a distant, but not yet materialized, threat. The Tallinn Manual 1 has thus suggested that the theory of "preemptive self-defense" in cyber-attacks could already be part of international law.(159) However, an in-depth analysis of the current state of positive law seems to show that international law does not accept either "preventive self-defense" or "pre-emptive self-defense".(160) Caution is therefore needed in an area where the risks of abuse and destabilization of the international system are very important.

b) Conditions of exercise

Respect for the principles of necessity and proportionality. As emphasized by the International Court of Justice in its Advisory Opinion of 8 July 1996 in the case concerning the *Legality of the Threat or Use of Nuclear Weapons*: "[t]he submission of the exercise of the right of self-defense to the conditions of necessity and proportionality is a rule of customary international law". Traditionally, the requirements of "necessity" and "proportionality" regarding an action taken in self-defense are but the two sides of the same coin. Indeed, military action in self-defense can only be justified if it is a measure designed to put an end to armed attack. The use of force in self-defense must be "necessary and proportional" to the extent that the State cannot attain this result (end the attack) by a different behavior that would not involve the use of armed force, or through a more restricted use of that force. It goes without saying that this criterion of proportionality raises very difficult and "technical" questions which we cannot analyze here.(161) But the fundamental point is that, as in the case of countermeasures, self-defense must aim only at repelling the attack without causing a new imbalance.

Subordination to the action of the Security Council. According to Article 51 of the Charter, States have a procedural obligation to inform the Council of any military actions undertaken in self-defense. Failure to do so does not result to the wrongfulness of the action *per se* (as an attack remains an attack), but it constitutes a violation of the Charter and could bear other, burdensome consequences to the perpetrator. Accordingly, the International Court of Justice has repeatedly held that by not informing the Security Council of its military actions within the territory of another State, the acting State may be perceived as not considering itself that it is acting in self-defense. At the same time, article 51 states that self-defense is a right "subordinate" to the action of the Security Council. Here we find the "multilateralist" vision of the drafters of the Charter who wanted to "ban" the unilateral use of force in international relations as much

(159) See *Tallinn Manual 1*, *supra* note 12, "Rule 15: The right to use force in self-defence arises if a cyber-armed attack occurs or is imminent".

(160) See especially O. Corten, *The Law Against War*, *op. cit.*, 406-442 and T. Christakis, "Existe-t-il un droit de légitime défense en cas de simple 'menace'? Une réponse au 'groupe de personnalités de haut niveau' de l'ONU" in SFDI, *Les métamorphoses de la sécurité collective*, Paris, Pedone, 2005, 197-222.

(161) See O. Corten, *The Law Against War*, *op. cit.*, 470-494.

as they could: unilateral action in self-defense is considered "necessary" (and thus justified) only in the absence of appropriate collective security measures. As we have said in the introduction, to our knowledge, a State has never referred a situation of "armed cyber-attack" to the UN Security Council. This hypothesis remains thus theoretical for the moment.

PART III. Hack-back, "active cyber defense" and the need for an orderly international system

Introduction: The important role of private actors in the event of cyber-attack

A) Passive defense

B) Attribution of cyber-attacks

C) Hack-back and "active cyber defense"

1. Arguments in favor and against hack-back

A) Interest and advantages of hack-back

B) Disadvantages and risks

2. The "wild" hack-back: can private actors unilaterally trigger cyber-offensive measures?

A) The absence of a "hack-back right" in international law

B) A Violation of international law?

C) Hack-back as a violation of domestic law

3. The "regulated" hack-back: can States rely on private actors to conduct counter-attacks?

A) Cooperation between public and private actors to respond to cyber-attacks?

B) The case of Private Military and Security Companies (PMSCs)

C) Can the international responsibility of States be triggered by hack-back measures initiated by private actors?

III. Hack-back, "active cyber defense" and the need for an orderly international system

Introduction: The important role of private actors in the event of cyber-attack

Private sector companies specializing in cyber security play an increasingly important role in preventing and responding to cyber-attacks, at three levels at least: passive defense (A), attribution of cyber-attacks (B), hack-back and other "active cyber defense" activities (C).

A) Passive Defense

Firstly, they intervene in a passive defense approach,(162) in order to protect the information systems and data of their clients, which may be legal entities that are governed by private law, public institutions, and individuals. They develop firewall and anti-intrusion systems and also help their customers to monitor their networks, update software, assess risks, detect and correct vulnerabilities and, more generally, improve cyber hygiene and adopt effective policies and good practices regarding the sustainability and security of IT systems.

B) Attribution of cyber-attacks

A second area where digital companies are increasingly involved is the attribution of cyber-attacks. This function takes two main forms.

a) In June 2012, Google announced that it would now notify its users in case they were hacked by States. Google explained that if an intrusion of the accounts of its users was suspected, then the user would receive the following message: "Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now".(163)

Similarly, Facebook announced in October 2015 that it would send a notification to its users if it believed their account had been hacked by a person suspected to be working on behalf of a government force.(164)

(162) This term refers generally to "Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative". US Department of Defense, *Dictionary of Military and Associated Terms*, mars 2017, p. 181 (www.dtic.mil/doctrine/new_pubs/dictionary.pdf).

(163) See Eric Grosse, "Security warnings for suspected state-sponsored attacks", Google, 5 June 2012, (https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html).

(164) Alex Stamos, "Notifications for targeted attacks", Facebook, 17 october 2015 (www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766/.

Yahoo[165] and Microsoft[166] followed suit in December 2015, while Twitter, although without having announced a similar policy, warned several political activists of similar intrusions.[167] All of these technology companies have accompanied their announcements with the clarification that "in order to protect the integrity of their methods and processes", they "won't be able to explain how they attribute certain attacks to suspected hackers" but that notification would take place "only in situations where the evidence strongly supports [their] conclusion".[168] The stated objective of these notifications would be that the hacked person changes his password and establishes security measures.

b) The second major function in terms of attribution concerns certain companies specializing in this field, that offer their services to private or public clients. For example, cyber-security companies such as FireEye, Novetta, Mandiant or CrowdStrike have been particularly active in recent years in this area, accusing foreign governments of hiding behind significant cyber-attacks, ranging from theft of intellectual property and industrial cyber-espionage[169] to the hacking of the Democratic Party in the US elections in 2016.[170]

The increasing role of private companies in the attribution of cyber-attacks raises a number of political and legal questions. For the first time, perhaps, in the history of international law, the attribution of an action to the State (followed by important consequences relating to issues of reaction and responsibility), is mainly assumed by private actors instead of States. However, it may be assumed that this "private attribution" could be encouraged by States in some cases, as they may be reluctant to assume responsibility, for a variety of reasons. But this occult and informal "partnership" in attribution is, as it has been pointed out correctly, tenuous and even dangerous:[171] the motives of private cyber-security companies (guided by their commercial interests and in pursuit of financial gain, while providing for an excellent advertisement by attributing attacks to powerful States), are not necessarily the same as those of a State that must protect its national security,

(165) Bob Lord, "Notifying Our Users of Attacks by Suspected State-Sponsored Actors", Yahoo, 21 december 2015 (https://yahoo-security.tumblr.com/post/135674131435/notifying-our-users-of-attacks-by-suspected).

(166) Scott Charney, "Additional steps to help keep your personal information secure", Microsoft, 30 décembre 2015 (https://blogs.microsoft.com/on-the-issues/2015/12/30/additional-steps-to-help-keep-your-personal-information-secure/).

(167) See Bethany Horne, "Twitter 'leaving us in the dark' over state hacking claims, activists say", *The Guardian*, 4 février 2016 (www.theguardian.com/technology/2016/feb/04/twitter-leaving-us-in-the-dark-over-state-hacking-claims-activists-say).

(168) According to the phrase used by Facebook. See also the warning by Google : "You might ask how we know this activity is state-sponsored. We can't go into the details without giving away information that would be helpful to these bad actors, but our detailed analysis—as well as victim reports—strongly suggest the involvement of states or groups that are state-sponsored".

(169) For more examples see K. Eichensehr, "The Private Frontline in Cybersecurity Offense and Defense", *Just Security*, 30 October 2014 (http://justsecurity.org/16907/private-frontline-cybersecurity-offense-defense/) or K. Eichensehr, "Public-Private Cybersecurity", *Texas Law Review*, No. 95, 2017, 19-23.

(170) See, for example, Ellen Nakashima, "Cybersecurity firm finds evidence that Russian military unit was behind DNC hack", *The Washington Post*, 22 December 2016 (goo.gl/hQFIqM).

(171) K. Eichensehr, "Public-Private Cybersecurity", *op. cit.*, p. 23.

legal and natural persons. The untimely action of a private enterprise that is poorly coordinated with the State could have negative repercussions on its foreign policy and create tensions with the State accused by the private company. The methods and techniques used might also require close monitoring by the State to verify the relevance of the attribution.

C) Hack-back and "active cyber defense"

Without neglecting the important issues raised by the role of the private sector in terms of attribution, we will concentrate on a third area of its involvement in cybersecurity; that of cyber offensive measures, adopted to counter a cyber-attack, mitigate its effects and prevent its repetition. The practice of "hack-back" is based on the idea that "the best defense is a good offense".

The term "hack-back", "hacking back", or "reverse hacking" does not really have a formal definition, while no international organization has really focused on this crucial but highly sensitive issue up to this point. This term, describes an activity that is easily understood as the retaliation of the victim of a cyber-attack against the attacker. The term "hack-back" indicates, therefore, that the response to a cyber-attack can implore as varied techniques as the attack ("hacking"(172)) itself.(173)

However, in order to avoid qualifying the victim who responds to such an attack as a hacker (certainly in "return", but a "hacker" anyway), business and some States tend to prefer the use of a euphemism: that of "active cyber defense". This cyber neologism(174) not only avoids the use of terms which may have a pejorative connotation to describe the victim's reaction, but also allows a high degree of legitimacy to be given to such reaction by referring implicitly to the victim's right to "self-defense". Moreover, this expression obscures the offensive nature of the measures adopted: the reaction does not constitute a counter-offensive measure,

(172) According to the definition proposed by *Technopedia*: "Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose" (www.techopedia.com/definition/26361/hacking).

(173) As it was already written by Renee Albersheim in 1999: "reverse hacking involves striking back at a hacker. A hacker is someone who through various technical means gains access to a computer system without authorization. With a reverse hack, a system administrator identifies the hacker as he enters the system, and sends a response back in kind. The purpose is to prevent damage to the administrator's system, while damaging the attacker's system in the hope that this will deter the hacker from attempting to try again". R. Albersheim, "The Legal Implications of Corporate Reverse Hacking", *Preventive Law Reporter*, Vol. 18, Summer 1999, p. 8.

(174) While this term is relatively new in the cyber context, the term "active defense" had already been used (not without controversy) in the context of conventional warfare as early as 1974. The US Department of Defense, *Dictionary of Military and Associated Terms*, defines "active defense" as "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy". For the history of this term and its transposition in the cyber field, see Robert M. Lee, "The Sliding Scale of Cyber Security", *SANS Analyst White Paper*, SANS Institute InfoSec Reading Room (2015), 9-11 (www.sans.org/readingroom/whitepapers/analyst/sliding-scale-cyber-security-36240) and "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats", Project Report, George Washington University Center for Cyber and Homeland Security (October 2016), p. 6-8 (https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf).

but, rather, is a means of "active defense". Apparently, this recalls Talleyrand's famous answer when he was asked to define the term "non-intervention". He replied: "it is a metaphysical and political word which means almost the same thing as intervention".

The literature in this field demonstrates that the term "active cyber defense" is used to describe various activities ranging from the "passive defense" described above (installing and activating a firewall or anti-virus could be characterized as "active cyber defense"), to certain particularly aggressive techniques such as the destruction of networks, systems or data of the opponent, through other measures such as disconnection, inactivation of botnets, temporary suspension of the functionality of a system or access to data, etc. As it concerns some techniques, it is rather challenging to establish within which of the two extremities (passive/offensive) of the spectrum of possible cyber defenses they belong. This is the case, for example, of the so-called "honeypots" designed to attract declared or potential adversaries to identify them and possibly neutralize them(175). These honeypots have the main function of attracting hackers to a specific space in order to unmask them, but they can also monitor the opponent's system in order to anticipate and prevent future attacks more efficiently. In a more aggressive logic, "honeypots" could also be used to introduce cyber-offensive capabilities into the opponent's system that could steal or destroy data, suspend networks or cause irreversible damage to their networks' Information Systems.

For the purposes of this study, instead of considering the whole spectrum of "active cyber defense", we will focus on its "reactive and offensive" component, namely hack-back. We will first present the arguments in support of hack-back, while showing the risks and disadvantages of this practice (1). We will then proceed to an analysis of international law that allows us to distinguish between the "wild" and uncontrolled hack-back, practiced unilaterally by the private sector, which finds no support in international law (2), and the "regulated" hack-back, which is conducted under the impetus and close control of the State and which, although posing certain difficulties, may be allowed by international law (3).

1. Arguments in favor and against hack-back

Several arguments have been implored in order to support the hack-back (A), but the risks and inconveniences of this practice are numerous (B).

(175) See for example, Darren PAULI, "Dell offers sweet, sweet, free honeypot tool to trap hungry hackers", *The Register*, 7 March 2016
(www.theregister.co.uk/2016/03/07/this_free_honeypot_tool_may_save_your_network_from_hacker_obliteration/).

A) Interest and advantages of hack-back

At least six arguments have been used(176) to praise the virtues of hack-back.

a) Hack-back could compensate for shortcomings in governmental action

One of the main arguments put forward in favor of hack-back is that governments are not in a position to protect legal and natural persons from cyber-attacks effectively. Governmental action, described as slow and strewn with pitfalls, would ultimately offer few guarantees to the victims. The hack-back would, therefore, avoid the delays caused by the executive and jurisdictional powers which are sometimes not very inclined or capable of acting in the digital space. As J.E. Messerschmidt noted:

> "Hackbacks avoid some of the most troublesome challenges of traditional remedies, including "lengthy prosecutions, thorny jurisdictional matters, technologically unsophisticated juries, and slow courts" which are unhelpful when viruses and worms can propagate at remarkable speeds. Traditional law enforcement typically lacks the resources or the expertise to adequately respond to cyber attacks, and is largely ineffective in cases of cross-border intrusions".(177)

On the ethical level, the State's inability to act effectively so as to protect legal and natural persons against cyber-attacks would open the way to derogations from the "social contract" which established the "monopoly on violence" (*Gewaltmonopol des Staates*) of the sovereign State:

> "[I]f there is a social contract to swap our natural executive powers for collective security—a reasonable arrangement—it seems premised on the ability of the state to live up to its purpose of protecting us. If the state fails in this duty with respect to a particular threat, the entire social contract is not necessarily voided, but the state's monopoly on violence could be apportioned back to citizens to defend ourselves".(178)

b) The hack-back would be faster and more efficient

This argument is in line with the previous one: cyber-attacks would require an immediate response in order to counter the adversary in an effective manner. Better still, they would require for work ahead, dealing with the anticipation of an attack and going through the development of decoys to trace the activities of hackers in the company system, to attribute the attack and to prevent, through active cyber defense techniques, the taking place of new attacks. To content

(176) Amongst the policy papers that defend hack-back, see for example, Irving LACHOW, "Active cyber defense: a framework for policymakers", *Center for a New American Security*, February 2013 (www.cnas.org/publications/policy-briefs/active-cyber-defense-a-framework-for-policymakers) and Patrick LIN, "Ethics of Hacking Back: Six arguments from armed conflict to zombies", *A Policy Paper on Cybersecurity, Ethics+Emerging Sciences Group*, 26 September 2016 (http://ethics.calpoly.edu/hackingback.pdf).

(177) J.E. MESSERSCHMIDT, "Hacback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm", *Columbia Journal of Transnational Law*, Vol. 52, No. 1, p. 293. See also Neal KATYAL, "Community Self-Help", *Journal of Law, Economics and Policy*, Vol. 1, 2005, p. 60.

(178) P. LIN, "Ethics of Hacking Back: Six Arguments from armed conflict to zombies", *op. cit.*, p. 8.

oneself with a purely "reactive" approach on behalf of the State would therefore mean leaving the initiative to the adversary. In addition, given the technical expertise and power of leading digital players (Google, Microsoft, Apple etc.) and cyber-security companies, private responses could be more effective than public responses. It should be highlighted that "hack-back" was popularized by Google's immediate response to the cyber-attack McAfee called "*Operation Aurora*". At the end of 2009 Google had realized that it was the victim of a significant and sophisticated cyber attack. At the time, it considered that an immediate response was required to avoid the theft and alteration of source codes, to identify the hackers and to stop their attack. The counter-attack enabled Google to establish that about thirty other companies, mostly American ones, had been affected by the operation, and to communicate both to them and law enforcement, information in this respect.(179)

This need for rapid self-protection would be all the more important since the development of the Internet of Things (IoT), which is accompanied by the placing on the market of billions of connected objects,(180) which by being capable of being mobilized in the context of cyber-attacks, render governmental reactions increasingly complicated.

c) Hack-back would have a significant deterrent effect

The deterrent effect of hack-back has often been advocated by its supporters. In a well-known report published in May 2013, the Commission on the Theft of American Intellectual Property recommended to the US government and Congress that American companies be given the opportunity to respond to cyber-attacks in a "**threat-based deterrence**" manner. According to the Commission:

> "Effective security concepts against targeted attacks must be based on the reality that a perfect defense against intrusion is impossible. The security concept of threat-based deterrence is designed to introduce countermeasures against targeted hackers to the point that they decide it is no longer worth making the attacks in the first place".(181)

The idea is that a rapid and robust response by the private sector could significantly increase the risks and costs for hackers and drive them to abandon future cyber attacks. Should a potential hacker know that a company like Google would counterattack(182) and that there would be serious consequences for him, it is likely that he would refrain from launching a cyber-attack. In this regard, even

(179) See Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show", *Wired*, 14 Januany 2010 (www.wired.com/2010/01/operation-aurora/).

(180) Estimations about the number of things connected to the IoT by year 2020 vary from 26 billion devices to an astonishing 212 billion devices! See, Michael Miller, *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World*, Indianapolis, Que Publishing, p. 12.

(181) The Commission on the Theft of American Intellectual Property, *The IP Commission Report*, May 2013, p. 80 (www.ipcommission.org/).

(182) As was written in a technology blog after the hack-back to Google during *Operation Aurora*: "it's pretty awesome: If you hack Google, they will hack your ass right back". Quoted by J.E. Messerschmidt, *supra* note 177, p. 277.

analogies with nuclear deterrence have been made; yet, there is a great difference in the context between the two situations[183] and, as we shall see, the dissuasive effect of hack-back is far from assured in some cases.

d) Hack-back would allow companies to not reveal their vulnerabilities

Companies may be reluctant to cooperate with the State authorities and may therefore prefer to provide their own defense, be it passive or active.

They may fear that an appeal to the State will render their security flaws and other vulnerabilities public. This could affect negatively the reputation of the company (for example, that it is not able to protect customer data), impact the share price of the company[184] (or its bonds), or even be used by its competitors for counter-advertising purposes.[185]

More generally, private companies may also not wish government departments to access their systems, their data and the data of their clients. The Snowden revelations have shown the extent of mass surveillance undertaken by the secret services of certain States, and the proliferation of surveillance laws around the world does not alleviate these fears. On an institutional level, a solution could be an organic separation within States between Intelligence and Cyber Security Activities. The example of France might be useful in this regard, because the National Cyber Security Agency (ANSSI)[186] is placed outside the intelligence community. This allows ANSSI to cooperate with private companies and other administrations, which are usually less inclined to cooperate with intelligence services, while encouraging responsible management of IT vulnerabilities.

e) Hack-back would solve delicate problems of extra-territoriality

Another advantage of hack-back would be that it would avoid sensitive issues of extra-territoriality. How can a State protect legal entities (or persons) located abroad, that are victims of cyber-attacks? It is true that, by virtue of its personal jurisdiction recognized by international law, the State may act for the protection of its nationals abroad, but such action may be subject to the exercise of the territorial jurisdiction of the State within whose territory these persons are found. Conversely, how could a State provide for the protection of foreign

(183) Among other things, nuclear deterrence involved only a very limited number of known state actors, threatened with "mutual assured destruction" (MAD) in the event of a nuclear attack. There is no such thing in cyberspace where potential perpetrators and victims of cyber-attacks are innumerable.

(184) For example, Gemalto's stock tumbled by 9% after the revelations that the NSA, the USA's National Security Agency, and its British counterpart, the SIGINT, had unauthorized access to the encryption keys from the world's largest manufacturer of SIM cards. See "L'action chute après le piratage par la NSA de ses clés de cryptage SIM", *Les Échos*, 20 février 2015 (https://investir.lesechos.fr/actions/actualites/l-action-chute-apres-le-piratage-par-la-nsa-de-ses-cles-de-cryptage-sim-1033016.php).

(185) For an analysis see J.E. *Messerschmidt*, *supra* note 177, 293-294.

(186) Agence nationale de la sécurité des systèmes d'information (www.ssi.gouv.fr/).

companies on its territory and what are the difficulties that may arise in this regard (including the risks of industrial cyber espionage and the objectives of confidentiality and discretion mentioned above)? Hack-back would avoid these difficulties by providing the opportunity to these companies to defend themselves against cyber-attacks without having to allow access to their computer systems to States.

f) Hack-back would be good for business and research

Finally, hack-back would enrich enormously the research and growth potential for the active cyber defense industry. Given the scale of threats, the cyber-security market is particularly lucrative. Despite the continuing doubts about the legality of hack-back activities, companies offering active cyber defense tools are increasing, regardless of whether they may be specialized cyber-security companies or large industrial players who develop activities in this field so as not to miss out on what they consider to be "a vast private-sector emerging market for cyber-security solutions".(187)

B) Disadvantages and risks

Hack-back involves various risks: risks for the international system and its stability, risks for the States, and risks for the companies as well. We present here ten of these main risks.

a) Risk of escalation

The use by private actors of cyber-offensive techniques against non-State actors in the territory of another State, and even against the State itself, could lead to a rapid escalation, transforming an initially relatively isolated event into a real international crisis. The foreign State targeted by the attack (or which wishes to defend its nationals) could reply by denouncing the attribution of the initial cyber-attack as erroneous or by denouncing the hack-back measures as neither necessary nor proportionate in view of the circumstances. This response could in and of itself generate a counter-retort on behalf of the other State which might wish to defend its physical or legal persons considering that they have been targeted twice. The hack-back could thus stuck lead to the entry of States in a dangerous vicious circle of counter-reactions. According to another scenario, third States whose legal or natural persons would be the collateral victims of hack-back measures, could also decide to act against the initiator of the hack-back.

Such situations would obviously be in total contradiction with the aims of contemporary international law, which offers States different mechanisms for the

(187) See Loren THOMPSON, "Lockheed Martin Moves To Dominate Cyber Defense of Electric Grid & Energy Complex", *Forbes*, 14 March 2014 (www.forbes.com/sites/lorenthompson/2014/03/14/lockheed-martin-moves-to-dominate-cyber-defense-of-electric-grid-energy-complex/).

peaceful settlement of disputes amongst each other (or of disputes affecting their nationals and property). As shown in Parts I and II, the normal reaction in the event of a cyber-attack should be to address the State from which the attack originated, asking it to act urgently and bring the attack to an end in virtue of its due diligence obligation. Cooperation (including its criminal dimension), the development of joint operations and the use of mechanisms for the peaceful settlement of disputes should be favored. Even assuming that such mechanisms are proved to be impossible to apply, or are impracticable under the circumstances (for example in an emergency), international law has entrusted States with the task of reacting using the means described in Part II. Allowing companies to "do justice themselves", could result in a dramatic increase in threats to international security, bearing in mind the risks of escalation.

b) Risks of destabilization

These security risks could easily destabilize the international system. If hack-back is allowed by a State and practiced by its companies, it is very likely that other States will follow suit. Since international law is based on the principle of reciprocity, such a course would inevitably lead to legal symmetry between the companies of the different States. As it would not be possible for hack-back to be legally reserved for companies in certain States, theoretically, it could be exercised by any company located anywhere in the world. When we are aware of the difficulties encountered by international law in establishing standards of peaceful coexistence between less than 200 states, we can hardly imagine what could happen if International Law had to deal with more or less 200 million existing companies worldwide determined to launch cross-border attacks by exercising hack-back if they are attacked.

c) Risks to the authority of the State

Beyond the international order, the internal order itself could be threatened. Accepting the idea that "States are not able to guarantee security in cyberspace"; that the "social contract" is, therefore, broken; and that the monopoly of legitimate State violence is thus called into question (see supra) could be dangerous. The legal order of the State is based on the idea of a substitution of institutional justice for private justice which prevailed in the "natural State" before the creation of civilized societies.(188) Challenging the principle "no one can take the law into his own hands" (or "no one can do justice to oneself") would be the same as allowing vigilantism and antisocial behaviors, likely to sow disorder. Admittedly, States could theoretically avoid an erosion of their regulatory and enforcement powers by forbidding "internal" hack-back, while allowing transnational "hack-back". The

(188) "[B]efore there were laws each was the sole judge and avenger of the offenses he had received…" wrote Jean-Jacques Rousseau, *Discourse on the Origin and Basis of Inequality Among Men*, 1754, p. 96.

confession of the State's powerlessness in the face of cross-border cyber-attacks, as well as its abdication in this regard would, nonetheless, send a disastrous message to the authority of the State and its capacity to exercise its regal functions in the face of new threats.

d) Risks to the conduct of foreign policy

An untimely or uncoordinated hack-back activity, undertaken without consultation with public authorities, could create diplomatic tensions and complicate the conduct of a State's foreign policy. This has been particularly evident when private cyber-security companies have publicly attributed a cyber-attack to a foreign State. For example, authors have pointed out that the release of the Mandiant Report in February 2013 "set off a bomb in one of the most delicate and thorny areas of US foreign policy"(189) and that "the decision to launch the bomb came from a private company marketing its services, not from the government agencies charged with diplomacy, national defense, or intelligence".(190)

e) Risks for the Intelligence and the fight against crime

Similar risks could arise within other areas of State activity. The individual actions of a private actor against a hacker could, for example, jeopardize operations carried out against the same target by the Intelligence agents of the State. Similarly, hack-back actions designed to erase data stolen by the hacker could destroy the evidence necessary for prosecution and, thus, hinder the activities of law enforcement. Even worse, hack-back could become an easy excuse for cyber-criminals to justify malicious acts. Today, the prohibition of all hacking activities by the domestic legal systems (see Part III 2C) allows for a clear distinction between the victims and the perpetrators of a cyber-attack. Authorizing hack-back would mean the blurring of this distinction: the perpetrators of a cyber-attack would undoubtedly pretend, henceforth, that they did nothing more than respond to initial attacks, prevent attacks, protect victims, gather evidence or establish attribution. Consequently, the fight against cyber-crime would become more complex.

f) Risks of collateral damage

Innocent third parties could also become victims of hack-back activities. This could, first of all, occur as a result of **errors in attribution**. The risk is all the more important, as the hack-back action could be launched without taking the necessary time to proceed with the attribution with relative certainty.(191) The experience obtained from the Military and Private Security Companies (PMSCs) which will be discussed later, shows that under-trained and/or over-zealous

(189) Shane Harris, *@WAR: The Rise of the Military-Internet Complex*, 2014, p. 206.
(190) K. Eichensehr, "Public-Private Cybersecurity", *op. cit.*, p. 23.
(191) See P. Lin, *supra* note 178.

private security agents may act in an untimely or even abusive manner. The risk of collateral damage also stems from the nature of some cyber-attacks. In the context of a Denial of Service attack (DDoS), for example, "zombie" computers can be used by hackers without their owners' knowledge; putting botnets out of service during a hack-back operation could then affect innocent parties.

g) Risks related to "automatic" active cyber defense

The previously mentioned risks are all the more important as active cyber defense is becoming increasingly "automated". In order to respond more effectively to cyber-attacks and to adapt to the growing complexity of the means used, active cyber defense uses machine learning and artificial intelligence. This increases the adaptability, reactivity, precision and, in fine, the effectiveness of the hack-back, but also the risks of error in case of bad design and programming of the system or in case of its manipulation by an external malicious act.(192)

h) Risks of a "backlash"

Companies that exercise hack-back could be confronted with a so-called "backlash". If giants such as Google or Microsoft have undoubtedly little to fear, SMEs that engage in counter-attacks against powerful hackers (linked, for example, to a State agency), could be crushed by the counter-offensive hacker. Acting in concert with their State could prove to be a wise decision.

i) Risks of an elitist or hypocritical active cyber defense

This last remark could be extended by highlighting the inequality between the few major players in digital technology, and the realm of millions of SMEs around the world. The latter may not have the financial resources to acquire effective cyber defense tools or the skilled human resources to use them; as a result, a small proportion of firms would have the technical capacity and skills to respond to cyber-attacks effectively and relatively safely. Even worse, a general authorization for hack-back could lead to mafia-like practices by unscrupulous cyber-security players who would launch attacks against SMEs without active cyber defense tools in order to sell them their "protection". Last but not least, hack-back could easily become a pretext to legitimize industrial cyber-espionage, or to harm competitors.

j) A questionable deterrent effect

The supposed deterrent effect of hack-back encounters important limitations. While the fear of a robust response could possibly deter isolated hackers motivated by the lure of gaining, it will probably have no effect (other than the

(192) See, for example, Ian Goodfellow, « Deep Learning Adversarial Examples – Clarifying Misconceptions », *KD Nuggets*, July 2015 (www.kdnuggets.com/2015/07/deep-learning-adversarial-examples-misconceptions.html).

need for better preparation or concealment) on terrorists or other actors with ideological motives such as "patriotic" or political hackers in connection with State interests.

2. The "wild" hack-back: can private actors unilaterally trigger cyber-offensive measures?

A positive law analysis is essential at this point, to examine the compatibility of hack-back with existing law. We will focus here on what we will call the "wild" hack-back, in order to describe uncontrolled responses to cyber-attacks, practiced unilaterally and autonomously by the private sector, which we will compare to what we will subsequently name a "wise" hack-back, undertaken under the impetus and the close control of the State. We shall see, first of all, that international law does not recognize any right of "wild" hack-back (A). This does not necessarily mean that a private hack-back operation violates international law as such (B); it is, however, in most cases, a violation of the domestic law of the country concerned, exposing the perpetrator to considerable legal risks (C).

A) The absence of a "hack-back right" in international law

In international law, non-State actors, regardless of whether they are individuals, national minorities or businesses, can be entitled to rights as a matter of principle. But for this to happen it is necessary that the States, the creators of international law, recognize these rights in international treaties or other classical ways of forming international law (in particular customary law and the unilateral acts of international organizations, invested by the States with a normative power). An analysis of positive international law clearly shows nonetheless that there is no right to "hack-back" by private actors.

On the one hand, it is clear that there are no specific and express rules drawn up by States to recognize such a right. The few international treaties that exist in this field do not express anything that could be interpreted as favoring the practice of hack-back. On the contrary, they often call on States to combat cybercrime; an example would be the 2001 Budapest Convention which calls on States, as we shall see, to criminalize infringements of the integrity of computer systems. As for soft law instruments, such as the rules approved by the GGE, they are far from favoring the unilateral actions of non-State actors, as they call upon States to "ensure that non-State actors do not use their territory to commit internationally wrongful acts by means of information and communications technology".(193)

(193) *GGE 2015*, *supra* note 2, p. 15.

On the other hand, as we shall see by examining several among them, the general rules of international law that also apply to cyber security can in no way be interpreted as conferring a right of hack-back on non-State actors.

It is at first **impossible for these non-State actors to rely on the theory of countermeasures**, analyzed in detail in Part II. Countermeasures could only be adopted by injured States(194) against other States under the strict conditions already analyzed. It is, therefore, the States which, according to the logic of international law, are entitled to take action by adopting countermeasures in response to the internationally wrongful act committed by another State which affected their rights or those of their nationals. On the basis of international law, States have a right not only to protect their territory and sovereignty but also to exercise their protection in favor of any natural or legal person in respect over which they have competence, starting with their nationals.(195) In this respect, they have the capability to adopt all measures permitted by international law, including countermeasures. This right does not exist, in principle, for private persons. As an author stated, "As far back as history can be traced, the right of reprisal has always been a public right, a sovereign and regal right".(196) Of course, as we shall see (*infra* Part III, 3), in certain circumstances States could expressly concede to private actors the possibility of exercising countermeasures, but this involves an express act, close control by the State and the risk for the latter to engage its responsibility, as the reactions subsequently adopted would be regarded as actions of the State itself.

In the same way, it is **impossible for private actors to rely on the theory of "self-defense"** in international law. In this regard, any possible confusion arising from the use of the term "cyber defense" (active or otherwise passive) should be clearly dismissed. The concept of self-defense in international law, as codified also by Article 51 of the Charter of the United Nations, refers to something very specific: an armed attack committed against a State. Self-defense, moreover, can only be invoked by the victim States. An individual, a company or a private actor cannot, from the point of view of international law, be the victim of "armed attack" or invoke the right of self-defense enshrined in Article 51 of the Charter. In recent years, it has been greatly debated concerning this doctrine of international law as to whether, beyond States, non-State actors (and especially terrorist groups such as Al-Qaeda or ISIS) could **also** commit an armed attack (and this, despite the traditional position of the International Court of Justice, according to which an armed attack can only be committed by one State against another).(197) Regardless of what

(194) International organizations, as subjects of international law, also have the capacity to adopt countermeasures under certain conditions. See Articles 22 and 5 & 57 of the Draft Articles on the Responsibility of International Organizations adopted by the United Nations International Law Commission in 2011 (http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf).

(195) See also the so-called "diplomatic protection" mechanism in international law.

(196) D. ALLAND, *Justice privée et ordre juridique international*, Paris, Pedone, 1994, p. 316. Our translation.

(197) Thus, in its Advisory Opinion of 9 July 2004 on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, the Court emphasized that: "Article 51 of the Charter recognizes […] the existence of an inherent right of self-defence in the case of armed attack by one State against another State".

the interest of this debate is, it has never been suggested in international legal scholarship that these actors could be victims of armed attack, providing them thus with the possibility of invoking "self-defense" to launch attacks against other States.

Nor can private actors rely on certain other mechanisms of self-protection recognized by international law, such as the "right of hot pursuit". This important Law of the Sea right is codified in Article 111 of the 1982 United Nations Convention on the Law of the Sea (Montego Bay Convention). According to it, a coastal State has the right, under certain conditions, to undertake the pursuit of a foreign ship when it has good reason to believe that this ship has violated the laws and regulations of the State. Such pursuit must be commenced when the foreign ship is within the internal waters, the territorial sea or the contiguous zone of the pursuing State, and may only be continued outside the territorial sea or the contiguous zone if the pursuit has not been interrupted. The right of hot pursuit ceases as soon as the ship pursued enters the territorial sea of its own State or of a third State. It might be tempting to draw inspiration from this old rule of the Law of the Sea and consider the idea of a "cyber right of hot pursuit". But like the traditional "right of hot pursuit", an extension into cyberspace should, in principle, be reserved only to State authorities. Article 111 of the Montego Bay Convention, for example, emphasizes that "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 and authorized to that effect".

Finally, private actors **cannot rely on human rights** to exercise hack-back measures. While it is true that certain instruments relating to the protection of human rights (such as the European Convention on Human Rights) proclaim important rights such as the right to life or the protection of private property, at no time do they invest individuals with a right to "take the law in their own hands" and use vigilante justice in order to protect themselves. The logic of international conventions for the protection of human rights is that the States must act to guarantee these rights by protecting their beneficiaries from attacks both by State agents and by private actors, in case the State knows, or ought to have known, that a serious threat exists (positive obligations theory). Again, it is impossible to erase the State from the equation of action, protection and reaction.

It should be added that **private actors cannot, of course, rely either on the concept of self-defense under domestic law** to launch such cross-border attacks. Beyond the fact that in many domestic legal systems it would be difficult to invoke "self-defense" to respond to a cyber-attack, such a possibility would not change anything from the point of view of international law. In other words, even if we assume that a right to hack-back is recognized in some legal systems (which seems not to be the case for the time being), it would, in no way, imply the existence of such a right within the international legal order, which is a distinct legal order. According to the fundamental rule codified by the International Law Commission

of the United Nations: "The characterization of an act of a State as internationally wrongful is governed by international law. Such characterization is not affected by the characterization of the same act as lawful by internal law".(198)

B) A violation of international law?

We have seen that international law does not provide private actors with a right to "hack-back". This does not mean that a hack-back operation by private actors would automatically be a "violation" of international law. It may well be the case that the international legal order does not, for the benefit of a natural or legal person, recognize a "right" to do something without, however, considering that such an action is "prohibited" by international law. This situation is often the result of a willingness to allow States to decide freely on certain matters falling within their "reserved domain".

The question of whether the "hack-back" undertaken by private actors constitutes a violation of international law has, as we shall see, relatively little practical interest. Nevertheless, it is necessary to examine this question quickly and to note that, most likely, international law does not at the moment prohibit a "private" hack-back as such.

Of course, a hack-back action by a State could, in certain circumstances, constitute a violation of the sovereignty of another State, or even a violation of the principles of non-interference and non-intervention. But, normally, only States can violate those principles; a private actor, whose actions are not attributable to a State, does not, in principle, violate the obligation of non-interference.(199) This does not mean, however, that the behavior of the private actor is in a legal *vacuum*. That conduct could, as we shall see, constitute a breach of the domestic law of that State, allowing for the private actor to be prosecuted. Moreover, the fact that the State which is responsible for the actions of the private actor has not taken the necessary measures to put an end to the hack-back which causes damage to another State in a manner not justified by international law, could constitute a breach of the State's due diligence obligation (see Part I), exposing that State to countermeasures on behalf of the victim State. The same is true, of course, if the acts of hack-back of the private actor can, in one way or another, be attributed

(198) *YILC 2001*, *supra* note 19, Art. 3.

(199) A position held also by the *Tallinn Manual 2.0*, *supra* note 12, Rule 33, §1 et 2: "[I]nternational law by and large does not regulate cyber operations conducted by non-State actors, such as private individuals or companies. The International Group of Experts agreed that cyber operations conducted by non-State actors that are not attributable to States do not violate the sovereignty of the State into which they are launched, constitute intervention or amount to a use of force because these breaches can be committed only by States". Paradoxically, while the experts unanimously acknowledged in this passage that non-State actors cannot violate the principle of the prohibition of the use of force, a majority of them later considered (Rule 71, §18-19) that these same non-State actors could nevertheless commit an "armed attack" (within the meaning of article 51 of the UN Charter), including by cyber means.

to a State.(200) As a result, we fall back into a classic "inter-State" logic where the reactions described in Part II are applicable.

It might also be asked whether the hack-back could be considered an "international crime" directly prohibited by international law. Indeed, international law may establish certain offenses attributable to individuals acting on a purely private basis as "international crimes" allowing for the triggering of their international criminal responsibility. This has been done, for example, with acts of piracy on the High Seas; the slave trade; hijacking of airplanes; drug trafficking; or certain acts of international terrorism. The creation of a new "international crime", nevertheless, requires the adoption of specific conventions in this regard or a clear recognition by the international community of States. As noted by Ellen S. Podgor, "membership in the exclusive club of international crimes is limited".(201) However, it is not certain that cyber-attacks have taken this step as such.(202) Instruments against cybercrime have been adopted, the most famous of which is the Budapest Convention on Cybercrime of 2001, now ratified by 52 States. The Convention requires States to adopt "the legislative and other measures that are necessary to establish as criminal offenses, in accordance with [their] domestic law", a whole series of conduct including breaches of data integrity or the integrity of computer systems.(203) The Budapest Convention does not explicitly define cybercrime as an "international crime" but by appealing to States to criminalize it within their domestic orders, to harmonize their legislation and to cooperate in combating it, clearly constitutes an effort to internationalize this offense. However, the calls for the adoption of a universal convention against cybercrime have not yet been met with success.(204) Moreover, even assuming that "hacking" could be considered an international offense, this should not automatically be the case of "hack-back" too, as it responds to a different logic.

Even if private "hack-back" is not an "international crime", the importance of such a conclusion should not be exaggerated or confusing. In fact, international criminal jurisdictions such as the International Criminal Court have no jurisdiction over such matters anyway. The real practical question is how national criminal law applies in this area and how a perpetrator of a hack-back operation

(200) See *infra*, Part III (3C).

(201) E.S. Podgor, "Cybercrime: National, Transnational or International ?", *Wayne Law Review*, Vol. 50, No. 97, 2004, p. 104.

(202) It goes without saying, however, that a cyber-attack could become the instrument by which an international crime could be committed (eg. an attack on civilians constituting a war crime).

(203) See: "Article 4 – Data interference. 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.", "Article 5 – System interference. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data".

(204) See J. Clough, "A World of Difference: The Budapest Convention on Cybercrime and The Challenges of Harmonisation", *Monash University Law Review*, Vol. 40, No. 3, 2014, 725-729.

could face the risk of prosecution at a national level and international criminal cooperation against him at the international level.

C) Hack-back as a violation of domestic law

Acting spontaneously or under the influence of instruments such as the Budapest Convention on Cybercrime of 2001, many countries have legislated against cybercrime by criminalizing violations of data integrity or the integrity of computer systems. A recent analysis has shown, for example, that all G8 countries have passed laws imposing fines and/or prison sentences for such violations.(205) None of them seems to allow private hack-back;(206) neither expressly prohibits it either, but it is normal to think that the same regime that prohibits "hacking", simultaneously prohibits in principle hacking back, unless certain classic exceptions or legal excuses (such as legitimate defense or necessity)(207) can justify it.(208) In some countries, legislation specifically provides for a response to cyber-attacks, allowing for the State or the persons authorized by it, to undertake such a response. In France, for example, the practice is governed by article 21 of the 2013 Military Programming Law, which provides that authorized State agents may take such measures to characterize an attack and/or neutralize its effects by accessing the information systems that are at the origin of the attack.(209)

A private actor who conducts a hack-back operation with transnational consequences could in fact violate the domestic law of several States: the State from

(205) See P. Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures", *Stanford Journal of International Law*, Vol. 50, 2014, 742-745.

(206) It should be noted, however, that a Bill introduced (but not yet adopted) in the United States on 23 February 2017 aims to legalize certain acts of hack-back for the first time. This is the Active Cyber Defense Certainty Act (ACDC), which seeks to amend section 1030 of the Computer Fraud and Abuse Act to allow victims of a cyber-attack to "access without authorization the computer of the attacker […] to gather information in order to establish attribution of criminal activity to share with law enforcement or to disrupt continued unauthorized activity against the victim's own network". However, this bill does not allow hacking victims to "destroy the information stored" on the attacker's computer, to "cause physical injury to another person", or to "create a threat to the public health or safety". For the text see Congressman Tom Graves's website (https://tomgraves.house.gov/uploadedfiles/discussion_draft_ac-dc_act.pdf).

(207) In this regard, it should be noted that according to para. 38 of the Explanatory Report to the Budapest Convention: "A specificity of the offences included is the express requirement that the conduct involved is done 'without right'. It reflects the insight that the conduct described is 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". The Report does not, however, consider the hypothesis of a private hack-back. It emphasizes that "The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences)". See (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b).

(208) It should be noted, however, that none of these laws seems to provide for mitigation from responsibility applying specifically to hack-back.

(209) According to Articles L. 2321-1 and L. 2321-2 of Chapter I, Title II, Book III of the second part of the Defense Code: "Art. L. 2321-1. - As part of the national security strategy and defense policy, the Prime Minister defines the policy and coordinates the government's action on the security and defense of information systems. To this end, he possesses the authority regarding the national security of the information systems, which ensures the function of a national authority for the defense of information systems". "Art. 2321-2. - In order to respond to a computer attack that targets information systems affecting the war or economic potential, security or survivability of the Nation, the State services may, under the conditions set by the Prime Minister, carry out the technical operations necessary to classify the attack and to neutralize its effects by accessing the information systems which are at the origin of the attack". Our translation. Emphasis added.

which it acts, and the State or States where hack-back causes damage. If these countries prohibit unauthorized access to computer systems and attacks on the integrity of such systems and data, prosecution may be initiated. Even assuming that the State of nationality of the perpetrator of the hack-back operation does not wish to act against him, it does not mean that the perpetrator will be immune from any consequences. The affected State(s) could, thus, use the channels of criminal cooperation and mutual legal assistance against him. They could issue arrest warrants and make requests for the arrest and extradition of the suspect (in exactly the same way as they sometimes do with a "hacker"). The author of the hack-back could, therefore, find himself caught in the net of international cooperation against cybercrime favored by instruments such as the Budapest Convention. In short, as one writer wrote: "Anyone who engages in retaliation should avoid international trips".(210)

So far, we have not heard of any prosecutions against perpetrators of hack-back operations. This is probably due to a number of reasons. On the one hand, both the perpetrators of such practices and hack-backed persons might prefer not to advertise such situations in order to avoid, precisely, the risks of prosecution. On the other hand, in most cases, which have become public, the hack-back took place most often in coordination with the State(211) or on the basis of an authorization delivered by the national judge.(212) As a result, this could lead us to the conclusion that we are often in the logic of a more "regulated" hack-back, undertaken under the impulse or with the consent of the State.

3. The "regulated" hack-back: can States rely on private actors to conduct counter-attacks?

A "wild" hack-back, conducted unilaterally by private actors, gives rise, as we have seen, to several legal and technical difficulties. In this context, it is necessary to consider now to which extent would a hack-back, undertaken following authorization by the State and in consultation with its authorities, be considered more "wise" and raise less legal difficulties. This question invites us to reflect on the prospects and possible forms of cooperation between public and private actors to respond to cyber-attacks (A). In this respect, the experience of private military and security firms shows an interesting parallel (B). More generally, the idea of a "regulated" hack-back brings us back to the fundamental question of the triggering of the international responsibility of States due to the conduct of private actors (C).

(210) J.A. Lewis, "Private Retaliation in Cyberspace", *Center for Strategic and International Studies*, 22 May 2013 (www.csis.org/analysis/private-retaliation-cyberspace).

(211) See, for example, *BBC*, "FBI and Microsoft take down $500m-theft botnet Citadel", 6 June 2013 (www.bbc.com/news/technology-22795074).

(212) See, for example, Robert Lemos, "Microsoft Can Retain Control of Zeus Botnet Under Federal Court Order", *eWeek*, December 2012 (www.eweek.com/security/microsoft-can-retain-control-of-zeus-botnet-under-federal-court-order).

A) Cooperation between public and private actors to respond to cyber-attacks?

The answer to the question "can States rely on private actors to hack-back?" is in principle very simple: yes. Yes, but only if the response respects the conditions discussed above (Part II). For example, the fact that a hack-back measure is conducted directly by a State or, instead, by a private entity authorized by that State does not alter the lawfulness of that action, if it constitutes a legitimate countermeasure. Therefore, here we have a profound change in logic and legal regime in relation to a "wild' hack-back triggered unilaterally by a company. In the "wild" hack-back, the company is a "lonesome cowboy" who "takes the law in his own hands" in a sort of lawless digital Far-West. On the other hand, in the "wise" hack-back, it is the State that acts, delegating, if necessary, some of its competences in terms of execution, to private companies. It is no longer a state of nature in which every private actor is "the judge of his own cause" but henceforward an ordered universe where the State maintains and assures its role as guarantor of the protection and execution of the law.

While the delegation of authority from a public authority to a private entity is a well-known institution in legal systems, its application in the field of national security and safety can sometimes present daunting difficulties. The ancient practice of sovereigns granting a "letter of marque and reprisal" to privateers is, in this respect, a good example. A letter of marque was indeed a document emanating from a sovereign enabling a captain to search, attack, seize and destroy, within territorial, international or foreign waters, the ships of an adverse nation from which the sovereign had received offense. The practice was strictly regulated (in France, for example, by the Colbert Ordinance of 1681). Yet it had posed such problems in the conduct of international relations, that the "marque" was eventually abolished in 1856 by the Paris Declaration.

Could we envisage today the resurgence of this practice in the form of "cyber privateers"?(213) To answer this question, it seems necessary to consider several possible situations.

A first scenario could be one in which a State solicits one or more private companies about a specific cyber-attack to which it wishes to respond in the most effective way. Such a hack-back, triggered under the close control of the State, does not seem to pose any problem of principle and could be compatible with

(213) Better term than that of a "cyber mercenary". The term "mercenary" refers to a very precise definition in international law which designates an individual who voluntarily enrolls in the combatant armed forces of a belligerent State of which he is not a national, for personal gains, including of financial nature. As such, it is mainly used in a situation of armed conflict. It should be noted, however, that the International Convention against the Recruitment, Use, Financing and Training of Mercenaries of 4 December 1989 provides for an extension of the term in a situation other than a situation of armed conflict, but this extension seems to be very difficult to apply in case of a hack-back. According to Article 1 (2) of the Convention: "A mercenary is also any person who, in any other situation: (a) Is specially recruited locally or abroad for the purpose of participating in a concerted act of violence aimed at: (i) overthrowing a Government or otherwise undermining the constitutional order of a State; or (ii) undermining the territorial integrity of a State".

international law if the conditions mentioned above (Part II) are respected. The same would apply if firms were to solicit and obtain the agreement and assistance of the State to respond to a specific cyber-attack. Practice offers, in fact, several examples of such situations(214) that cannot be equated to the old practice of "letters of marque".

A second scenario could be what some authors have called "certified active cyber defense". According to this scenario, a State could authorize "a limited number of certified private entities to work with government to take active defense measures focused on attribution, initially to protect critical information within the defense industrial base".(215) Unlike the first scenario (which deals with an *ad hoc* response to a cyber-attack), the State would establish ahead something similar to a "public/private partnership" with companies, designated to respond more effectively to cyber-attacks. To the extent that the State retains a close control over the activities of these private actors, which is all the more efficient because of the limited number of such actors, this scenario does not seem to present insurmountable legal difficulties. Such a solution would make it possible to devise a precise legal framework for "public/private" cyber-security relations, which are often *de facto* and uncoordinated. In so doing, it would ensure that the values of the rule of law such as transparency, access to justice, accountability or protection of privacy are respected.(216) Such a legal framework would, by definition, be regulated by State control and oversight of the activities of its private partners, thereby avoiding a large number of disadvantages associated with the hack-back analyzed above (Part III 1B).

Much more problematic could be a third scenario where the State would give a "carte blanche" to all companies to practice hack-back, based on their own assessment of the need to act. The "hack-back" in such a situation would no longer be truly "wise" and would become "savage" again, rendering effective and narrow control by the State practically impossible. The development of a myriad of "cyber privateers" considering themselves empowered by the State to exercise a right of reprisal could arouse strong international tensions and agitate the specter of the escalation of violence and the destabilization of the States, as already mentioned (Part III 1B).

B) The case of Private Military and Security Companies (PMSCs)

A parallel is necessary here, in relation with the attitude of States towards PMSCs, which has been widely debated in international law over the recent years.

(214) See notes 211 and 212.

(215) Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence", *Atlantic Council Issue Brief* (December 2013), p. 2 et 6-7 (www.atlanticcouncil.org/publications/issue-briefs/cybersecurity-and-tailored-deterrence).

(216) See, in this regard, the recent study of K. Eichensehr, "Public-Private Cybersecurity", *op. cit.*, p. 1-64.

The use of PMSCs has grown considerably over the last two decades for many reasons including the following: the multiplication of external operations since the end of the Cold War; the reduction of the number of armies; the end of conscription; the development of the concept of "zero death"; the management by the United States and its allies of the consequences of the invasion of Iraq in 2003; and the fight against maritime piracy. Today, there are no fewer than 100 PMSCs worldwide with nearly 200,000 employees with an estimated trade volume of $100 billion.(217) Alongside their development, the missions entrusted to the PMSCs have broadly diversified. These may now include advisory services; tactical assistance; the creation and training of police forces and regular armed forces; the protection and surveillance of persons, including the securing of sensitive areas; intelligence operations; refueling and logistical assistance to the troops. The use of PMSCs, a practice often considered as useful by the States, serves to meet needs that the national armed forces can no longer meet, or no longer wish to meet.

The fight against maritime piracy is a rather consensual example of recourse to the PMSCs, despite the major difficulties encountered. The phenomenon of piracy off the coasts of East Africa and especially Somalia has taken on a particularly worrying dimension since the second half of the 2000s. Between 2008 and 2009, the number of attacks by pirates in the area had increased by 300%, despite the progressive development of joint naval operations between States in the context of impressive international cooperation.(218) Although of unquestionable utility, State naval operations have shown their limits in eradicating the phenomenon. Faced with this situation, States have gradually allowed national flag vessels to take on armed members of PMSCs. This, combined with increasingly effective State naval operations, as well as other factors, has led to a dramatic reduction in both the number of successful attacks and the number of attacks themselves.

Despite their usefulness in some specific operational frameworks, the activities of PMSCs have, nevertheless, often been at the heart of important controversies. In various operations, several reports have uncovered abusive practices by members of PMSCs, and even violations of human rights or humanitarian law. The case involving Blackwater employees, accused of killing fourteen people in a shootout in Baghdad on 16 September 2007 and ultimately sentenced to heavy prison sentences in 2015, was arguably the most publicized. Even in the fight against maritime piracy, reports have denounced under-trained and overzealous members of PMSCs killing indiscriminately innocent fishermen mistakenly considered as pirates.

A recent study argues that despite the willingness of States to strictly regulate PMSCs, domestic laws, which are often hesitant and highly diversified, are not

(217) According to the recent book by Thierry Garcia, *Les entreprises militaires et de sécurité privées appréhendées par le droit*, Mare & Martin, 2017 (forthcoming).

(218) *Cf.* David Axe, "Why the Somali pirates are winning", *The Guardian*, 9 April 2009 (www.theguardian.com/commentisfree/cifamerica/2009/apr/09/piracy-somalia-alabama-us-navy).

always sufficient to provide effective regulation for the activities of PMSCs and their members. As for positive international law, both in its regional and international dimension, it has proved to be inadequate and ineffective. Soft law proliferates then, while the self-regulation advocated by the PMSCs has led to the adoption of private codes of conduct whose limits are highlighted in this study.(219)

The various difficulties encountered by States using PMSCs in areas where control is much easier than cyber security do not strongly support a "*carte blanche*" granted to the private sector in the field of hack-back. States are also aware of the risk of their liability being incurred as a result of the activities of these private persons.

C) Can the international responsibility of States be triggered by hack-back measures initiated by private actors?

In international law, States are responsible for the acts (including cyber acts) of their agents, even if they act *ultra vires*.(220) On the other hand, as a rule, the conduct of private persons or entities is not attributable to the States, under international law. Circumstances may, however, arise, where such a conduct may be attributable to a State because there is a *de facto* relationship between the person or entity conducting the activity and the State. Moreover, a violation of the principle of due diligence analyzed above (Part I), can also engage the responsibility of the State.

a) The State is responsible if it empowers private actors to exercise the prerogatives of public authority

According to Article 5 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts", adopted in 2001:

> "The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance".

Thus, a State may be liable if it empowers a private company "to exercise functions of a public character normally exercised by State organs, and the conduct of the entity relates to the exercise of the governmental authority concerned".(221) This could be the case if the State empowers one or more private companies to conduct hack-back operations that violate international law. In such a case, the

(219) T. Garcia, *supra* note 217.

(220) According to article 7 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, adopted in 2001: "The conduct of an organ of a State or of a person or entity empowered to exercise elements of the governmental authority shall be considered an act of the State under international law if the organ, person or entity acts in that capacity, even if it exceeds its authority or contravenes instructions.", *YILC 2001*, *supra* note 19.

(221) Commentary of article 5 §2, *YILC 2001*, *supra* note 19, p. 43.

responsibility of the State would be engaged, without even a need to prove that the hack-back took place under the control of that State.(222)

b) The State is responsible if private actors act on its instructions, directives or under its control

As discussed above (Part I), Article 8 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts" mentions that:

> "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct".

This article could be summarized for the purposes of our analysis as follows:

First of all, the State engages its responsibility if, without "empowering" a private company to exercise the prerogatives of public authority (a hypothesis already discussed above), it recruits private companies as "auxiliaries", or it encourages them to act in this capacity while remaining outside the official structures of the State. An example might be that of a State which "specifically instructed an IT department within a university to carry out a Distributed Denial of Service (DDoS) attack against a designated target" auquel cas "the resulting operation would be attributable to the State in question".(223)

In the Commission's own view, "More complex issues arise in determining whether conduct was carried out 'under the direction or control' of a State. Such conduct will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation".(224) The degree of control that the State must have exercised in order for the conduct to be attributed to it has given rise to much debate and divergence in international jurisprudence. The Commission preferred to conclude that "it is a matter for appreciation in each case whether particular conduct was or was not carried out under the control of a State, to such an extent that the conduct controlled should be attributed to it".(225) In any event, one could conclude that if a hack-back activity by a private company is conducted under the effective control of the State (which monitors its conduct) the State's responsibility can be triggered. On the other hand, if a State has simply encouraged private actors to conduct hack-back operations (without, however, controlling their operations), the responsibility of the State cannot be incurred on the basis of Article 8. It may, nevertheless,

(222) According to the commentary of ILC, "For the purposes of article 5, an entity is covered even if its exercise of authority involves an independent discretion or power to act; there is no need to show that the conduct was in fact carried out under the control of the State.", *YILC 2001*, *Ibid.*

(223) K. Macak, "Decoding Article 8 of the International Law Commission's Article on State Responsibility : Attribution of Cyber Operations by Non-State Actors", *op. cit.*

(224) *YILC 2001*, *supra* note 19, p. 47.

(225) *Ibid.*, p. 48.

be considered in such a case that a State which has encouraged private actors to undertake operations harmful to third States has failed to fulfill its duty of care.

c) The State is responsible if it has recognized the actions of private actors as its own

According to Article 11 of the ILC "Articles on the Responsibility of States for Internationally Wrongful Acts":

> "Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own".

In international jurisprudence, the often cited example is the judgment of the ICJ in the *Case Concerning United States Diplomatic and Consular Staff in Tehran* (1980). In it, the Court clearly distinguished between the legal situations: the one that was created by the taking of hostages of the personnel of the United States Embassy, and that which was created by the decree of the Iranian State, which expressly approved such an action. As it concerns cyber security, an analogy could be drawn with the situation where a hack-back operation initially undertaken by a private acting company, is subsequently endorsed by the State itself.

d) The State is liable if it has breached its obligations of due diligence

This situation differs greatly from those described above. In the previously mentioned situations, certain circumstances make it possible to attribute the conduct of a private company to a State: it is considered that what the private company has done is an action of the State. If the act in question constitutes an internationally wrongful act, then the State has a duty to repair its harmful consequences.

On the other hand, in the present case, the act of the private company is not attributable to the State. The latter can be held liable to the extent only that it has not taken the necessary and required measures in order to prevent the harmful cross-border actions of a private company. Therefore, here, we find, in terms of responsibility, the consequences arising from a violation of the obligations set out above (Part I): "he who can, and does not prevent, sins".

Conclusion

Our analysis has shown that international law already includes many rules that can govern relations both between States and between States and private actors in the event of a cyber-attack.

We have shown the usefulness of the concept of cyber-diligence not only in order to prevent cyber-attacks, but also to act quickly to put an end to them. The duty of due diligence which States must exercise with regard to non-State actors operating from their territory (be them terrorist groups, cybercriminals, companies or mere hackers) derives directly from the obligation of any State "not to allow knowingly its territory to be used for acts contrary to the rights of other States".

We then examined the legal regime applicable to cyber-attacks by classifying the possible reactions. We have distinguished between reactions that are always permitted and other reactions that are permissible only if it can be established that a State has committed an "internationally wrongful act" by action or omission. We stressed the need for international cooperation in this area, beginning with the approach of the victim State to the State from which the cyber-attack originated, requesting its intervention against the perpetrators of the malicious acts in question. We have also warned against any "trivialization" of responses that are in principle violations of international law but are "excused" as circumstances precluding wrongfulness or responsibility. This applies both to "the state of necessity", the invocation of which is rarely accepted in practice by international courts and tribunals, and to countermeasures. The latter are, admittedly, authorized by international law as a response to a cyber-attack that violates international law and is attributed to a State, but it still remains in use "for lack of a better" means. In different areas "private justice" processes have given way to institutional procedures for judicial settlement of disputes and centralized enforcement mechanisms. Even though countermeasures remain an important means for States (but not for private actors) to respond to cyber-attacks, any trivialization or proliferation of these private justice processes that involve risks to the international order and, by definition, make the most of the most powerful, should be avoided to the biggest extent possible.

Finally, we have carried out a detailed study of the problems of "active cyber defense" and "hack-back" from the point of view of both international and comparative law. We have shown the many legal obstacles and risks involved in a hack-back operation unilaterally initiated by non-State actors. Private actors would therefore be better off investing in cyber hygiene and the implementation of good

safety practices, rather than trying to acquire offensive tools. If, nevertheless, they are victims of a cyber-attack, instead of launching a—technically and legally—hazardous hack-back, it would be better if they notified the State authorities of the attack and asked them to act, and also exercised their legal rights against the perpetrator of the cyber-attack, assuming that the perpetrator can be identified. States should act within the framework of international law (and especially human rights law) to enhance their proactive and reactive capabilities in order to avoid giving the impression that proper legal forms of reaction are either nonexistent or insufficient. Indeed, the impression of inadequate and inefficient government gatekeeping in the field of cyber-security serves the interests of those who call for cyber-vigilantism. States could, if needed, rely on private actors to conduct counter-attacks under certain circumstances, but this should be done under States' close control, with the risk of triggering their international responsibility.

Supporting that positive law provides solutions to different problems concerning the prevention of cyber-attacks and the reactions to them, does not mean in any way that States should disengage. As we have seen throughout this analysis, as new questions emerge, many gray areas remain in international law on fundamental issues. It is therefore imperative for the international community to cooperate closely in order to find answers to these questions by using all appropriate means available under international law in light of the circumstances: the adoption of new mandatory instruments; adoption of soft law texts; a dynamic and evolving interpretation of existing rules, etc.

After a period of relative inaction, over the recent years States have been exploring much more actively the problem of the security of the digital world in general and the issue of cyber-attacks, in particular. They negotiate and cooperate in different *fora* by increasing their initiatives in various international institutions: organizations with a universal vocation, mostly the UN (where, nevertheless, the GGE is for the time being an organ of restricted membership) and the International Telecommunication Union; or regional or closed organizations, such as the European Union, the Council of Europe, the OSCE, the OECD, the African Union, the Shanghai Cooperation Organization, NATO, the G20 and more others.

The problem, however, is that the proliferation of these initiatives in very diverse *fora* does not necessarily reflect good governance of cyber security. Some States have proposed the creation of a new centralized international organization specializing in cyber security, as a remedy for this dispersal. Yet, internationally, the era may no longer really be about the adoption of heavy structures that are born from the time-consuming negotiations of new constitutive treaties that could, probably, never be ratified by certain States. Nor does the era seem to be about the creation of new international organizations with a universal vocation endowed with normative powers. On the contrary, there is an increase in the number of "*fora*", "networks", "groups", "agencies", "committees" and other informal institutions which perhaps do not correspond to the classical definition of an international

organization, but which perform their functions efficiently. As one author emphasized: "Alternatives to international law are created through diverse intergovernmental coordinated actions that do not involve the setting up of international organizations that are subjects of international law".(226)

These observations seem to be particularly relevant in the area of cyber security. As things stand, it is difficult to see how States could engage in the creation of an international organization specializing in this field. It is also difficult to see how they could transfer to such an international institution powers in the field of cyber security, widely perceived to belong in the domain of "national security" and the "human" security of their populations, in short, of their quintessential governmental functions.

However, the need for better co-operation and rationalization of initiatives is being felt, as is the need to strengthen measures of confidence-building and assistance towards the many countries that are lagging behind in cyber security. The creation of a body capable of combining these actions, monitoring commitments but also initiating studies or even providing training and promoting good safety practices and a culture of cyber hygiene, seems indispensable. However, such a body could be effective only if it was flexible, open and without any normative powers that might raise the fears of many States.

Such a body should, of course, place great importance on private actors by providing for a multi-stakeholder composition or, at least, the creation of a formal mechanism for the integration of the private sector, such as a "Corporate Partnership Board". In this regard, it is worth recalling the recent proposal made by Microsoft to create such an informal body by adding to the G20 an ICT20—the 20 largest information and communications technology companies (ICT).(227) We think that it would be more effective (and more consistent with the interstate logic of international law—especially in areas directly affecting the national security of States) to create instead a flexible inter-governmental body enabling participation of large ICT and other companies, including representatives of SMEs, through a "Corporate Partnership Board". Such a multi-stakeholder international institution could allow governments, policy makers and businesses to work together in order to find effective solutions to the many current and future cyber security challenges.

---

(226) Eyal Benvenisti, "Substituting International Law", in "The Move from Institutions?", *American Society of International Law Proceedings*, Vol. 100, 2006, p. 289-290.

(227) See Microsoft, *Reducing conflict in an Internet-dependent world*, 2015, p. 18: "A third option could be leveraging existing frameworks, such as G20, and extending them to 20 leading ICT providers (ICT20). The G20 + ICT20 would have the advantage of being global in nature yet manageable in terms of size. An agreed-upon norms document between these stakeholders could represent a powerful contribution to a first cyber security norms baseline. It would also allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace. The drawback of such a group is its lack of truly global representation and its limited input from civil society. However, creating a G20 + ICT20 and top 20 nongovernmental organizations (NGO20) could improve collaboration and improve outcomes on norms. It will not be easy to establish criteria for selecting the ICT20 and NGO20, but it is well worth the effort to address this challenge".

CONTENTS