Effective Remedy in the Context of Hacking by Intelligence Services

Lori Roussey

2017

Abstract

This dissertation attempts to cast a legal perspective on the right to effective remedy in the context of intelligence services' recourse or acquisition of hacking tools. It attempts to provide elements and insights on public and private law principles regarding redress applied to the recourse to hacking tools by intelligence services, as well as the implications entailed by transfers of such tools to private persons or between services. Prior to obtaining damages or any form of compensation for his losses one first needs to be given legal minimum safeguards against hacking by intelligence services. For this reason, this paper will begin by the assessment of existing safeguards as well as potential redress avenues. This assessment shall then be completed by a reflection on what could lead to a satisfactory reparation.

This master thesis was written under the direction of judge Myriam Quéméner and attorney at law Brad Spitz, who I wish to express my gratitude for their guidance and support.

Contents

Introduction

On May 12 2017, numerous patients at the UK National Health Service (NHS) who needed to undergo medical operations did not get to see a surgeon. Their operations had been postponed. The cause? Connections between computers, X-ray scanners used to treat cancers, and other medical equipment had been interrupted and rendered inoperable. Communication channels within and between NHS trusts, such as emails and phone lines, were unavailable. Patient records were no longer accessible: they had been encrypted[1]. Instead, NHS staff saw a strange pop-up window replacing patient records, demanding a 300$ ransom per machine, accompanied by a spine-chilling warning:

> "Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service. [...] You only have 3 days to submit the payment. After that the price will be doubled. Also if you don't pay in 7 days, you won't be able to recover your files forever."

In few hours, 47 trusts had been hit. In the course of the week-end, 150 countries suffered computer infections[2].

At the root of this unprecedented and global mayhem is the United States of America's National Security Agency (NSA)[3]. For last summer, a group of hackers calling themselves the Shadow Brokers announced it had stolen "digital weapons" from US intelligence services, including the NSA. In March 2017, the Shadow Brokers started releasing several programs specially designed to take advantage of targeted vulnerabilities. Cybersecurity experts swiftly analysed

[1] Gayle D., Topping A., Sample I., Marsh S. and Dodd V., "NHS seeks to recover from global cyber-attack as security concerns resurface" *the Guardian* (London, 13 May 2017) https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack accessed 3 June 2017

[2] Campbell D., Siddique H., "Operations cancelled as Hunt accused of ignoring cyber-attack warnings" *the Guardian* (London, 15 May 2017) available athttps://www.theguardian.com/technology/2017/may/15/warning-of-nhs-cyber-attack-was-not-acted-on-cybersecurity accessed 3 June 2017

[3] See "The cyber-attacks on Friday appeared to be the first time a cyberweapon developed by the N.S.A., funded by American taxpayers and stolen by an adversary had been unleashed by cybercriminals against patients, hospitals, businesses, governments and ordinary citizens", from Sanger D. E. and Perlroth N.'s article, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool" *the New York Times* (New-York, 12 May 2017) available at https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html accessed 12 May 2017

the release and found it relatively harmless, as most of these "exploits" were outdated. The remainder of exploits, including a few Microsoft zero-days, were patched within days to prevent the vulnerabilities from being exploited. Among these Microsoft zero-days was the "EternalBlue" exploit.

It is the very same exploit, called WannaCrypt or WannaCry, that was included in the ransomware that hit NHS Trusts. Even two months after the patch, massive damages were caused, because computer systems had not been updated.

In the wake of these appalling events and enormous damages caused by exploits developed or acquired on the darkweb with tax-payers' money, a question is left unanswered. Who can victims turn to? How can victims get their damages repaired? If one causes someone else damages by their fault, they oblige themselves to repair it. This is a founding principle of private law around the globe. Yet, in the context of intelligence services hacking tools, obtaining legal redress remains highly uncertain for a private legal or natural person. This creates a cognitive dissonance once confronted to the UK's Government Communications Headquarters (GCHQ)'s admission that in 2013 20% of its reports contained information derived from hacking[4]. Hacking techniques may be deployed against "computers, servers, routers, laptops, mobile phones and other devices" such as smart devices connected to the internet.[5]

For this reason, this dissertation attempts to cast a legal perspective on the right to effective remedy in the context of intelligence services' recourse or acquisition of hacking tools.

Evolution of the verb to hack. Originally the verb "to hack" had no negative connotation whatsoever with breaking into a system. It meant to find one's way out of a given physical or nonphysical challenge. A hacker would be someone thinking outside of the box. In the digital field, such a person would then apply this thinking to software as well as hardware. Mindful of this semantic background, in the context of surveillance intelligence services often refer to synonyms of hacking, like Active Signal Intelligence (ActiveSIGINT) or Computer Network Exploitation (CNE) and Computer Network Attack (CNA)[6]. These expressions illustrate the essence of today's connotation of hacking: the act of voluntarily interfering with data or equipment.

The critical notion of exploit. Today's assertion of the term hacking associates it with the compromising of an equipment or software. This assertion goes hand in hand with the critical notion of exploit. According to the Internet Corporation for Assigned Names and Numbers (ICANN), "[t]he term exploit is commonly used to describe a software program that has been developed to attack an asset by taking advantage of a vulnerability". When referring to exploits cyber security

[4]Admission made before the British Investigatory Powers Tribunal (IPT). Bowcott O., "GCHQ accused of 'persistent' illegal hacking at security tribunal" *the Guardian* (London, 1 December 2015) available at https://www.theguardian.com/uk-news/2015/dec/01/gchq-accused-of-persistent-illegal-hacking-at-security-tribunal accessed 3 June 2017

[5]Intelligence and Security Committee, Parliament of the United Kingdom (12 March 2015) *Privacy and Security: A modern and transparent legal framework* at 13 and 14

[6]See the witness statement of Eric King in Privacy International's case against GCHQ's hacking, cases No. IPT 14/85/CH and No. IPT 14/120-126/CH (London, 5 Octobre 2015), page 4. Available at https://www.privacyinternational.org/sites/default/files/Witness_Statement_Of_Eric_King.pdf. To put it simply, CNE mines data from computers and networks, whereas CNA disrupts, damages or destroys data.

experts often mention zero-days. A zero-day is an exploit that has not yet been revealed to the public or the person in charge of fixing it. In that sense, zero-days enabling to take the control of a commonly used program or equipment, such as the Microsoft XP program exploited by WannaCrypt, are rare and have a tremendous harm potential. The interest of intelligence services in zero-days has allowed a grey market to flourish on the darkweb, as services' financial resources make it a highly lucrative activity. In her book *Countdown to zero-day*, former Wired journalist Kim Zetter cites the NSA budget for "covert purchases of software vulnerabilities" from private vendors: $25.1 million in 2013[7].

The notion of Intelligence services. Turning to the notion of intelligence services, this dissertation will only reflect on the recourse to hacking tools by intelligence gathering agencies, not law enforcement ones. Intelligence services may resort to hacking tools in a wide variety of cases, sometimes remotely related to "national security" per se, ranging from rendering a favour to another country[8], to sabotaging an other country's nuclear facilities[9], to spying on organisations such as the European Commission or the European Parliament[10].

Scope of this dissertation. This dissertation is not aimed at leading a general reflection on public international law. It attempts to provide elements and insights on public and private law principles regarding redress applied to the recourse to hacking tools by intelligence services, as well as the implications entailed by transfers of such tools to private persons or between services.

A strain on the rule of law. Hacking and the transfer of hacking tools are used in practice by intelligence services around the world. The use of such tools fortuitously happens to increasingly strain the rule of law, directly or because they nurture international criminality. This analysis leads to study national, regional and international law due to fragmentation as well as shared competences. This is illustrated by the EU's subsidiarity principle restricting Union competences[11] and its creation of new standards for all Members States to abide to on matters of surveillance.[12] Still, civil and criminal law principles will

[7]Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014) 519

[8]Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014) 456 - 463. Besides, given the strong financial and influence ties (with the US giving up £100m to GCHQ between 2010 and 2013) between the NSA and the GCHQ it seems difficult to imagine the GCHQ not rendering favours to the US, as outlined by *the Guardian* https://www.theguardian.com/world/interactive/2013/aug/01/gchq-spy-agency-nsa-edward-snowden#part-one (accessed 22 May 2017) and https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden (accessed 22 May 2017)

[9]See Sanger D. E., "Obama Order Sped Up Wave of Cyberattacks Against Iran" *the New York Times* (New York, 1 June 2012) available at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html accessed 2 May 2017

[10]In two of the Snowden documents the most important Belgian telecommunications operator, Belgacom, is said to have been attacked by GCHQ. One QCHQ 2011 presentation states: "Ultimate Goal - enable CNE access to BELGACOM Core GRX Routers" https://search.edwardsnowden.com/docs/MobileNetworksinMyNOCWorld2014-12-13nsadocs. Among Belgacom's customers are the European Commission and the European Parliament. For further detail see Gallagher R., "Operation Socialist The Inside Story of How British Spies Hacked Belgium's Largest Telco" *the Intercept* (13 December 2014). Available at https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

[11]Nuotio K., 'European Criminal Law' in Dubber M. D. and Hörnle T. (eds), *The Oxford Handbook of Criminal Law* (Oxford University Press, Oxford, 2014) 1115 - 1138

[12]These last three years the European Court of Justice has rendered bold rulings touching upon EU Member States, such as the *Schrems* (C-362/14) ECJ, g. ch., Oct. 6, 2015, the

be the leading themes of this dissertation, as it aims at indicating what could be paths for reflection and action on legal redress in the form of compensation, an international civil law principle, as well as reflecting on the need to obtain the prosecution of abuses harmful to the cohesion[13] of society, an international criminal law principle.

Various legal tools establish effective remedy requirements in their own words. Hence, the provision of a general perspective on this notion in the context of intelligence services' hacking seems necessary and will be twofold.

Existing and potential safeguards. Prior to obtaining damages or any form of compensation for his losses one first needs to be given legal minimum safeguards against hacking by intelligence services. For this reason, this paper will begin by the assessment of existing safeguards as well as potential redress avenues.

Providing satisfactory compensations. This assessment shall then be completed by a reflection on what could lead to a satisfactory reparation.

Why an analysis from an effective remedy perspective? The answer to this legitimate question can be condensed in the following statement by former Member of Parliament and former Defense Minister Hervé Morin, during the preparation of the French 2015 Intelligence Bill:

> "What I don't want is that in France, one day, in 2017 or in 2022, an arbitrary regime uses these monitoring tools without any control. Power is always associated with a servile court phenomenon, and I will always doubt the capacity of a central administration director to resist the pressure of a head of state."[14]

The provision of effective remedy, going hand in hand with fair reparation, enables the enshrinement of what constitutes the essence of the rule of law.

Digital Rights Ireland (C-293/12, C-594/12) ECJ, g. ch., Apr. 8, 2014 and the *Tele2 Sverige* (C-203/15, C-698/15) ECJ, g. ch., Dec. 21, 2016 rulings.

[13] "[U]tiles et nécessaires à la cohésion et à la survie de la communauté" (Free translation), J.-P. Delmas Saint-Hilaire, "Sans nécessité, loi pénale ne vaut" | Heurs et malheurs du principe de de légalité des délits et des peines (suite)" (2004), Politéia 113-118

[14] Free translation. Original quote in French: "Ce que je ne veux pas c'est qu'en France, un jour, en 2017 ou en 2022, un régime arbitraire utilise ces outils de surveillance sans aucun contrôle. Le pouvoir est toujours associé à un phénomène de cour servile, et je douterai toujours de la capacité d'un directeur d'administration centrale à résister à la pression d'un chef de l'Etat." Source: Follorou J., "Comment le renseignement se prépare à l'éventualité d'une victoire de Marine Le Pen", *Le Monde* (Paris, 10 April 2017) http://abonnes.lemonde.fr/societe/article/2017/04/10/comment-le-renseignement-se-prepare-a-l-eventualite-d-une-victoire-de-marine-le-pen_5108826_3224.html?h=12 accessed 10 April 2017

Remedy Avenues in Intelligence Services Hacking Related Cases

The provision of redress mechanisms is a fundamental principle in private law, to secure access to justice and effective remedy.

A general principle of Union law The right to access to effective remedy is based on Article 13[15] of the 1950 European Convention on Human Rights (ECHR hereafter). In the European Union, this right was reinforced by the *Johnston v. Chief Constable of the Royal Ulster Constabulary* (222/84) CJEC, May 15, 1986 judgment of 15 May 1986 by the Court of Justice, making the right to an effective remedy a general principle of Union law.

For legal and natural persons to benefit from an effective remedy in case of damage or any form of encroachment on their rights, remedy avenues must be provided to meet this effective remedy criterion.

Balancing sovereignty and human right principles Still, when it comes to surveillance programmes it seems that legal milestone principles are difficult to implement, as they might weaken State sovereignty. As a consequence, lawyers must ponder to help find a balance so that State sovereignty is not secured at the expense of basic human rights principles, such as the right of access to justice or the right to private life.

To that end, this first chapter shall focus on existing remedy avenues available to direct or indirect victims of hacking by intelligence services.

International standards and national frameworks. To grasp a better sense of the state of available redress avenues offered to victims of hacking related to intelligence services' activity let us get the gist of international conventional provisions and case-law on the matter. Secondly, one shall cast a closer look to national representative or particularly interesting legal frameworks surrounding hacking by the services.

[15] Article 13 (exerpt):
"Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

Potential unbattered remedy avenues After that, potential unexplored of future remedy avenues will be considered.

1) International Stipulations and case-law

To address the pressing issue of the resort to CNE by services, it is of foremost importance to begin with an overview of the international framework applicable to guide the recourse to such techniques. Then this overview will be completed with the interpretation opted for by regional courts.

A) International Stipulations on Effective Remedy and Hacking by Intelligence Services

First, this chapter shall introduce the relevant legal framework applying to the effective remedy criterion in international and regional laws. This presentation will be followed by the overview of the legal framework applicable in case of CNE and the exchange of CNE tools.

The Effective Remedy Criterium in International and Regional Law

From a United Nations (UN) Perspective

The effective remedy principle is enshrined in the Universal Declaration of Human Rights (UDHR) of 1948[16] and in the 2005 Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law[17]. The latter are of foremost interest as they go exhaustively in details. The UN General Assembly opens its 60/147 Resolution adopting the Basic Principles and Guidelines on remedy and reparation by recommending that:

> "States take the Basic Principles and Guidelines into account, promote respect thereof and bring them to the attention of members of the executive bodies of government, in particular law enforcement officials and military and security forces [...]."

This recommendation's wording is circumstantial to introduce this study of intelligence services' handling of highly intrusive intelligence techniques.

Article I(2) of the Guidelines further provides that states shall adopt "appropriate and effective legislative and administrative procedures and other appropriate measures that provide fair, effective and prompt access to justice" and concretely set up "available adequate, effective, prompt and appropriate remedies, including

[16] Article 8:
"Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law."

[17] Available at http://www.ohchr.org/EN/ProfessionalInterest/Pages/RemedyAndReparation.aspx

reparation"[18]. In addition, this article hints at the non-discrimination principle[19] in application of which states shall ensure "that their domestic law provides at least the same level of protection for victims as that required by their international obligations"[20].

Articles 3 and 11[21] reinforce states' duty to provide for "equal and effective access to justice" as well as "[a]dequate, effective and prompt reparation for harm suffered", and to do so "irrespective of who may ultimately be the bearer of responsibility for the violation".

The Guidelines go in depth regarding reparation by devoting nine of their articles to the matter, from Article 15 to 24. The obligation to repair victims shall be scrutinized in the second part of this paper.

It is noteworthy to stress that the Guidelines expressly put emphasis on the fact that its remedy and reparation stipulations shall not be derogated from[22].

The International Covenant on Civil and Political Rights (ICCPR)

[18] Article I(2):
"If they have not already done so, States shall, as required under international law, ensure that their domestic law is consistent with their international legal obligations by:
"(a) Incorporating norms of international human rights law and international humanitarian law into their domestic law, or otherwise implementing them in their domestic legal system;
"(b) Adopting appropriate and effective legislative and administrative procedures and other appropriate measures that provide fair, effective and prompt access to justice;
"(c) Making available adequate, effective, prompt and appropriate remedies, including reparation, as defined below;
"(d) Ensuring that their domestic law provides at least the same level of protection for victims as that required by their international obligations."

[19] Further dealt with at Article 25 of the Guidelines.

[20] Article I(2):
"If they have not already done so, States shall, as required under international law, ensure that their domestic law is consistent with their international legal obligations by:
"(a) Incorporating norms of international human rights law and international humanitarian law into their domestic law, or otherwise implementing them in their domestic legal system;
"(b) Adopting appropriate and effective legislative and administrative procedures and other appropriate measures that provide fair, effective and prompt access to justice;
"(c) Making available adequate, effective, prompt and appropriate remedies, including reparation, as defined below;
"(d) Ensuring that their domestic law provides at least the same level of protection for victims as that required by their international obligations."

[21] *Article 3 (excerpts):
"The obligation to respect, ensure respect for and implement international human rights law and international humanitarian law as provided for under the respective bodies of law, includes, inter alia, the duty to:
"(c) Provide those who claim to be victims of a human rights or humanitarian law violation with equal and effective access to justice, as described below, irrespective of who may ultimately be the bearer of responsibility for the violation;[...]"

*Article 11:
"Remedies for gross violations of international human rights law and serious violations of international humanitarian law include the victim's right to the following as provided for under international law:
"(a) Equal and effective access to justice;
"(b) Adequate, effective and prompt reparation for harm suffered;
"(c) Access to relevant information concerning violations and reparation mechanisms."

[22] Article 26:
"[I]t is understood that the present Basic Principles and Guidelines are without prejudice to the right to a remedy and reparation for victims of all violations of international human rights law and international humanitarian law."

The ICCPR[23] reinforces safeguards, providing that States must undertake to ensure that any person whose rights or freedoms are violated has an effective remedy, that such rights and freedoms shall be "determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and [shall] develop the possibilities of judicial remedy". In like manner, state parties must make certain "the competent authorities shall enforce such remedies when granted"[24]. In a nutshell, state Parties have a proactive obligation vis-à-vis potential victims to set up strong, enforceable and judicially reviewed remedy avenues.

Besides, Article 3(a) carries a welcome specification in the context of CNE by intelligence services, by highlighting in fine that effective remedy shall be assumed, "notwithstanding that the violation has been committed by persons acting in an official capacity"[25].

The European Convention on Human Rights (ECHR)

For its part, pursuant to its Article 13 the ECHR[26] ensures the protection of the right to an effective remedy. Unlike the ICCPR, the Convention strikes no distinction whether the remedy avenues shall be ensured before an administrative or a judicial authority ("national authority"). On the other hand the ECHR emphasizes in the very same wording as the ICCPR that effective remedy shall be assumed, "notwithstanding that the violation has been committed by persons acting in an official capacity"[27].

The EU Charter

By the same token, the EU Charter[28] affords similar guarantees at its Article 47 and associates the right to an effective remedy with the right to a fair trial

[23] Available at http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

[24] Article 3. Each State Party to the present Covenant undertakes:
"(a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
"(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;
"(c) To ensure that the competent authorities shall enforce such remedies when granted."

[25] Article 3. Each State Party to the present Covenant undertakes:
"(a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
"(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;
"(c) To ensure that the competent authorities shall enforce such remedies when granted."

[26] Available at http://www.echr.coe.int/Documents/Convention_ENG.pdf

[27] Article 13:
"Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

[28] Available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf

and effective access to justice[29], ensuring individuals the power to challenge authorities.

The African Charter on Human and Peoples' Rights (ACHPR)

To finish, though rudimentary worded, the ACHPR[30] provides in its turn for a form of effective remedy. Yet, this example remains anecdotal as its effectiveness criterion seems only relevant in terms of timeliness of the proceedings[31]. This is in no way satisfactory as it may hinder cases of blatant encroachment on the UN right to an effective remedy if they were for instance limited to the unreasonable cost of proceedings.

In conclusion, the right to an effective remedy is soundly enshrined in international and regional law as a building block allowing for other fundamental rights to thrive. It is regularly associated with the right to a fair trial, to access to justice and to reparation. Let us now ponder on the effective remedy principle from an CNE perspective.

CNE and Remedy Avenues in Case of Hacking Related Damages

CNE and Associated Redress Avenues in the Light of the Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime[32] is a particularly notable legal instrument as it is the first and most prominent international treaty on crimes committed via computer networks. This initiative emanates from the Council of Europe (CoE) but is open to any state outside of its Members. The Convention has three main goals:

- Harmonising domestic criminal substantive law on elements of offences and connected provisions in the area of cyber-crime;
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form and ;

[29] Article 47 (Right to an effective remedy and to a fair trial):
"Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.
"Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.
"Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice."

[30] Available at http://www.humanrights.se/wp-content/uploads/2012/01/African-Charter-on-Human-and-Peoples-Rights.pdf

[31] Article 50
"The Commission can only deal with a matter submitted to it after making sure that all local remedies, if they exist, have been ex- hausted, unless it is obvious to the Commission that the procedure of achieving these remedies would be unduly prolonged."

[32] The ETS No.185 Budapest Convention on Cybercrime has entered into force on 2004. The Convention is available at http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

- Setting up a fast and effective regime of international co-operation.[33]

As of today, it gathers 69 countries, ranging from the USA to Israel, Russia, Canada and the UK. In its preamble, the Budapest Convention expressly aims at enhancing harmonisation of criminal policies and providing cybersecurity around the globe.

CNE per se Regarding CNE per se, the Budapest Convention affords guaranties within Article 32[34], where it prevents any Party from penetrating a computer network situated on an other Party's territory without "the lawful and voluntary consent of the person who has the lawful authority to disclose the data". The wording of this article translates the ambition of the Convention. That is, fostering sound cooperation for a safer digital space.

The sharing of CNE tools and intelligence On the sharing of intelligence services hacking tools, Article 6[35] provides that any misuse of device shall be subject to "criminal offences under [...] domestic law, when committed intentionally and without right". Yet, the Convention accompanies this obligation with a possibility to derogate from this stipulation, safe "the sale, distribution or otherwise making available of [...] data by which the whole or any part of a computer system is capable of being accessed", that must always be provided for in the Party's statutes.

A Convention providing for no remedy avenues Regrettably, the Convention does not provide for particular remedy avenues, but refers to the rights protected by "the 1950 Council of Europe Convention for the Protection of Human Rights and

[33] See the Budapest Convention's Explanatory report, page 4. Available at https://rm.coe.int/16800cce5b

[34] Article 32 – Trans-border access to stored computer data with consent or where publicly available:

"A Party may, without the authorisation of another Party:
"a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

[35] Article 6 – Misuse of devices

"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 and without right: "- a. the production, sale, procurement for use, import, distribution or otherwise making available of:
"i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; "ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
"- b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
"2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. "3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article."

Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties". Its enforceability is hence considerably diminished. So far the Convention has no case-law interpreting its provisions.

UN on CNEs: State of Negotiations

Slow negotiations The UN has been gathering countries around the table to draw up a common instrument regarding CNEs for several years. A handful of countries, like China and Russia, have shown reservations on multiple aspects of the negotiations by fear of interference and, simultaneously, loss of their sovereignty on the matter. Tensions reside particularly on procedural aspects, hence directly impacting the right to an effective remedy and the right to reparation the UN attaches to it. Nevertheless, negotiations may resume, as these last months have seen some of the most reluctant countries invest themselves in the furtherance joint pondering to foster the elaboration of a shared playing-field.[36]

A rudimentary framework To conclude, even if the Budapest Convention of 2001 stands for a symbolic sign that most countries can gather and set out common rules they are willing to abide to, the current framework on CNEs remains rudimentary in the light of the aggressive policy[37] and the damages caused by unfettered recourse to CNE/CNA and CNE/CNA tools by intelligence services.

A framework entailed by fragmentation Despite the existence of the Budapest Convention, nowadays the legal framework applicable on matters related to CNEs is characterized by fragmentation and lack of respect of the legality principle, partly due to secrecy and disparate national dispositions. Countries' unwillingness to give away their sovereignty on the matter calls for a detailed analysis of the interpretation opted for by the Courts on matters of effective remedy in surveillance cases.

B) International Case-law on Effective Remedy Applied to Surveillance

Technical neutrality In the first place, it is of foremost importance for the reader to bear in mind that following the ECtHR *R.E. v. U.K.* ruling, whatever surveillance technique is resorted to "[. . .] the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference"(*R.E. v. U.K.* (62498/11) ECtHR, 4th sect., Oct. 25, 2015, point 130). Hence, analogies will be drawn throughout this chapter to read the European Courts' case-law in the light of hacking by intelligence services.

[36]Quéméner M., "Cybercriminalité" lessons, Faculty of Law of the Versailles University (2017)

[37]See the aforementioned Belgacom case. The GCHQ's attack on the most important Belgian telecommunications operator, Belgacom. Among Belgacom's customers are the European Commission and the European Parliament. For further detail see Gallagher R., "Operation Socialist | The Inside Story of How British Spies Hacked Belgium's Largest Telco" *the Intercept* (13 December 2014). Available at https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

European Court of Human Rights (ECtHR) Case-law

The right to an effective remedy as a mean to guarantee other fundamental rights As seen above, the European Convention on Human Rights' Article 13 stipulates that "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity." In that sense, the Court considers that "[a]rticle 13 of the Convention guarantees the availability at national level of a remedy to enforce the substance of the Convention rights and freedoms in whatever form they are secured in the domestic legal order. The effect of this Article is thus to require the provision of a domestic remedy allowing the competent national authority both to deal with an "arguable complaint" under the Convention and to grant appropriate relief." (*Souza Ribeiro v. France* (22689/07) ECtHR, g. ch., Dec. 13, 2012, para. 78). Put simply, the right to an effective remedy is a mean to guarantee the protection of other fundamental rights found in the Convention from encroachment, such as the right to privacy.

Secret surveillance's mere existence as a interference Besides, the ECtHR has relentlessly made clear its appreciation of what legitimate surveillance consists of. "[T]he mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied" (*Liberty v. UK* (58243/00) ECtHR, 4th sect., Jul. 1, 2008, para. 56), implying that this sole factual possibility "amounts in itself to an interference" of the right to privacy. Furthermore the Court stressed there is no need to provide evidence that a person "has been subject to a concrete measure of surveillance" (*Klass and others v. Germany* (5029/71) ECtHR, Plen., Sep. 6, 1978, para. 37-38; see also *Weber v. Germany* (54934/00) ECtHR, 3rd sect., Jun. 20, 2006, para. 78).

Secret surveillance as an acute threat to redress avenues This general position of the Court is further confirmed by its all-encompassing wording of the acute threat posed by secret surveillance to redress avenues in this *Klass* case, where it held that "where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 (art. 8) could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 (art. 8), or even to be deprived of the right granted by that Article (art. 8), without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions." (*Klass and others v. Germany* (5029/71) ECtHR, Plen., Sep. 6, 1978, para. 36).

Secret surveillance shall not be judicially unchallengeable In the eyes of the ECtHR it is critical "to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court" (*Kennedy v. the United Kingdom* (26839/05) ECtHR, 4th sect., May 18, 2010, para. 124).

Effectiveness to be assessed in concreto This positioning of the Court is consistent throughout time, as it starkly averred in *Pruteanu v. Romania* that in any system of surveillance, adequate and effective safeguards must be provided against abuse.

The Court went as far as to specify that the effectivity of the safeguards was to be assessed, inter alia, on the kind of remedy avenues provided by the national law. In addition, the Court found that Romania should have provided rulings proving that the domestic effective avenues put in place were effective in practice (*Pruteanu v. Romania* (30181/05) ECtHR, 3rd sect., Feb. 3, 2015, para. 48, 55).

To conclude, in its case-law the European human rights jurisdiction takes a clear stand on secret surveillance. National legal frameworks must have effective remedy avenues in place for a surveillance programme to be deemed lawful. Regrettably, the scarcity of its guidance on what such remedy avenues could be leave room for interpretation and discretion, even though the assessment in concreto is a robust safeguard.

European Court of Justice (ECJ) Case-law

The ECJ to take the path of the ECtHR Even if the European Union's origins are rooted in commercial harmonisation, since the Snowden revelations of 2013, the European Court of Justice (ECJ) has delivered landmark rulings on surveillance programmes. As a matter of fact, the Union is increasingly following the ECtHR's path in drawing clear fundamental safeguards for EU citizens.

Since the enshrinement of the effective remedy principle as a general EU law principle with the *Les Verts v Parliament* (*Les Verts* (294/83) CJEC, Apr. 23, 1986, para 23) and the *Johnston* (*Johnston v. Chief Constable of the Royal Ulster Constabulary* (222/84) CJEC, May 15, 1986, para 18 and 19) cases, it has not been extensively interpreted by judges.

Following the in concreto approach? Nevertheless, before proceeding to the application of this principle to surveillance measures, a light shall be shone on the opinion[38] of the Advocate General in the Aarhus case(*Aarhus* (C-243/15) ECJ, g. ch., Nov. 8, 2016). In her Opinion, Mme Kokott chose to assert whether the national rules at hand were making it "impossible or excessively difficult to exercise rights conferred by EU law (principle of effectiveness)" (para 98), since this very principle "gives effect to Article 47 of the Charter" (para 99). This methodical approach of what constitutes effectiveness in domestic law appears optimal.

The landmark Schrems ruling Mme Kokott's Opinion was rendered in an environmental law context but it mirrors the choice made by the ECJ in 2015 when judges were faced with an Austrian citizen deprived from any remedy avenue to question the American surveillance operated on his personal data sent oversea in accordance with the Safe Harbor decision of 2000. Indeed, judges opted to interpret Article 47 of the Charter in that it "requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial scrutiny designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law" (*Schrems* (C-362/14) ECJ, g. ch., Oct. 6, 2015 para 95).

[38] Advocate General Kokott's opinion is available here http://curia.europa.eu/juris/document/document.jsf?text=&docid=181062&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=30614 (ECLI:EU:C:2016:49).

Effective judicial scrutiny inherent in the existence of the rule of law UE case-law, in contrast with the ECtHR, has taken some time to be confronted with surveillance techniques as it is originally not meant to have jurisdiction on national security matters. Still, with commerce becoming increasingly intertwined with surveillance scandals, it was foreseeable that the ECJ would someday find itself competent when a particularly interfering case would be referred before it. With its landmark *Schrems* ruling the Court of Luxembourg has audibly averred that a prerequisite for a surveillance programme to be legitimate under the rule of law is the provision of an effective remedy, and in particular, an effective judicial review.

As seen supra, the acception of the effective remedy notion and the interpretation attached to it by European Courts in surveillance cases have been anchored in the last few years. It shall now be confronted to a national framework as, despite the ratification of the Budapest Convention, countries' statutes regarding CNEs and the provision of an effective remedy thereof remain fragmented, primarily for sovereignty reasons.

It was found by the expert study lead in response to a request of the European Parliament's LIBE Committee[39] that in practice the judiciary's office is considerably hindered in guaranteeing the rights of the defence in national security related cases. These observations stemmed from the close analysis of both national legal frameworks regarding the services' activities and techniques as well as the unravelling of proceedings before Courts and oversight bodies. In order to illustrate and reflect on the report's conclusions, French national provisions on intelligence services' hacking and the remedy avenues provided by thereto shall be scurinized extensively.

2) Case Study: France, Between Autonomy and Heteronomy

France's case is one of particular interest as it is a historically strong state, economics and intelligence-wise. While it has inextricably developed a sharp sense of sovereignty, it is also an EU Member State, a Member of the Council of Europe and a Budapest Convention ratifier. In that sense it may be said as between autonomy and heteronomy. Heteronomy is the opposite of autonomy, where an entity lives and interacts with the outer world according to its very own nature and values. In this context, being heteronomous means to thrive according to legal norms enshrined by superior levels of authority. Indeed, France's legal norms encompass primary international and European law as well as the fundamental rights found and enforced by supranational courts and the guidance emanating from organisations such as the UN. For these reasons this country will be extensively studied as regards its legal framework, its remedy avenues and the effectivity of the right to effective remedy in practice.

[39]Study requested by the LIBE committee of the European Parliament, "National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges" (2014), 67. Available at http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf

A) French Legal Framework Pertaining to CNEs and Effective Remedy

Hacking by Intelligence Services

The French Penal Code The French relevant provisions on CNEs and CNAs per se can be found at Article L853-2[40] of the ISC and in Chapter III[41] of the Penal Code on unauthorised access to automated data processing systems, at Articles 323-1, 323-2 and 323-3[42].

The Intelligence Act Article L853-2 allows services to resort to techniques such a keyloggers recording every key pressed by the victim, or tools similar to the ones used by the GCHQ like Flame to take computer screenshots[43], Captivatedaudience to hijack computer microphones[44], Gumfish to activate computer webcams and take pictures[45], or Tracker Smurf activating the GPS tracker of a phone, even if it is switched off[46].

[40] Article L853-2:

"I.- In accordance with Chapter I of Part II of this book, when intelligence cannot be collected by any other legally authorised mean, usage of technical devices may be authorised as to allow:

"1. To access computer data stored in a computer system, to collect, retain and transmit it;

"2. To access computer data, to collect, retain and transmit it, as it is displayed onscreen for the user of an automated data processing system, as it is entered by keystrokes or as received and transmitted by audiovisual peripheral devices.

"II.- By derogation from Article L. 821-4, authorisation to deploy techniques mentioned in 1 of I of the present Article is issued for a maximum period of thirty days and the one mentioned in paragraph 2 of the same I for a maximum period of two months. Authorisation is renewable under the same conditions of duration." [*Note: The two Intelligence Acts of 2015 have not been officially translated. This is the unofficial translation made by the volunteers of French organisation La Quadrature du Net of the entire 8th Book of France's Internal Security Code (ISC), where most of the Laws' provisions have been codified. This translation is available at https://wiki.laquadrature.net/French_Intelligence_Laws*]

[41] Chapter III of the second Title of the Penal Code's third Book.

[42] Official translation:

"Article 323-1 (excerpts):

"Fraudulently accessing or remaining within all or part of an automated data processing system is punished by two year's imprisonment and a fine of €60,000.

"Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is three years' imprisonment and a fine of €100,000.

"Article 323-2 (excerpts):

"Obstructing or interfering with the functioning of an automated data processing system is punished by five years' imprisonment and a fine of €150,000.

"Article 323-3 (excerpts):

"The fraudulent introduction of data into an automated data processing system, [extraction, retention, reproduction transmission,] or the fraudulent deletion or modification of the data that it contains is punished by five years' imprisonment and a fine of €150,000."

"*Note of the author: The words in bracket in Article 323-3 have been added by the law n° 2014-1353 of 13 November 2014 and have not yet been officially translated.*

[43] The Flame malware takes screenshots of whatever is on the screen every 15 seconds when it detects that a communication application is in use. If it is not, it will only take screenshots every 60 seconds. See Zetter, K. "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers" *Wired* (San Francisco, 28 May 2012). Available at http://www.wired.com/2012/05/flame/ accessed 13 June 2017

[44] See Greenwald, G. and Gallagher, R. "How The NSA Plans To Infect 'Millions' Of Computers" *the Intercept* (12 March 2014). Available at <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ accessed 13 June 2017

[45] Ibid.

[46] See Ball, J. "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data" *the Guardian* (London, 28 January 2014). Available

The following article, L853-3, provides for circumstances when services need to penetrate a private space (vehicle or private location) to place, use of remove devices needed to resort to techniques specified at Article L853-2.

The wide material scope of article 323-8 Articles of the Penal Code go further in-depth. They notably include in the definition of hacking the exploitation of computer networks by way of, inter alia, accessing, remaining, modifying, interfering, extracting or transmitting data. This definition is completed by Article 323-8[47], setting extremely vague grounds to implement surveillance measures whenever they are meant to "ensure the protection of the fundamental interests of the Nation [...] outside the national territory". It is apparent from the Code that these measures may be implemented from within the national territory as well as from outside of it.

Implications of article 323-8 Interestingly, Articles 323-1, 323-2 and 323-3 do not mention that the CNEs they define may be resorted to by intelligence services. It is simply implied by Article 323-8 that carries a derogation for services when such CNEs are meant to protect France's interests outside its borders.

Transfers of CNE and CNA Tools

Legitimate transfers Regarding transfers of CNE and CNA data and programs the aforementioned Article 323-3 defines it but again, without allowing services to resort to it. Their usage of this technique is merely implied by Article 323-8. Transfers within or across the French border are further depicted at Article 323-3-1[48]. This article is the only one of the Chapter on Unauthorised access to automated data processing systems that provides for the eventuality that such transfers may be done with a legitimate motive. This raises two observations.

Firstly, it is bitterly regrettable that Article 323-3-1 provides for "legitimate motive" instead of "lawful motive". This wording is neither future-proof nor a dispassionate democratic illustration that the French society is willing to set out a clear legal framework of its recourse to intelligence techniques. The current formulation of Article 323-3-1 may give leeway for secrete interpretations of this article to be developed in the future.

Secondly, a bold interpretation of the derogation created by 323-8 could lead one to use the liberty given by this article introduced in 2015 to justify that to

---

at: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data accessed 13 June 2017. To go further, see the expert report of Eric King in Privacy International's case against GCHQ's hacking. Available at https://www.privacyinternational.org/sites/default/files/Witness_Statement_Of_Eric_King.pdf

[47] Article 323-8 (amendment of 2015 - translation by the author as no official translation is available):

"This chapter shall not apply to measures implemented by the authorized agents of the State services designated by the Prime Minister's Order from among the specialized intelligence services mentioned in Article L. 811-2 of the Code of Civil Procedure. To ensure the protection of the fundamental interests of the Nation mentioned in Article L. 811-3 of the same Code outside the national territory."

[48] Article 323-3-1 (Amendment of 1992):

"A person who, without legitimate motive, imports, possesses, offers, transfers or makes available any equipment, instrument, computer program or information created or specially adapted to commit one or more of the offences prohibited by Articles 323-1 to 323-3 [note: articles defining intrusions and other hacking methods], is punished by the penalties prescribed for the offence itself, or the one that carries the heaviest penalty."

exchange hacking tools Intelligence services would not always have to invoke France's interest. Such transfers might also be done to render a favour to an ally service, taking the example of the Stuxnet hacking tool developed by the NSA together with the Israeli Mossad. In her book, intelligence services expert journalist Kim Zetter stresses that the US have chosen to develop and transfer this tool with Israel to render a favour to the later[49].

Plausible breach of the legality principle Again, Article 323-8 creates a broad derogation whenever transfers within as well as outside the country are operated by French Intelligence services in the name of the protection of French interests outside France's territory. Such provision affords the risk of being deemed in breach of the criminal law principle of legality[50].

No French oversight for intelligence "provided by foreign agencies" Last but not least, Article L. 833-2[51] of the Internal Security Code (CSI) sets out the missions of the French Intelligence oversight body, the Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR)[52]. The fourth point of this article expressly provides that "elements provided by foreign agencies" shall not enter the material scope of its oversight. As seen supra with the Stuxnet example, hacking tools are and may very well continue to be passed on among national services.

Therefore, today French intelligence services have numerous means to avoid accountability or oversight. A considerable impediment for one seeking remedy avenues. These shall now be studied.

Remedy Avenues

As already mentioned, the French Intelligence Act of 2015 have predominantly been codified in the eighth Book of the Internal Security Code (ISC). So were the special remedy avenues for litigation against intelligence services' techniques, that can be found at the fourth Title of the eighth Book of the Code.

General Competence of the Council of State

[49] Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014) 456 - 463, op. cit.

[50] Even though the legality principle is at the very heart of French criminal law. See Scalia D., 'Du principe de légalité des peines en droit international pénal' (Bruylant, Brussels, 2011) 304 - 305

[51] Article L. 833-2: To accomplish its mission, the Commission:

"[. . .]

"4. May request from the Prime Minister any elements necessary for the accomplishment of its missions, including when the deployed intelligence-gathering technique has neither been requested nor authorised or does not meet the traceability requirements, except for elements provided by foreign agencies or by international bodies or that may give knowledge to the Commission, directly or indirectly, of the identity of the sources of the specialised intelligence services;"

"[*Note: The two Intelligence Acts of 2015 have not been officially translated. This is the unofficial translation made by the volunteers of French organisation La Quadrature du Net of the entire 8th Book of France's Internal Security Code (ISC), where most of the Intelligence Acts' provisions have been codified. Translation is available at https://wiki.laquadrature.net/French_Intelligence_Laws*]

[52] This acronym could be freely translated as the National commission for control of intelligence gathering techniques.

Pursuant to Article L801-1 ISC, the Council of State now has exclusive jurisdiction over such litigation.

Oversight by the Council of State Under this special venue, the Council of State may check: - Whether the use and implementation of an intelligence technique complies with Book VIII of the ISC (e.g. in terms of authorization by the Prime minister, intelligence data retention, etc.), and - Whether the processing of personal data in the context of a secret Government database made in the interest of State security complies with the French Act no. 78-17 of 6 January 1978.

Redress offered by the Council of State Regarding redress offered by the Council of State, it may cancel the authorisation to proceed to the surveillance and, potentially, order the destruction of unlawfully collected intelligence. Otherwise, if the Council deems the surveillance illegitimate it may order the rectification, update or deletion of data.[53]

Secrecy and the formation spécialisée The proceedings are made before a special court of the Council of State (called "formation spécialisée"). This special court of the Council of State is constituted of administrative judges subject to State secrecy clearance pursuant to Article L832-5. The proceedings are governed by specific rules modifying administrative justice procedure to underpin State secrecy. For instance, pursuant to Article R773-20 of the ISC, some of the evidence submitted to the court for analysis may not be disclosed to the other parties.

Proceedings Brought by a Person

Who may refer a case before the CNCTR Proceedings may be brought by any person - after having filed a complaint to the CNCTR -, or by the CNCTR itself, or the subject matter may be referred to in a preliminary way by any administrative or judicial judge in the context of an ongoing case, where the decision of the special court of the Council of State affects such case.

CNCTR, then Council of State Therefore, in theory, the 2015 Intelligence Act opens the possibility for any person to obtain a verification of the legality of intelligence techniques, without having to bring evidence or to demonstrate standing, by first filing a complaint to the CNCTR pursuant to Article L854-9 of the ISC[54], and then by filing a case before the special court of the Council of State Article L. 841-1[55].

[53] Pursuant to Article R773-26 of the ISC.

[54] Article L854-9 of the ISC (excerpt):

"On its own initiative or by request of any person wishing to verify that no surveillance measure is irregularly being performed against them, the Commission shall ensure that the measures implemented under this chapter meet the conditions that it specifies as well as those defined by the regulations made thereunder and the decisions and authorisations of the Prime Minister or his delegates. It shall notify the claimant that it has carried out the necessary checks, without confirming nor denying the deployment of surveillance measures."

[55] Article L841-1 of the ISC:

"Subject to provisions included in article L. 854-9 of this text, the Council of State is competent, under conditions laid down in chapter III bis of title VII of book VII of the administrative justice code, for requests concerning the deployment of intelligence-gathering techniques specified in title V of this book. Cases may be brought before the Council of State by:

The first step allows natural and legal persons to refer claims before the CNCTR so that it "verif[ies] that no surveillance measure is irregularly being directed against them".

The Council of State is not a judicial jurisdiction The second one is before the Council of State and stands for what could be compared to an appeal court as persons may only refer their case before it after the CNCTR has had a chance to verify their claims. Still, one point calls for specification. The appeal provided by the Intelligence Act before the Council of State is not a judicial remedy. Indeed, the Council of State is the top of the administrative French apparatus, not the judicial one. No special judicial review or remedy as been set up to deal with intelligence related claims.

To finish, as already mentioned the CNCTR remains free to examine a case on its own initiative, according to Article L. 854-9.

Redress offered by the CNCTR Redress offered by the CNCTR: - The oversight body will neither confirm nor deny the legitimacy of any possible surveillance; - If it deems the surveillance illegitimate it "may" issue non-binding "recommendations" to obtain from the relevant minister the termination of the surveillance and the deletion of the collected intelligence. - If the CNCTR deems the measures following its recommendations not satisfactory, its President of three of its members may bring the case before the Council of State.

The Flaws of the French Legal Framework Related to CNEs and Effective Remedy

The plausible violation of the Budapest Convention regarding hacking and the transfer of hacking tools

Plausible contravention of Budapest's article 6 The sixth article of the Budapest Convention of Cybercrime prevents countries from derogating to their obligation to set up a legal framework regarding the transfer of hacking tools. Yet precisely, as seen above, French provisions on the matter - Article 323-3 and 323-8 of the Penal Code as well as Article L. 833-2 of the Internal Security Code (ISC) - imply or infer at transfers of hacking tools without setting out a clear legal framework in order to provide accountability or oversight.

Plausible contravention of Budapest's article 32 By the same token, in order to harmonize and build up confidence between countries the Convention's Article 32 obliges services align with other countries' authorities before resorting to techniques such as hacking. Then again, French provisions above appear to be

"1. Any person wishing to ascertain that no intelligence practice is carried out improperly against them, after prior recourse to the procedure set out in article L. 833-4;

"2. The National Oversight Commission for Intelligence-Gathering Techniques, as established by the provisions in article L. 833-8. When a legal proceeding or dispute whose resolution depends upon the examination of the lawfulness of one or more intelligence gathering practices is brought before an administrative court or a judicial authority, it can, on its own initiative or upon request of one of the involved parties, refer to the Council of State for a preliminary ruling. The Council of State shall issue a decision within a month of the referral."

in contradiction with France's obligations towards other Parties to the main international law instrument pertaining hacking[56].

The Absence of Remedy Avenues Thereof

As it is inferred by Article L. 833-2 setting out the missions of the French intelligence oversight body, there is no remedy avenue for claimants fearing that a set of data or a hacking too transferred to French intelligence services by "foreign agencies". This has two consequences. For a start, this very provision is blatantly in breach of all France's obligations vis-à-vis the right to an effective remedy. On top of that, such a legal loophole incentivizes services to obtain questionable intelligence gathering hacking tools or data through other agencies. The High Commissioner for Human Rights report of 2014 sums these concerning points by stressing that "[a] State cannot avoid its human rights responsibilities simply by refraining from bringing those powers within the bounds of law. To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other."[57].

Moreover, the 2015 International Surveillance Act creates a derogatory regime where proceedings before the special court of the Council of State in matters of surveillance of so-called "international communications" may only be brought by the CNCTR, excluding any person or any judge.

No sanctions in case of abuse by the services In the same way, Article 323-8 of the French Penal Code poses a serious threat to the principle of legality, as well as it bypasses the fragile possibility that hacking and the transfer of hacking tools could be sanctioned in case of abuse by the services, when done to protect France's interests aboard. Yet, as hinted at, Article 323-8 is the only article of the Penal Code expressly referring to services, even if it were only to create a derogation of sanctions in case of abuse. It could be implicitly acknowledged that other articles do cover the services' activities. Nevertheless in the case of hacking and transfer of hacking tools no article provides for their sanction in case of abuse. A worthy detail considering the sacrosanct criminal law principle requiring that any wrongdoing shall not be sanctioned if it is not expressly associated with a sanction in the law. In the context of the Penal Code's article on hacking this translates itself into a blanket impunity for services' transfers of hacking tools or their resort to such tools to gather intelligence in case of abuse as well as an absence of criminal law remedy avenues.

A a consequence, potential claimants may not rest assured to have any remedy nor reparation if they are collateral victims or victims of abuse of hacking tools.

French framework in contravention with EU standards In short, under many aspects the French legal provisions pertaining hacking blatantly contravene European Courts' interpretation of the EU Charter and the European Convention

[56]To go further, see the Exegetes' brief (in French) on the matter, available at <to be published in July 2017>. If you wish to enter with them on the matter, write and email at this address: contact@exegetes.eu.org or visit their website <exegetes.eu.org>.

[57]See the annual report of the United Nations High Commissioner for Human Rights of the 30 June 2014, page 11. Available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc

on Human Rights, as well as international law, regarding the right to an effective remedy and the right to reparation.

B) Confronting Theory with Practice: Current Proceedings

Trying the 2015 Intelligence Act mechanisms Careful attention shall now be paid to proceedings brought in collaboration with "the Exegetes"[58] gives an insightful and concrete view of the state of proceedings linked to intelligence services activities in France. Although no proceedings relating to intelligence services in France are known to target hacking activities in particular, several proceedings brought through the remedy avenues created by the 2015 Intelligence Act shed light on the process.

Verifications Before the CNCTR

$M^{me}A$ The Exegetes volunteered to help a French citizen ("M$^{\text{me}}$ B… A…", hereafter M$^{\text{me}}$ A) put this in practice.

First, M$^{\text{me}}$ A referred a claim to the CNCTR, for it to proceed to all relevant checks to ensure "that no surveillance measure [had been or were still] irregularly being directed against [her]".

Surprising checks The claimant was asking the CNCTR to make sure she had not been subject to illegal international surveillance between 2008 and December 2015, a period of time during which she had had numerous contacts abroad. The claimant lodged her complaint to the CNCTR on November 2, 2015. Almost one month later, on November 23, the CNCTR answered with a letter asking for the numbers of all her phone lines to check (but made no specific reference to other means of communications such as Internet-based communications). The claimant answered with three different phone lines on December 22. Surprisingly, the CNCTR notified the claimant that it had proceeded with all relevant checks, in a letter dated December 23. Such delay appears particularly short for an administrative authority whose resources were deemed highly sufficient by its former Director[59].

In practice, the notification from the CNCTR shall mean that it was able, in less than 24 hours, to check with the DGSE[60] and with other intelligence services who may retain data resulting from the DGSE surveillance apparatus (there are currently 6 specialised intelligence services pursuant to Decree no. 2015-1185), and to write a letter to notify the claimant that it had proceeded with all checks all of this accomplished on the day before Christmas Eve.

[58] A working group of volunteers between three French non-profit organizations French Data Network, La Quadrature du Net, and the Federation of non-profit Internet access providers.

[59] Declaration of Mr. Delon to the French Senate on the 10 February 2016. Available at http://videos.senat.fr/video.166865_57d282f75660a. For further details, see Rees M. "Loi Renseignement : le cri d'alarme du surveillant des surveillants" *NextInpact* (FR) (Paris, 16 February 2016) https://www.nextinpact.com/news/98556-loi-renseignement-cri-d-alarme-surveillant-surveillants.htm. In his article, Rees observes that "Delon confesses with dignity: « We will have to process 40 000 requests yearly, which is considerable ». Meaning a total of 109 requests a day (365/365) or 4,6 requests an hour (24h/24) will have to be checked by the CNCTR.".

[60] French foreign intelligence services (acronym for the General Directorate for External Security).

No appeal available Second, M^{me} A. filed a suit before the Council of State relating to her complaint to the CNCTR. In its "Mme A." decision[61], the Council of State rejected the claim, stating that since the claim pertains to international surveillance, the claimant had no mean to appeal the CNCTR notification[62].

This portrays a gloomy insight of what the sole remedy avenue provided for by the Intelligence Act of 2015 comes down to in practice. Not only the oversight of eight years worth of communications with multiple countries was done with a rare expeditiousness, but when appealing to the Council of State, the latter found it had no jurisdiction to review the case.

Analogy in case of abuse of hacking tools This remedy avenue echoes the European courts' case-law by illustrating the difference between the mere provision of a remedy avenue and the setting up of mechanisms that may effectively be activated and lead to proper reparation. This experience of the Intelligence Act remedy avenue provides precious information on the plausible fate of a claimant's action in case of damages or abuse of CNE by the services.

A reckless treatment of sensitive rulings On a side note, the Exegetes' article also denounces that the French Council of State sent its decision to numerous journalists on its own initiative, without anonymising it beforehand[63]. M^{me} A was outraged by what she felt was a deep lack of respect for citizens who took the risk to expose their private life to the intelligence apparatus for the sake of the rule of law and a more democratic society.

Hacking victims should not be dealt with recklessly In the context of proceedings against use of hacking techniques, this could mean the reckless unveiling of hacked individuals or corporations, or the exposing of vulnerabilities, by the French top administrative jurisdiction to journalists. Such behaviour of the French administration would carry tremendous computer security threats for all computer users. This may be the sign that the handling of Intelligence and hacking related cases should be subject to strict official guidelines.

When No Remedy Avenue is Available

Another case led in collaboration with the Exegetes is worth mentioning to draw an analogy with remedy avenues available for victims of damages and/or abuse of hacking by the services.

---

[61]

1. Available at the Council of State's website http://www.conseil-etat.fr/content/download/74775/693991/version/1/file/CE_397623_19102016.anon_compl.pdf

[62] See the Exegetes' article on their experiences, "How to Check You Have Not Been Subject to Undue Surveillance" (Paris, soon to be published), available at https://exegetes.eu.org/en/how-to-check-you-have-not-been-subject-to-undue-surveillance/

[63] Which is interesting, since the Council of State has an obligation to anonymise its decisions to protect the private life of claimants. As it turns out, the decision was published anonymised. Versions of it were unilaterally sent to the press before it had been anonymised. This is a gross violation of someone's private life. Unfortunately, this lack of due care vis-à-vis the claimant's private life has had a chilling effect on the claimant, who decided not to lodge a complaint before the ECtHR.

The in 'T Veld claim This action opposes the Member of the European Parliament (MEP) Sophia in 't Veld to the French Intelligence apparatus[64]. As a MEP, Ms in 't Veld works between Brussels and Strasbourg, as well as in her country, the Netherlands. Therefore, her communications are inherently international. On 2 May 2016, she lodged a complaint before the CNCTR[65], asking it to conduct a check in order to make sure none of her communications had been unlawfully intercepted under France's international surveillance apparatus.

The two in 'T Veld cases In application of the remedy avenue presented supra, after turning to the CNCTR the European parliamentarian referred her case to the Council of State. Aware of the Constitutional Council's decision of November 2016[66] openly noting that the French legal framework offers no possibility for persons to go to a judge in case of international interceptions of communications, Ms in 't Veld and the Exegetes chose to bring two cases before the Council of State. One to appeal the CNCTR - absence of - notification, and one on the grounds that the French authority had exceeded its powers, through what is called a *recours pour excès de pouvoir* (REP) remedy.

Thinking outside the box: recourse to the REP The REP remedy stands for the ultimate safeguard of personal freedoms against the administration. It is supposed to always remain an available remedy for who deems his rights and freedoms violated by the French authority, whether or not a law provides for this remedy avenue. To put it simply, the second case was intended to prove the complete absence of remedy before French jurisdictions. Either the Council of State was recognising victims of international surveillance an ultimate remedy avenue in the REP, or it would enshrine the absence of remedy for potential victims of international surveillance. Either way, the Exegetes and MEP in 't Veld would obtain satisfaction as the first solution would provide France with a minimum remedy, even if non-judicial, or the Council of State would prove that France breaches its international and regional obligations to offer an effective remedy to possible victims of surveillance techniques.

This two-cases strategy chosen by the Exegetes and Ms in 't Veld shall be an inspiration for possible future hacking related cases. Indeed, apart from the Penal Code providing no remedy at all, the remedy instituted by the Intelligence Act before the CNCTR could be the only one available to direct victims of intelligence hacking. Yet, in the in 't Veld and the Mme A. cases this remedy avenue has proven to be of little use, if any. To remedy this tragic fact the Exegetes' creativity has the merit to have possibly paved the way for a new redress avenue. In other words, the REP procedure could very well be the last resort of every CNE abuse victim when no procedural remedy seems available.

Contravention with the Effective Remedy Standard

[64]The briefs submitted by MEP in 't Veld and the Exegetes are available at https://exegetes.eu.org/recours/verifcnctr/

[65]MEP in 't Veld's claim can be found on the second page of this document https://exegetes.eu.org/recours/verifcnctr/CNCTR/2016-05-02-Lettre%20CNCTR.pdf

[66]See recital 18 of *Décision relative à la Loi relative aux mesures de surveillance des communications électroniques internationales* (n° 2015-722) French Constitutional Council, Nov. 26, 2015, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-722-dc/decision-n-2015-722-dc-du-26-novembre-2015.146546.html

Lastly, the in 't Veld cases - like the Mme A. one - raise several procedural concerns regarding the right to an effective remedy.

Possible interference with the right to fair trial For a start, as seen supra, the UN expressly associates the notion of effective remedy to the fairness of trial. Yet, in 't Veld's attorney Me Hugo Roy might not be allowed to speak or stay in the Council's Chamber during "hearings"[67]. This breach of the adversarial principle may be interpreted as a gross encroachment on the right to a fair trial. Unlike the UK's security-cleared lawyers[68], France has no special attorneys who may have the right to attend hearings subject to State secrecy rules.

Moreover, the proceedings have lacked due process in several aspects.

First of all, Article R. 773-30 of the French Administrative Justice Code provides that if the CNCTR has not conducted its checks and answered to the claimant in a two month window following the date of the claimant's first letter, the later may bring a case before the Council of State at the end of a four month window after the claimant's original letter. In the in 't Veld cases the MEP's letter was sent to the CNCTR on 2 May 2016. With no answer from the CNCTR, the MEP had to wait until 2 September to lodge an appeal before the Council of State.

On the 3rd of September, the CNCTR had produced no answer. For this reason, the following days Ms in 't Veld lodged a complaint before the Council. On the 3rd of October Ms in 't Veld received an answer from the CNCTR dating back from 13 September. Surprisingly in their following exchanges with the administration, represented by the Prime Minister, the later does not seem to consider the oversight body's timeliness questionable[69].

Exceptionally short time to produce legal briefs In addition, when the MEP lodged her appeal before the Council of State, she was soon notified by a letter of the Council of State dating back of the 5th of October 2016. This letter warned her that unlike usual procedures leaving three months to the claimant between the introduction of the case and the production of her first legal brief, her defence brief was due one month from the date of the letter. Not only this delay could seem unfair in a case where there are no precedents, but more importantly, the shortening of the delay for an exceptionally complex case cannot be deemed reasonable. To top it all, it must be stressed that before the 9th of March 2017 MEP in 't Veld had no attorney to represent her. Meaning any legally unadvised citizen would have been severely strained in terms of procedure. These facts appear in no way aligned with the due process principle.

Pending preliminary ruling The 9th of March attorney Me Roy was chosen by the claimant to represent her before the Council of State. On the 14th of March he has sent to the Council a second brief in which he, inter alia, raised a question asking for an ECJ preliminary ruling on effective remedy grounds.

[67] Due to the monopoly on speaking held by Council Attorneys before the Council of State and because the cases, dealt with by Council's specialised Chamber oversighting national security questions, can be deemed to require that persons with no defence or national security clearance must leave the room.

[68] See Article 6 of the 2013 Justice and Security Act.

[69] In 'T Veld v. French Prime Minister, *Mémoire en réplique*, case No. 404013 (14 March 2017) pts 29 et seq. available at https://exegetes.eu.org/recours/verifcnctr/CEtat/2017-03-14-Replique-CSI-PremierMinistre.pdf accessed 20 May 2017

The in 't Veld cases are still pending. Ms in 't Veld had to produce her answer before the 23rt of March 2015, for a hearing initially envisaged in March. Yet, the hearing date has been postponed several times. These facts appear to indicate an encroachment on the effective remedy principle and a skewed equality of arms, to the disadvantage of a European citizen seeking to ensure she had not been subject to illegal surveillance.

The study of the pending in 't Veld cases provides us with concrete evidence that the current French legal framework is far from in line with basic procedural rights enshrined by European fundamental rights stipulations, let alone international applicable instruments.

There is little chance that a citizen victim of or seeking to ensure she has not been subject to illegal hacking would be guaranteed to experience more respectful proceedings. As a matter of fact, chances are it would be even more complicated as data obtained by way of hacking techniques could be easily obtained from an other countries' agency, preventing the CNCTR from conducting even the slightest legality or legitimacy check. Not to mention that intelligence services hacking is usually thought to leave no digital evidence.

Put together, France's framework and past or pending cases yield us with multiple grounds for concerns in terms of the availability of an effective remedy to potential victims of hacking by intelligence services.

To conclude, the legal framework of this chosen Budapest Convention ratifier seems to shows a lack of respect of the legality principle. For instance, the recourse to exchange of CNE and CNA tools between intelligence services, nationally as well as internationally, is absent of most national frameworks. Despite its dangerousness and its possible impact on every end-user's computer around the globe (see the Stuxnet worm, infra). On this mater France is an interesting exception, as it expressly refers to data shared by other countries' Intelligence services. Though it is worth stressing that this mention is made for the only purpose of derogating received data from the CNCTR's oversight. This derogation, while openly creating an incentive for services to ask favours of allies to provide them with somehow questionable intelligence, is a severe breach of the effective remedy principle since the French national administrative authority is hence deprived from the ability to pursue checks on behalf of claimants. By the same token, the French Penal Code carries a blanket impunity for agents recieving or transfering CNE tools "[t]o ensure the protection of the fundamental interests of the Nation [...] outside the national territory" (art. 323-8 CSI). While this provision stands for a critical breach of the Budapest Convention's Article 6, it must be underscored that other Parties to the Convention's silence on the matter does not imply they do not play along the same lines. On the contrary.

The French framework echoed the EU Parliament's findings This observation is echoed by the 2014 report on National Security and Secret Evidence in Legislation and before the Courts ordered by the civil liberties Committee the European Parliament (LIBE). This independent expert study found that EU Member States' current frameworks carry a clear risk that the executive and secret services may act arbitrarily, partly because of the recourse to the slack and too nebulously defined "national security" ground. The report additionally put

emphasis on transnational intelligence practices and cooperation, to stress their need to be brought into line with the ECJ and ECtHR rule of law standards. The expert also pointed out that "States secrets too often 'over-protect' the executive from proper accountability and oversight in cases of wrongdoing and fundamental rights interferences. [...] The reliance on intelligence materials is thus too often based on a presumption that governmental agencies are acting in good faith [...]." Leading the experts to conclude their report by stressing that the "increasing number of cases revealing unlawful practices by secret services and governments demonstrate the need for a more careful assessment by judicial authorities."[70]

3) Unbattered Redress Avenues

The very core of the notion of right bears with it the obligation to redress its violation. This is even more necessary in a context where it may be considerably intricate to hold services responsible for CNEs they have indirectly ordered. Indeed, French newspaper Liberation has shown that services do not hesitate to abuse skilled individuals by making promises they do not attend to keep in exchange of CNE services. In its article[71], Liberation shows the example of a gifted asylum seeker who hoped to become French. Intelligence services reached him to offer asylum in exchange of the CNE of a library where soon-to-be ISIS members where suspected to communicate via freely available computers. The young asylum seeker did his part of the bargain and obtained the needed evidence, but the services never reached him out again. This outsourcing of CNEs on private individuals, especially a non-European individual, make it next to impossible to use any specialised remedy avenue. For this reason, unbattered redress avenues shall be contemplated.

A) Data Protection

As EU case-law illustrates it, the question of hacking by the services is intertwined with the question of the protection of natural persons' private shpere. As a result, EU Data Protection law could provide with complementariy avenues in the newly adopted Privacy Shield decision or the 2016 General Data Protection Regulation (GDPR).

The Ombudsman Avenue Set Up by the Privacy Shield

Referral before the informal panel The Privacy Shield Implementing Decision[72] is meant to provide safeguards for the commercial transfer of personal data between

[70] Study requested by the LIBE committee of the European Parliament, "National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges" (2014) 66 – 67. Available at http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf

[71] See Escarnot J-M, 'Antiterrorisme : l'espion aux espoirs déçus' (Antiterrorism: the spy with dashed hopes) (2017), Libération http://www.liberation.fr/france/2017/02/16/antiterrorisme-l-espion-aux-espoirs-decus_1549029 accessed 17 February 2017

[72] Commission implementing decision no. 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, available at http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

the US and Europe. Among these safeguards it has enabled the European Data Protection Authorities (DPAs) to set up in 2017 a remedy avenue for individuals fearing to have been subject to unlawful surveillance. The undeniable strength of this mechanism resides in the possibility for any individuals to obtain a verification of the legality of intelligence techniques, without having to bring evidence or to demonstrate standing, by simply filing a complaint referred to an "Informal Panel" of national DPAs. This Panel would then be free to investigate or relay the complaint to the US authorised authorities[73].

Unfortunately, so far the potential of such avenue remains uncertain as the relief they could offer to victims is unsettled and, most importantly, the Privacy Shield may be struck down by the ECJ as it fails to comply with the findings made by the Grand Chamber in the *Schrems* (C-362/14) ECJ, g. ch., Oct. 6, 2015 ruling[74].

Potential Remedies Offered by the GDPR[75]

Likewise, the GDPR offers avenues to refer potential encroachments before an authority and, in fine, a judicial jurisdiction. The enforceability of GDPR avenues make then seem a most preferable solution to consider for a potential victim of abusive or damaging hacking by the services.

Obligation to compensate in the GDPR First, pursuant to article 82(1)[76] of the GDPR on the Right to Compensation and Liability, it the processor or the controller's responsibility to repair any material or non-material damage caused to a person - a data subject - as a result of an infringement of this Regulation. This particular provision shall be read in the light of article 32, laying down a positive duty for processors and controllers to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". In that sense, it could be interpreted that certain sets of data, due to their sensitivity, could be foreseeably be targeted by any country's intelligence service and hence require special security measures. To use the aforementioned case of Belgacom, the GDPR could possibly let a judge ground on article 32 its interpretation and analysis of the telecom operator's security measures implemented and conclude it has to provide additional security measures since it is the entry point to access EU institutions' staff communications.

The GDPR provides for effective judicial remedy Secondly, pursuant to article 78 and 79 of the GDPR natural persons may respectively seek "effective judicial remedy" against Supervisory authorities as well as processors or controllers.

In cases pertaining to direct or indirect hacking by the services French data subjects could for instance envisage bringing a case before a court against the

[73]For further details see the Article 29 Working Party (WP29) "Rules of Procedure for the "Informal Panel of EU DPAs" according to the EU-US Privacy Shield" (2017) available at http://www.documentcloud.org/documents/3472691-Article-29-WP-Privacy-Shield-Rules-of-Procedure.html

[74]See Tracol X., "EU–U.S. Privacy Shield: The saga continues", Computer Law & Security Review, volume 32 (2016) 775–777

[75]Please note that the GDPR will only enter into force 25 May 2018.

[76]Article 82(1):

"1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

French DPA on the ground that it should have sanctioned French authorities from contracting with Hacking team, the Italian hacking services provider[77].

In like manner, European data subjects could envisage to sue a controller if she could reasonably assume that the processor she had contracted with no longer presented the necessary technical securities to shield if from an plausible/expectable hack.

B) Civil Law

Aside from data protection law, the most promising avenue to enjoy an effective remedy could be through civil law.

The analysis of the French framework above allows to draw clear conclusions. As intelligence services agents shall not be held criminally liable for their hacks, services may still be held liable before civil law judges. Yet to pursue civil law avenues, a person would not only have to prove she has been a victim, but would additionally have to prove a causality link between the harm suffered and the services' hacking. This critical criterion might turn out to be an unreasonably cumbersome and unfavourable one in such a case.

Along with unpractical direct remedy avenues against services, one must ponder on indirect remedy avenues.

The Insurance Sector

Dangerous promises for insurers The insurance sector comes inevitably to mind. Insurance-wise there are two scenarios. Either the insurer is bound by contract to the end-user, or he is contractually bound to the service provider through which the attack has been carried out. As an instance, the AXA cyber insurance comprises the suppression of pieces of ransomware programs from their corporate clients' computers[78]. Yet what characterises zero-days is that no computer scientist has ever heard of such software vulnerability. It may take months for a digital forensic expert to spot and fix a zero-day, especially one obfuscated by expert teams of hackers financed by a nation-state. It seems unrealistic to assure the "suppression of ransomware programs" from clients' computers in a context of State sponsored cyberweapons. It equivalents to insuring corporations against shells at a time of war, on a territory that may be bombed any day.

Besides, cyberinsurers usually all cover ransomware - also referred to as cyberextortion. Nevertheless, in their contracts insurers usually specify they will only cover foreseeable attacks. Therefore, the main angle to benefit from their business liability is the one of negligence, hardly invokable in practice.

If they were to be silent on such foreseeable attacks, insurers could turn to the reassurance sector. Even if the chances for such contracts to attract buyers

[77] See Medium user Paraig O'Mara's analysis (at https://medium.com/@beyourownreason/revealed-the-true-extent-of-hacking-team-contacts-across-europe-dc04e5bdde2) of the HackingTeam email leaks of Wikileaks (at https://wikileaks.org/hackingteam/emails/?q=france&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult.

[78] See their offers online (FR) at https://entreprise.axa.fr/assurance-biens-entreprise/cyber-risques.html#panel2 (accessed 19 June 2017)

willing to be transferred the risk are tremendously slim[79] in a context where governments hold secret exploits of vulnerabilities breaking the security of most common computer devices.

These considerations beg the question: should the insurance sector be in charge of paying for the damages caused by the zero-days bought or discovered by governments with taxes?

The IT Security Sector

The security sector stands out on matters of liability. In Amalfitano's book[80], he argues that the tortious liability of heads of legal persons seems especially furture-proof on matters of risk and prevention, such as the security serctor providing services to companies or insurers. These private legal persons or their representatives must be aware of the risks born by the handling of certain data or equipments. Not acting in accordance should engage their tortious or their business liability.

Sophos and WannaCrypt. The tragic events known by NHS trusts in England are of particular interest. Yes UK politicians had chosen to free the NHS from its ties with Microsoft by not resuming the contract between the company and the British administration. In that sense, British politicians could be seen as negligent[81]. Yet their role is to act in accordance with their voters' will, not to be IT specialists. Yes, NHS Trusts' IT security provider, Sophos, had then to compose with servers whose software would rapidly be obsolete. Nonetheless, as the security provider of infrastructure dealing with "data concerning health"[82], Sophos should have relentlessly alerted authorities to pivot for a new software provider. Indeed, the company is in a position of warranty and control vis-à-vis third persons. Their clients recourse to their services because they cannot protect themselves independently due to their lack of education and know-how on the matter[83].

In that sense it could appear possible for victims to invoke the company's business liability, raising its plausible negligence.

[79] Pouillot P., Senior Underwriter, "Les conséquences et la nécessité d'être bien assuré : la relation entre le RSSI et les assurances", at the Cybersecurity: How to deal with cyberattacks conference of the AFDIT association (Paris, 25 November 2016)

[80] Book in which he reflects on his PhD thesis on legal person's liability.

[81] See Townsend M. and Doward J., "Cyber-attack sparks bitter political row over NHS spending" *the Guardian* (London, 14 May 2017) available at https://www.theguardian.com/technology/2017/may/13/cyber-attack-on-nhs-sparks-bitter-election-battle accessed 19 June 2017

[82] Pursuant to article 9 of the GDPR, "data concerning health" relates to not mere personal data, but a "special categor[y] [. . .] of personal data" deserving scrupulous caution.

[83] Amalfitano A., La responsabilité pénale des personnes morales en Europe | Une recherche pour la construction d'un modèle commun (L'Harmattan, Condé-sur-Noireau 2015) 148

Thoughts on Free and Open Software

A liable maintainance provider However, the NHS Trusts episode being intertwined with the debate on EU countries' dependency on Microsoft[84], it allows us to consider options from a remedy avenues perspective. A recurring fear regarding the private sector's reliance on free software is the impression that no liability could be invoked before a judge in case of harm. This fear is groundless. Yes, if end-users use the Linux Mint distribution based on Debian[85], they will not be able to invoke anybody's liability in case of harm, but by using a community-driven operating system at no charge one could hardly expect for more. Conversely, if a company relies on a particular operating system or software to conduct its business or has particular IT security needs, it may certainly afford to pay a maintainance provider. The difference being whether it chooses to turn to a free or a non-free software provider and/or maintainer. A free-software support provider example is the Oracle company.

No lock-in effect The advantage of free or open software providers and maintainers is the avoidance of "lock-in" effects. Typically in the WannaCrypt example, the difficulty for Trusts is that they have been running proprietary software preventing their IT teams to study their program or modify their functionalities. Worst, Trusts could not easily change their maintainance provider to find a cheaper one without having to run on a completely new server software. If the NHS had been running an open software they could have turned to a more competitive maintainance provider to make cuts, without switching to some new software. That way, the WannaCrypt attack would not have infected the hospitals' network, patients would not have suffered any harm and politicians would have made harmless cuts. In short, the recourse to open or free software is more future-proof than proprietary ones since their cost-effectiveness make them less subject to political budget cuts.

To sum up, with reserves on their effectiveness as none of these avenues have been tried to this day, data protection as well as civil law appear to provide for remedy avenues that could be experimented. To afford a strengthened protection to digital services users, and to rebuild their confidence, it must still be underlined that the legal person's liability remains to be harmonised. It is so EU-wide as well as in the entire world, in particular when it is associated with sectors carrying international stakes.[86] The IT security sector being the priority.

Conclusion:

Even if the right to an effective remedy is soundly provided for in international, regional law and in European jurisdictions' case-law, national laws remain fragmented and worst, do not implement either this human rights principle nor the Cybercrime Convention when it comes to intelligence services hacking. Unfortunately, impunity to hack or the failure of national legal systems to bring

[84] See Investigate Europe's article, "Why Europe's dependency on Microsoft is a huge security risk" (Internet, 13 May 2017) available at http://www.investigate-europe.eu/en/why-europes-dependency-on-microsoft-is-a-huge-security-risk/

[85] See the GNU/Linux Distribution Timeline 12.10, available at http://futurist.se/gldt/wp-content/uploads/12.10/gldt1210.png

[86] Amalfitano, op. cit.

to justice perpetrators or negligent actors[87] is a central hurdle to guaranteeing the protection of fundamental rights. As a matter of facts, as services may even be emboldened by the absence of legal consequences.

That being said, even if remedy avenues were to be available and access to judge was feasible, this does not suffice as a safeguard in case of abuse. As mentioned above, the UN and the ICCPR portray the effective remedy criterion as twofold. Effectiveness may only be deemed met if oversight and judicial reviews are available and reparations obtained in case of abuse are satisfactory. For this reason this paper shall now focus on compensations for victims, may they be direct or indirect.

[87] As they are often targeted and used by the services to carry out attacks.

Illusory Compensations for Victims of Services' Hacking or Hacking Tools

In criminal law, judges sanction culprits with punitive damages. These damages are meant to mend the harm brought to society as a whole[88]. Whereas in civil law judges aim to compensate the material injury or the non-pecuniary damage. Yet in the context of hacking the damages inflicted to society as a whole in terms of confidence in governments or the private sector are colossal. So is the encroachment on end-users' right to personal data protection and private life, or even physical equipment.

As mentioned above, the effective remedy notion finds its essence only if one mirrors it with the compensations obtained by victims at the end of the day. This calls for an overview of damages and potential compensations, as well as an objective reflection on how could satisfactory compensations be structurally ensured for victims. This implies to consider the due process principle in the perspective of compensating victims of state hacking. Before doing so, the very notion of "victim" shall be examined, in general international law as well as in the context of intelligence services hacking.

1) Damages and Losses Suffered

A) Typology of Victims

Definition of the term victim. The UN's Basic Principles and Guidelines on remedy and reparation define the notion of victim at articles 8 and 9[89]. This UN definition shall be the one referred to in this paper as it encompasses victims of

[88] Van Sliedregt E., "International criminal law" in Dubber M. D. and Hörnle T. (eds), *The Oxford Handbook of Criminal Law* (Oxford University Press, Oxford, 2014) 1139 - 1163

[89] Articles 8 and 9:

"8. For purposes of the present document, victims are persons who individually or collectively suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that constitute gross violations of international human rights law, or serious violations of international humanitarian law. Where appropriate, and in accordance with domestic law, the term "victim" also includes the immediate family or dependants of the direct victim and persons who have suffered harm in intervening to assist victims in distress or to prevent victimization.

mental harm, direct as well as indirect victims and it specifies that one does not need to be associated to a named perpetrator to be granted the status of victim.

Direct Victims

Countries. Countries are direct targets of cyberweapons comprising exploits. These weapons increasingly aim at critical infrastructure, like transportation, healthcare, telecommunications, energy grids or plants and financial services. The Stuxnet malicious software, or "malware", illustrates this. The NSA and the Mossad teamed together to attack Iran's nuclear facility of Natanz. The program's payload[90] was to take control of uranium enrichment centrifuges to make them spin to their point of failure, in order to generate physical damages to the facility. The long-term goal being to slow down the Iranian nuclear programme and to make the country incur unexpectedly heavy costs. An other illustration is the attack on Ukrainian power centers in 2015. This attack was the first one in history to take down an entire power grid[91].

Organisations. Like countries, organisations are direct targets of intelligence services hacking tools such as the Animal Farm's Tafalcou and Babar[92]. Every attack is scrupulous. Tafalcou would infect a computer network, and Babar would be sent to take profit of the infection and spy on governmental organisations and humanitarian organisations[93] between 2011 and 2013, as explained by the Kaspersky Lab[94]. The Animal Farm is or was a state group suspected by Canadian intelligence services to be French[95].

Businesses. Businesses can be an ideal entry point to reach other persons' communications. The aforementioned example of GCHQ's CNE of the Belgacom telecommunication operator illustrates this perfectly. In order to access EU institutions' staff communications the easiest way for intelligence services was to hack a point from where all communications had to transit. Internet Access or Service Providers are hence a prey of choice.

Individuals. Lastly, individuals are very often a direct target of intelligence services as they constitute the three categories above. Like businesses, they are an entry point. When the US and Israel were trying to infiltrate Natanz they had

"9. A person shall be considered a victim regardless of whether the perpetrator of the violation is identified, apprehended, prosecuted, or convicted and regardless of the familial relationship between the perpetrator and the victim."

[90]Whole purpose (of a given malware).

[91]Zetter K., "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" *Wired* (3 March 2016), available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ acessed 7 April 2017

[92]See Untersinger M., "« La Ferme des animaux », concepteur de logiciels espions depuis au moins 2009" *Le Monde* (Paris, 6 March 2015), available at http://www.lemonde.fr/pixels/article/2015/03/06/la-ferme-des-animaux-concepteurs-de-logiciels-espions-depuis-au-moins-2009_4588510_4408996.html

[93]Among other targets, such as journalists, corporations and activists.

[94]The Kaspersky lab is one of the world's most respected IT security company. It is equally famous for the precision of its malware analysis.

[95]Article by the research team of the Kaspersky Lab, "Animals in the APT Farm" (Russia, 6 March 2015), available at: https://securelist.com/animals-in-the-apt-farm/69114/. For further information see the European Union Agency for Network and Information Security (ENISA) member Paganini P.'s article "Dino Malware that targeting Iran belong to Animal Farm's arsenal" (Brussels, 1 July 2015), available at http://securityaffairs.co/wordpress/38204/cyber-crime/dino-malware-animal-farm.html

to primarily infect a programmer's computer as the Natanz facility was air gaped, that is to say a voluntarily standalone network not connected to the internet for IT security reasons. To infect the facility the services firstly had to spot who was in charge of software updates and then infect his personal computer, that would at some point be connected to a programmable logic controller (PLC)[96] or infect the PLCs via a usb-key used to transport updates[97].

Indirect Victims

Of all intelligence services CNE tools victims, the most numerous are the indirect ones.

Unpredictable enormous costs born by the private sector Businesses and community projects must be capable of gathering and spending - in utter urgency - thousands of costly man-hours patching vulnerabilities. Not regular vulnerabilities. Vulnerabilities so scarce, unknown and embedded in major brands' equipment that services invested millions to obtain, and associate them with detrimental exploits. Whenever an intelligence service's exploit is published online[98], businesses throughout the globe must work round the clock to understand and fix their products, or their client's security is put at great danger. These unpredictable exploit publications are impossible to take into account in a yearly budget and can be fatal to businesses as they necessitate considerable energy, time and money resources. Even if companies are not related to the IT sector they may be impacted, as it was the case for several factories of the car producer Renault during the WannaCrypt attack[99]. Private companies should not have to bear this cost nor the life and death urgency stress it casts on them, as it puts their very existence at stake. If services were to keep their hacking practices in the future, coupled with the inevitable overbidding spiral accompanying it, it is of utmost importance that we find legal ways to repair their consequential damages on companies, be they inflicted to property, non-pecuniary or lost incomes and benefits.

Individuals evenly struck indirectly by services' hacking tools. Individuals suffer extensive damages when they are the customers of affected companies or equipments, such as the users of the Microsoft products that had not updated their machinebefore the WannaCrypt attack. WannaCrypt also tremendously impacted the lives of all NHS patients when the worm infected the British Trusts. Emergency patients have even been redirected towards other hospitals, or their schedules were postponed to the following week. Ukrainians deprived from power in the heart of winter too were most probably consequential victims of intelligence services hacking. Finally, it is too rarely underlined that the Stuxnet worm had

[96] Piece of hardware controlling the industrial mechanism it is associated to. It can for instance turn a program on/off or change the speed. Siemens PLCs, as the ones used at Natanz, have a making number. Natanz's PLCs were directly aimed at by the (original) code of Stuxnet as their making numbers were integrated amid the code.

[97] See Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014) 222 - 226

[98] As it was the case when Wikileaks started publishing the CIA's hacking tools it had developed in secret leaks. Wikileaks, press release (7 March 2017) < https://wikileaks.org/ciav7p1/>

[99] Johnston C., Russell G., Levin S., Wong J. C. and Rawlinson K., "Disruption from cyber-attack to last for days, says NHS Digital – as it happened" *the Guardian* (London, 13 May 2017) available at https://www.theguardian.com/society/live/2017/may/12/england-hospitals-cyber-attack-nhs-live-updates accessed 15 May 2017

a response team at Natanz and there are theories that some nuclear scientists assassinated after the attack were members of this team[100]. If it is so, there were undeniably consequential victims of the launch of the intelligence service's Stuxnet hacking tool. With the assassination of civilians comes third-party damages suffered by the person's relatives. These non-pecuniary losses should all be accounted for too.

B) Observed Damages: a Striking Diversity of Damages Caused

With this variety of victims comes a variety of damages caused.

Damages Caused by the Launch of Cyberweapons by Intelligence Services or the Transfer of Sacking Tools by Services

The Stuxnet case. In the case of Stuxnet, damages suffered were twofold. On the one hand there was the wreaking havoc of Natanz's centrifuges, the plausible assassinations and threats[101] of scientists working to understand and fix the software the enrichment was relying on, and the third party damages suffered by relatives of victims. On the other hand were all the private sector companies that had to struggle against the malware after its second launch by Israel went wrong and it spread globally[102]. Plus their customers world-wide.

Damages Caused by the Stealth of Cyberweapons Developed by Intelligence Services

The WannaCrypt case. In the case of WannaCrypt the question of liability may be even more tedious as damages were caused by the stealth and the rewriting of malevolent programs with the NSA's EternalBlue piece of code. As mentioned above, damages have been extremely various, ranging from NHS emergency patients' having to dash to other hospitals or cancer patients having to wait few more days before their next X-ray treatment, to companies like FedEX who have seen their routine operations hampered by the virus[103]. Not to forget the millions of people throughout the world who chose to pay the ransom demanded by the malware in hope to see their files unencrypted.

As they keep on buying priceless zero-days on the darkweb and put enormous resources in developing stable types of malware, intelligence services will always be a target of choice. This observation incidentally begs for the recognition of victims' right to be compensated and to obtain damages, for the stealth of cyberweapons is not ready to end.

[100] See Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014) 593 and blog article "Dead nuclear scientist headed Iran's response team to Stuxnet" available at https://israelmatzav.blogspot.com/2010/12/dead-nuclear-scientist-headed-irans.html

[101] See Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014) 594

[102] See Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014) 596 - 617

[103] See Sanger D. E., Chan S. and Scott M., "Ransomware's Aftershocks Feared as U.S. Warns of Complexity" *the New York Times* (New York, 14 May 2017) available at https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html accessed 16 May 2017

2) Right to a Satisfactory Compensation

A) From a United Nations Perspective

The right to reparation as a human right principle and a component of the effective remedy notion. The aforementioned Principles and Guidelines of 2005 associate reparation to the principles of accountability, justice and the rule of law. Alongside this association, the UN enshrines this right as a building block of a strengthened protection of human rights throughout the globe. According to the stipulations of the Guidelines, victims must be afforded adequate, effective, full and prompt reparation, proportional to the gravity of the violation and harm they have suffered.

The Guidelines go in detail in their description of what the right to reparation entails. First, pursuant to article 15 of the Guidelines "a State shall provide reparation to victims for acts or omissions which can be attributed to the State". The expression "attributed to the State" is fortunate regarding hacking as the general observed trend is the recourse to State sponsored hacking. Article 15's wording appears future-proof as it allows for an interpretation encompassing damages or harm directly or indirectly inflicted.

As of harm and losses that might not be legally linkable to the services, such as the harm caused by the insertion of one of their zero-day exploit in the WannaCrypt malware, the Guidelines lay down a two steps mechanism. First, when a natural person, a legal person, or an other entity is found liable for reparation to a victim, she may be guaranteed reparation by the State. After that, the Guidelines expressly allow State parties to be compensated by the person or entity liable.

Besides, States ought to enforce the right to reparation, even if it was recognised by a foreign ruling, as long as it is recognised valid by an independent court.

Forms of reparation include - but are not limited to - "restitution, compensation, rehabilitation, satisfaction and guarantees of non-repetition". Every one of these notions is scrupulously defined from article 19 to 23 of the Guidelines. Of these definitions is it worth noting that victims must be guaranteed compensation for "economically assessable damage". While satisfaction implies inter alia the cessation of violations, the verification of facts, the public disclosure of the truth, public apologies, judicial and administrative sanctions and the inclusion of an accurate account of the violations[104].

B) From a Criminal and Civil Law Perspective

From a criminal law point of view, conduct considered harmful to society ought to be prohibited by statute and associated with sanctions[105]. Damages have a punitive value. Whereas from a civil law point of view reparation shall cover, and be restricted to, the very non-pecuniary losses or the damages inflicted to property in order to restore as far as possible the situation existing before the breach.

[104]See articles 15 to 23 of the UN Guidelines.

[105]Grotuis H., *De Jure Belli Ac Pacis* (51615), Book II, ch. XXI, para. II (transl. F. W. Kelsey c.s., 1964), 523

What distinguishes these two approaches the most in terms of redress is that the civil law principle allows by essence for much higher compensations. In addition, they intrinsically differ because international criminal law holds as a sacrosanct principle that no one may be punished for someone else's wrongdoings[106]. It is the opposite in civil law, hence the thriving of the insurance sector.

Yet in the case of computer network exploitation by intelligence services both perspectives seem relevant, as the reckless use or abuse of the ability to hack one natural and legal persons' systems has tremendously intrusive consequences. Consequences harmful to society as a whole, as well as often associated with property or non-pecuniary losses.

C) European Case-law

Article 41 of the ECHR provides that "[i]f the [ECtHR] Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

As seen above, European jurisdictions have rendered numerous rulings asserting that undue or unlawful surveillance represents too much of an encroachment on fundamental rights to remain unrepaired. Nonetheless, on multiple occasions the ECtHR has opted to issue no monetary compensation to plaintiffs coming before it with surveillance cases, only to deem that symbolic nominal damages were sufficient.

The Zakharov ruling As an instance in the *Zakharov* ruling, the "Court consider[ed] that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage caused to the applicant." For this reason this secret surveillance case intertwined with the recognition of a lack of effective remedy avenues in the respondent country was repaired by a mere finding that a violation had taken place and that the claimant's proved expenses would be reimbursed.

Likewise, in the *Gillan* ruling the Court sided with the British Government and decided that "the finding of a violation constitutes sufficient just satisfaction in the circumstances of the present case" (*Gillan v. the United Kingdom* (4158/05) ECtHR, 4th sect., Jan. 12, 2010, para. 94)

In the *Pruteanu* ruling the appellant was granted 4 500 € for his non-pecuniary losses, but this amount was pertaining to his status of attorney, whose communications with his client should not have been used as evidence in proceedings.

Rulings to adapt to today's technical context Although the Court's rulings are clear, resort to CNE and CNA by the services has never been the subject of its cases and services are increasingly using CNE and worst, are now often aiming at sabotaging physical equipment. Judicial jurisdictions are bound to allow for more substantial reparations, or the private sector will remain at the mercy of security failures of intelligence services around the globe. The WannaCrypt malware constitutes a perfect example, as the Shadow Brokers

[106] As an instance, this criminal law principle was deemed constitutionnal by Constitutionnal council decisions. See Cons. const., 13 March 2003, dec. n° 2003-467 DC, Rec, 211 and Cons. const., 25 Feb. 2010, dec. n° 2010-604 DC, Rec, para 70

stole the NSA exploit EternalBlue during summer 2016, published it in March 2017, and malicious hackers inserted it in a ransomware before throwing it on the internet. To continue with this example, its impact on civilians' confidence in their administrations, their hospitals, and their computers may never fully restore or worst, leave permanent trauma. Not to mention the enormous losses inflicted to legal persons. In this paradigm shift symbolic nominal damages may hardly be regarded as sufficient.

3) Towards Securing Satisfactory Reparations

This last chapter ambitions to participate to the current academic debate on the recourse to state hacking, by way of insights on paths that could lead to satisfactory reparations. To do so one would first have to sift through potentially available redress avenues to focus on the ones carrying the soundest chances to prove effective and to provide victims with relief. To finish by an overview of potential improvements available to due process conditions in secret surveillance related cases.

A) Which Redress Avenues to Choose and on What Grounds

As seen earlier, it seems there are or will soon be several potential remedy avenues available for cases related to intelligence services' resort to CNEs. Yet not all of them seem to lead to satisfactory reparations.

The Privacy Shield avenue shall not be prioritised To begin with, the Privacy Shield avenue before the Informal Panel, even if not yet available or experimented, might not prove satisfactory. It most certainly will offer an avenue to make one's voice heard by DPAs, but chances to obtain the cessation of violations by the US surveillance apparatus, a public apology or administrative or judicial sanctions seem improbable.

The GDPR offers sound promises The GDPR, pursuant to article 79, seems more likely to lead to reparations decided by a judge. This regulation's avenue remains to be experimented, but the enforceability on European legal persons makes no doubt as regulations are an EU law binding legislative act that must be applied in its entirety and its provisions may directly be invoked before national judges in Member States. Between actions against DPAs and actions against controllers or processors, the latter may be far more preferable as judges may be more inclined to grant pecuniary reliefs to victims.

Civil law avenues to prioritise In like manner, general domestic civil avenues against corporations possibly bear the most substantial chances of success in term of satisfactory reparation, for the same reasons. Especially if the claimant is a consumer and the respondent is an IT security company. Plus, civil law judges are generally more inclined than criminal law ones to award generous compensations to victims. That said, they should be associated with criminal law claims to maximise chance to see victims relieved.

In a nutshell, it is merely the avenues against corporations that may seem the most promising in terms of satisfactory reparations. Nevertheless, if a potential

victim was to seek for relief, no avenues should be left unbattered. One could rather say it is a matter of prioritisation, as no avenue should be left unexplored.

Yet as already highlighted, general international civil law imposes the provision of a strict causality link between the harm or losses suffered and a third-party's positive action, or lack of action. Prerequisite that could appear far too cumbersome in cases of hacking by the services, an intrusive surveillance technique that is not only secret, but meant to leave no evidence. As a result, the due process principle, when applied to hacking pertaining to intelligence services, shall encompass particular guarantees.

B) Honing Due Process Conditions

Possible victims of hacking must be granted particular procedural attention. This can be inferred from article 4 of the EU directive 2012/29/UE, providing that EU Members' must afford victims individualized attention "depending on the specific needs and personal circumstances of the victim and the type or nature of the crime". In cases pertaining to direct or indirect hacking by intelligence services, specific needs of victims could primarily encompass exceptional means devoted to investigations and digital forensic as well as substantially lightened standing criterion to assess harm. Yet to ensure due process in this type of cases prior safeguards must be secured as well.

Investigations: Crucial on Hacking Cases

Basic principles regarding evidence are hindered The expert report on the use of secrecy in proceeding in Europe concluded that "the reliance on intelligence materials is [...] too often based on a presumption that governmental agencies are acting in good faith"[107]. Particular attention should thus be paid to the fact that it is next to impossible for direct or indirect victims of hacking by the services to honour the basic civil law principle that who comes before a court pretending to have suffered a damage caused by a third party must prove it.

CNE and CNA tools meant to leave no evidence It is a fact, intelligence services develop hacking tools to hide the malware[108] they use to collect information. Mindful of this, it should be echoed with the declaration of Privacy International (PI) counsel Mr. Jaffey in the course of PI's legal action against GCHQ's hacking: "If state authorities are permitted to alter or impair the operation of a computer, the reliability and admissibility of such evidence will be called into question"[109]. This observation is in line with Article 14(1)[110] of the Budapest Convention and

[107] Study requested by the LIBE committee of the European Parliament, "National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges" (2014), 67. Available at http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf

[108] As the tool Paranoid Smurf developped by GCHQ and revealed by Snowden in 2013. Paranoid Smurf is a piece of code ensuring that all malware remain hidden. Source: Bowcott O., "GCHQ accused of 'persistent' illegal hacking at security tribunal" (2015) available at https://www.theguardian.com/uk-news/2015/dec/01/gchq-accused-of-persistent-illegal-hacking-at-security-tribunal

[109] Quote of Jaffey B. of PI, Bowcott O., "GCHQ accused of 'persistent' illegal hacking at security tribunal" (2015) available at https://www.theguardian.com/uk-news/2015/dec/01/gchq-accused-of-persistent-illegal-hacking-at-security-tribunal

[110]

reinforced by the conclusions of UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression's report in 2013. In his report, he denounces "[o]ffensive intrusion software such as Trojans, or mass interception capabilities, constitut[ing] such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. There are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings."[111] This last point has consistently been shone a light on by the French cybercriminal law advisor of the Interior Ministry, judge Quéméner[112] acknowledging that digital proofs are subject to acute questioning in courts. One cannot but fully agree with the fact that the reliability of proofs is a milestone of a fair trial. To reconcile this and fundamental rights, courts should enshrine a right to meticulous and methodical investigatio n of hacking complaints, in particular when they might pertain to intelligence services activity.

This way, more reliable evidence would underpin the parties' arguments and countries may find themselves less reluctant to uphold the adversarial principle in the context of surveillance-related legal actions. On top of that, the services' operations would tremendously gain in legitimacy in the public's eye.

Duty to investigate The concrete upholding of a right to particularly meticulous investigations when plausible victims seek remedy avenues is a duty for Parties. Indeed, pursuant to article 3(b) of the UN Basic Principles and Guidelines, States must "[i]nvestigate violations effectively, promptly, thoroughly and impartially and, where appropriate, take action against those allegedly responsible in accordance with domestic and international law. This duty is even reinforced by Article 4, that expressly provides that"States have the duty to investigate". Yet, it goes without saying that such investigations, to be deemed effective, ought to be associated with robust independence safeguards.

Investigations would enable to and should go hand in hand with the establishment of sanctions to companies providing, buying or praising the recourse to hacking tools. These sanctions would have to be fines indexed on the company's worldwide turnover, in analogy with the GDPR's rationale that sanctions shall now take into account globalisation of businesses. Hacking being a borderless calamity, a fund could be in charge of the management of the sums gathered with fines and be in charge of redistributing it among investigating teams of countries and (international) organisations and, by the same token, victims. This redistribution mechanism could allow for a sound and healthy competition among private and public sectors and would not prevent citizens of countries with lesser resources

"Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings."

[111]Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (2013) pt 62

[112]Quéméner M., "Cybercriminalité" lessons, Faculty of Law of the Versailles University (2017)

or different spending strategies from benefiting of the digital forensic provided to build a safer digital space. Lastly, for the sake of right to information as well as transparency, publication of sanctions could provide an effective incentive for companies not to engage in such activities.

Standing and Notification of Harm: a Prerequisite for a Satisfactory Compensation?

In order to secure access to remedies for victims, they must be given effective access to counsel. If the lack of evidences makes it unappealing for a private counsel of an organisation to provide them with legal advise, victims will be deprived from their right to bring their claims before a judge or an oversight body. Especially in the context of State hacking, where proceedings are particularly technical. For this reason, it is crucial that claimants be granted lighter standing prerequisites.

Knowing one's rights have been interfered with That said, victims of hacking equally need be aware of their damage or its source for their right to effective remedy to be safeguarded. To fulfill this condition, it is first and foremost necessary that they be given the chance to know if and when they have been subject to hacking. This is in line with the ECHR's interpretation opted for the judges in the *Klass versus Germany* case, where they held that "[t]he Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation."[113]. In the *Zakharov* case judges went further, by affirming that "The Court concludes [...] that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject." They even specify that "after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers"[114].

In other words, in light of the ECtHR case-law the shadow of a doubt regarding hacking by the services is no longer possible: notification requirements are necessary for a country to be deemed to comply with article 13 of the ECHR.

In that sense too, disclosures must be legally provided for, depending on the dangerousness and the time passed since the dossier is closed. By the same token, gagging orders shall be accompanied with the duty for services to let persons and legal persons participate to transparence reports after some time. This is critical to mend the public's distrust.

[113] *Klass and others v. Germany* (5029/71) ECtHR, Plen., Sep. 6, 1978, para. 36
[114] *Zakharov v. Russia* (47143/06) ECtHR, g. ch., Dec. 4, 2015, para. 298 and 234

Right to Information Earlier On

Knowing violations and remedy avenues exist Last but not least, pursuant to article 11(c) of the aforementioned UN Guidelines of 2005, States have an active duty to provide persons with "[a]ccess to relevant information concerning violations and reparation mechanisms". It is indeed necessary for one to be aware of his rights and their possible infringement to protect them. This goes hand in hand with being practically aware of means to redress such violations.

Conclusion

The basic effective remedy principle, even if robustly enshrined in international and regional law and case-law, can barely be said to be assured to direct or indirect victims of the recourse to hacking tools by intelligence services. It is understandable that the same criteria shall not apply mutatis mutandis to the intelligence sector. Yet today our societies are nowhere near an equilibrium between the effective and full reparation of victims and the collection of intelligence material by services. To strike such balance, legal frameworks should at a minimum, inter alia, inform populations on remedy avenues in case of possible violations, notify persons who have been subject to hacking and provide for the criminal sanction of agents in case of abuse of reckless recourse to hacking tools or their transfer. Legal frameworks should ensure flexible standing and evidence standard to possible victims as well, in conjunction with a guaranteed access to a judicial judge and strong digital investigation conditions in cases possibly related to intelligence hacking. Lastly, States must comply and enforce satisfactory reparations for victims.

That being said, for the sake of eased spying governments render all computer users vulnerable. The WannaCrypt episode proved it. Fortunately, the WannaCrypt incidents did not lead to deadly consequences. Yet, as Cambridge University professor Anderson puts it, "it is only a matter of time before CNE causes fatal accidents"[115]. Nowadays computers are embedded in devices that surround us and our loved ones round the clock. Devices on which our societies increasingly rely upon, even for the most critical infrastructure. As this trend shows no signs of slowing down, intelligence services' accumulation of computer vulnerabilities seems questionable for the least, if not completely irresponsible. As malware expert warned in the wake of the disclosure of NSA's hacking tools, the resort to such tools could inadvertently be undermining the security of the Internet.[116] Even if the services assure the public they "never carry out reckless and irresponsible CNE operations"[117], they will always be a target of choice for malevolent hackers, leading us all in a dangerous spiral where taxpayers' money is used to buy tools that threaten the security of the technologies increasingly pervading every aspect of their life. Lessons learned by the WannaCrypt incident lead but to one conclusion. Ideally, intelligence services should not resort to hacking tools. The prohibition of state hacking should go hand in hand with national laws imposing clear and precise purposes[118] firmly limiting access requests made by services to the private sector. To be legitimate, such requests must be subject to judicial approval.

[115]Bowcott O., "GCHQ accused of 'persistent' illegal hacking at security tribunal" (2015) available at https://www.theguardian.com/uk-news/2015/dec/01/gchq-accused-of-persistent-illegal-hacking-at-security-tribunal

[116]Hypponen M. is an expert in malware who serves as chief research officer at the Finnish security firm F-Secure. See See Gallagher, R. and Greenwald, G. (12 March 2014) "How The NSA Plans To Infect 'Millions' Of Computers, The Intercept. Available at <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ accessed 13 June 2017

[117]Ciaran Martin, director of cyber security at GCHQ. Bowcott O., "GCHQ accused of 'persistent' illegal hacking at security tribunal" (2015) available at https://www.theguardian.com/uk-news/2015/dec/01/gchq-accused-of-persistent-illegal-hacking-at-security-tribunal

[118]Point 93 of the Schrems ECJ ruling already mentioned above. The ECJ goes in-depth on purpose lilitation requirements, that must be "specific, strictly restricted and capable of justifying the interference".

Bibliography

Legal Instruments

International

General International Law

- Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law (16 December 2005), General Assembly Resolution 60/147
- International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)
- Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR)

Cybercrime

- Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004), ETS N° 185
- Explanatory report to the Convention on Cybercrime (Budapest, 23 November 2001) ETS N° 185

Regional

EU Hard and Soft Law

- Charter of Fundamental Rights of the European Union, 2012/C 326/02 (EU Charter)
- Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)
- Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- The Article 29 Working Party (WP29) paper, “Rules of Procedure for the “Informal Panel of EU DPAs” according to the EU-US Privacy Shield" (2017)
- Study for the LIBE committee of the European Parliament, “National Security and Secret Evidence in Legislation and before the Courts: Exploring

the Challenges" Directorate General for Internal Policies of the European Parliament (Brussels, September 2014) PE 509.991

African Law

- African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) 21 ILM 58 (African Charter, ACHPR)

National

- French Intelligence Act (loi relative au renseignement), law n° 2015-912, 2015 codified in Book VIII, France's Interior Security Code (Code de la Sécurité Intérieure)
- French International Intelligence Act (loi relative aux mesures de surveillance des communications électroniques internationales), law n° 2015-1556, 2015, codified in Book VIII, France's Interior Security Code (Code de la Sécurité Intérieure)
- French Penal Code
- French Administrative Justice Code

Intergovernmental Organisations

- Annual report of the United Nations High Commissioner for Human Rights (UNHCHR) A/HRC/27/37, 30 June 2014

Books

- Amalfitano A., *La responsabilité pénale des personnes morales en Europe / Une recherche pour la construction d'un modèle commun* (L'Harmattan, Condé-sur-Noireau 2015)
- Delmas Saint-Hilaire J.-P., "Sans nécessité, loi pénale ne vaut" | Heurs et malheurs du principe de de légalité des délits et des peines (suite)" (2004), Politéia
- Nuotio K., "European Criminal Law" in Dubber M. D. and Hörnle T. (eds), *The Oxford Handbook of Criminal Law* (Oxford University Press, Oxford, 2014)
- Scalia D., *Du principe de légalité des peines en droit international pénal* (Bruylant, Brussels, 2011)
- Van Sliedregt E., "International criminal law" in Dubber M. D. and Hörnle T. (eds), *The Oxford Handbook of Criminal Law* (Oxford University Press, Oxford, 2014)
- Zetter K., *Countdown to zero-day* (Crown Publishers New York, New York, 2014)

Legal Briefs, Witness Statements and Opinions

- La Quadrature du Net, FFDN and FDN v Prime Minister, *Mémoire en réplique* on the Decree N° 2015-1185 (*to be published in July 2017*)

- Opinion of Advocate General Kokott in Lesoochranárske zoskupenie VLK v. Obvodný úrad Trenčín (C243/15) ECJ, ch., 8 November 2016
- Sophia In 't Veld's letter sent to the CNCTR, 2 May 2016
- Sophia In 'T Veld v. French Prime Minister, *Mémoire en réplique*, case No. 404013 (14 March 2017)
- King E., Witness Statement for Privacy International, cases No. IPT 14/85/CH and No. IPT 14/120-126/CH (London, 5 Octobre 2015)

Statements Before Parliament

- Declaration of Mr. Delon to the French Senate on the 10 February 2016

Law Reviews

- Tracol X., "EU–U.S. Privacy Shield: The saga continues", Computer Law & Security Review, volume 32 (2016)

Conferences and Lessons

- Pouillot P., Senior Underwriter, "Les conséquences et la nécessité d'être bien assuré : la relation entre le RSSI et les assurances", at the Cybersecurity: How to deal with cyberattacks conference of the AFDIT association (Paris, 25 November 2016)
- Quéméner M., "Cybercriminalité" lessons, *Faculty of Law of the Versailles University* (Versailles, February 2017)

Newspaper articles

- Ball, J. "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data" *the Guardian* (London, 28 January 2014)
- Bowcott O. "GCHQ accused of 'persistent' illegal hacking at security tribunal" *the Guardian* (London, 1 December 2015)
- Campbell D., Siddique H. "Operations cancelled as Hunt accused of ignoring cyber-attack warnings" *the Guardian* (London, 15 May 2017)
- Escarnot J-M "Antiterrorisme : l'espion aux espoirs déçus" (Antiterrorism: the spy with dashed hopes) *Libération* (Paris, 16 February 2017)
- Follorou J. "Comment le renseignement se prépare à l'éventualité d'une victoire de Marine Le Pen", *Le Monde* (Paris, 10 April 2017)
- Gallagher R. "Operation Socialist The Inside Story of How British Spies Hacked Belgium's Largest Telco" *the Intercept* (13 December 2014)
- Gayle D., Topping A., Sample I., Marsh S. and Dodd V. "NHS seeks to recover from global cyber-attack as security concerns resurface" *the Guardian* (London, 13 May 2017)
- Greenwald, G. and Gallagher, R. "How The NSA Plans To Infect 'Millions' Of Computers" *the Intercept* (12 March 2014)
- Investigate Europe "Why Europe's dependency on Microsoft is a huge security risk" (Internet, 13 May 2017)

- Johnston C., Russell G., Levin S., Wong J. C. and Rawlinson K., "Disruption from cyber-attack to last for days, says NHS Digital – as it happened" *the Guardian* (13 May 2017)
- Rees M. "Loi Renseignement : le cri d'alarme du surveillant des surveillants" *NextInpact* (FR) (Paris, 16 February 2016)
- Sanger D. E., Chan S. and Scott M., "Ransomware's Aftershocks Feared as U.S. Warns of Complexity" *the New York Times* (New York, 14 May 2017)
- Sanger D. E. and Perlroth N., "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool" *the New York Times* (New-York, 12 May 2017)
- Sanger D. E., "Obama Order Sped Up Wave of Cyberattacks Against Iran" *the New York Times* (New York, 1 June 2012)
- Townsend M. and Doward J., "Cyber-attack sparks bitter political row over NHS spending" *the Guardian* (London, 14 May 2017)
- Untersinger M., "« La Ferme des animaux », concepteur de logiciels espions depuis au moins 2009" *Le Monde* (Paris, 6 March 2015)
- Zetter, K. "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers" *Wired* (San Francisco, 28 May 2012)
- Zetter K. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" *Wired* (3 March 2016)

Cybersecurity Experts Articles

- Research team of the Kaspersky Lab "Animals in the APT Farm" (Russia, 6 March 2015)
- Paganini P. "Dino Malware that targeting Iran belong to Animal Farm's arsenal" (Brussels, 1 July 2015)

Leaks

- Snowden revelations (2014) (at https://search.edwardsnowden.com/docs/MobileNetworksinMyNOCWorld2014-12-13nsadocs)
- Wikileaks, HackingTeam email leaks (at https://wikileaks.org/hackingteam/emails/?q=france&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult)
- Wikileaks, "Vault 7: CIA Hacking Tools Revealed" (press release, 7 March 2017)

Technical Documentation

- The GNU/Linux Distribution Timeline 12.10, available at http://futurist.se/gldt/wp-content/uploads/12.10/gldt1210.png

Civil Society Documents

- Unofficial translation made by the volunteers of French organisation La Quadrature du Net of the 8th Book of France's Internal Security Code

(ISC). Translation is available at https://wiki.laquadrature.net/French_Intelligence_Laws

Miscellaneous

- Article of the Exegetes, "How to Check You Have Not Been Subject to Undue Surveillance" (Paris, soon to be published)

Websites

- Axa's : https://entreprise.axa.fr

Case-law

Les Verts c. Parliament (294/83) CJEC, Apr. 23, 1986

Marguerite Johnston v. Chief Constable of the Royal Ulster Constabulary (222/84) CJEC, May 15, 1986

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others and Kärntner Landesregierung and others (C-293/12, C-594/12) ECJ, g. ch., Apr. 8, 2014

Maximilian Schrems v Data Protection Commissioner (C-362/14) ECJ, g. ch., Oct. 6, 2015

Lesoochranárske zoskupenie VLK v. Obvodný úrad Trenčín (C-243/15) ECJ, g. ch., Nov. 8, 2016

Tele2 Sverige AB v. Postoch telestyrelsen et Secretary of State for the Home Department (C-203/15, C-698/15) ECJ, g. ch., Dec. 21, 2016

Klass and others v. Germany (5029/71) ECtHR, Plen., Sep. 6, 1978

Weber and Saravia v. Germany (54934/00) ECtHR, 3rd sect., Jun. 20, 2006

Liberty et autres v. United Kingdom (58243/00) ECtHR, 4th sect., Jul. 1, 2008

Gillan and Quinton v. the United Kingdom (4158/05) ECtHR, 4th sect., Jan. 12, 2010

Kennedy v. the United Kingdom (26839/05) ECtHR, 4th sect., May 18, 2010

De Souza Ribeiro v. France (22689/07) ECtHR, g. ch., Dec. 13, 2012

Pruteanu v. Romania (30181/05) ECtHR, 3rd sect., Feb. 3, 2015

R.E. v. United Kingdom (62498/11) ECtHR, 4th sect., Oct. 25, 2015

Roman Zakharov v. Russia (47143/06) ECtHR, g. ch., Dec. 4, 2015

Décision relative à la Loi relative aux mesures de surveillance des communications électroniques internationales (n° 2015-722) French Constitutional Council, Nov. 26, 2015

Acronyms

ACHPR African Charter on Human and Peoples' Rights

CFR (EU) Charter of Fundamental Rights

CJEC Court of Justice of the European Communities

CNA Computer Network Attack

CNCTR Commission Nationale de Contrôle des Techniques de Renseignement

CNE Computer Network Exploitation

CoE Council of Europe

DGSE Direction Générale de la Sécurité Extérieure

DPA Data Protection Authority

ECHR European Convention on Human Rights

ECtHR European Court of Human Rights

ECJ European Court of Justice

EU European Union

GCHQ UK Government Communications Headquarters

GDPR General Data Protection Regulation

ICANN Internet Corporation for Assigned Names and Numbers

ICCPR International Covenant on Civil and Political Rights

IPT Investigatory Powers Tribunal

ISC (French) Internal Security Code

LIBE European Parliament Committee on Civil Liberties, Justice and Home Affairs

NHS National Health Service

NSA National Security Agency

PLC Programmable Logic Controller

UDHR Universal Declaration of Human Rights

UN United Nations

US United States

UK United Kingdom

REP Recours pour Excès de Pouvoir

SIGINT Signal Intelligence

WP29 Working Party 29 (gathering the EU Member States DPAs)