EUROPEAN COURT OF
HUMAN RIGHTS

First Section
Application no. 46259/16

Privacy International and Others
Applicants
v.
United Kingdom
Respondent Gov.

WRITTEN OBSERVATIONS BY
L. ROUSSEY AND FRENCH DATA NETWORK
IN SUPPORT OF APPLICANTS

Ms Lori Roussey and French Data Network ("Interveners") respectfully submit the following observations to provide the Court with a French legal perspective on the implications of intelligence services' resort to equipment interference, and the negative effects of a legal regime that does not provide effective remedy.

1. Introduction: The Notable Consequences Of Computer Network Exploitations And Attacks By State Actors

On May 12 2017 in the UK, numerous National Health Service (NHS) patients about to undergo medical operations were suddenly unable to receive them. The cause of this critical infrastructure disruption? Connections between computers, X-ray scanners used to treat cancers, and other medical equipment were interrupted and had become inoperable. Communication channels within and between NHS trusts, such as emails and phone lines, had been made unavailable. More importantly, patient records were no longer accessible.

In few hours, 47 British hospitals had been hit by the same malware, coined "WannaCry". In the course of the week-end, similar computer infections were suffered in 150 countries, affecting multiple businesses. In Europe only: the malware forced Renault to halt car factories in France, while it infected Dacia in Romania, Nissan in the UK, Telenor Hungary and Telefónica in Spain.

At the root of this life threatening and extremely costly chaos is the theft of a hacking tool from the United States of America's National Security Agency (NSA), an intelligence service. One piece of code, enabling whoever uses it to exploit a vulnerability found in most servers around the globe at that time.

The power gained by hacking tools, and the plethora of risks they create for the public, the private and the third sectors when used recklessly, are mind numbing. For this very reason, the present lack of legal safeguards applying to the obtention and use of hacking tools by intelligence services must be considered all the more seriously.

Hacking tools, or Computer Network Exploitations (CNEs) and Attacks (CNAs), are meant for surveillance, but they also increasingly aim to sabotage physical infrastructure, not just computers and networks. In other words, hacking tools can leave long-lasting damages, not only for individuals, but also for a legal person's physical and digital resources. Hereby jeopardising investments and profitable activities.

Not to mention that CNE and CNA tools held by intelligence services attract ill-intentioned attackers - be they state-sponsored or private "black hat hackers" exploiting computers to e.g. ransom or collect economical intelligence. This results today in the theft of heavily infectious malicious software, causing enormous damages to the private sector and critical infrastructure if they are cast on the public.

In the Interveners' opinion, it is becoming absolutely urgent that the possibility to seek **effective remedy** in intelligence hacking and intelligence hacking tools cases is strengthened.

This can be illustrated, in particular, with the activities of GCHQ in relation to the Belgacom attacks.

In 2013 the Snowden revelations shone a light on GCHQ's hacking of Belgacom, the internet service provider providing its services to, among other clients, the European Commission, the European Council and the European Parliament[1]. Belgacom, now called Proximus, indicated that 5,000 of its machines had been infected[2]. As a result of the attack of its resources, the private company sought to obtain compensation by lodging a complaint before Belgian courts.

De Standaard[3] has found that the Belgacom judicial investigation has proven that the source of the hacking was GCHQ but regrettably the "British department of the interior [Home Office] [was] refusing to co-operate with the investigation"[4]. The right to access to remedy and fair reparation, as well as the need for proportionality, need to be urgently upheld as private persons cannot be left with unsatisfactory protection of their fundamental rights and losses when incurring losses as a result of being trapped in the net of intelligence services hacking.

This is not an isolated case. During an interview to German television channel ARD on Thursday 23 January 2014 Edward Snowden indicated that the NSA's espionage activities are not only aimed at protecting US national security but also at companies and private individuals[5]. This was alarmingly corroborated by the internationally renown Citizen Lab, whose research unveiled the existence of a dense web of countries, such as France, who had contracted an Israeli company to use hacking tools (the Pegasus spyware) on the public, targeting journalists, human rights defenders, opposition politicians, lawyers, and anti-corruption advocates[6].

Consequences can also be economically devastating. Extremely elaborated and dangerous new hacking tools used against private entities cause colossal losses to companies.

While there is no available estimation of losses for Belgacom, more recently, the international French company Saint Gobain estimated, one month after it was infected by NotPetya in 2017 – an attack mainly derived from a hacking tool of the USA's National Security Agency (NSA) also used in WannaCry as described on page 1 – that its losses amounted to 250 million Euros[7].

[1] See GCHQ's attack on the most important Belgian telecommunications operator, Belgacom. The targets of GCHQ were the customers of Belgacom, the European Commission, the European Council 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/

[2] See Corfield G., "Belgium: Oi, Brits, explain why Belgacom hack IPs pointed at you and your GCHQ" *The Register* (26 October 2018). Available at https://www.theregister.co.uk/2018/10/26/belgium_finds_evidence_gchq_belgacom_hack_proximus/

[3] De Standaard is the Belgian newspaper that had worked with the Intercept to cover the Snowden revelations. Its article are not quoted as they are mainly available in Dutch.

[4] "Specifically, these are IP addresses of computers where the spyware software communicated from Belgacom. [Regarding the proceedings, De Standaard] quoted the "British department of the interior" [Home Office] as refusing to co-operate with the investigation. The refusal to co-operate is unsurprising. For all manner of obvious diplomatic reasons, the UK is not going to confess to hacking one of its supposedly closest allies; an ally which hosts the key institutions of the EU as well as NATO". See Corfield G.,"Belgium: Oi, Brits, explain why Belgacom hack IPs pointed at you and your GCHQ" *The Register* (26 October 2018). Available at https://www.theregister.co.uk/2018/10/26/belgium_finds_evidence_gchq_belgacom_hack_proximus/

[5] Transcript available here: https://edwardsnowden.com/2014/01/27/video-ard-interview-with-edward-snowden/

[6] Research summary of the University fo Toronto's Citizen Lab, available online at https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[7] "L'impact financier de l'attaque au ransomware menée en juin contre les entreprises au niveau mondial vient d'être très concrètement chiffré par l'industriel français Saint-Gobain sur son exercice 2017. Il approche 250 millions d'euros sur ses ventes et 80 millions d'euros sur son résultat d'exploitation." See Gros M., "Saint-Gobain évalue à 250 M€ les dégâts liés à l'attaque NotPetya" *Le Monde Informatique* (01 August 2017). Available at https://www.lemondeinformatique.fr/actualites/lire-saint-gobain-evalue-a-250-meteuro-les-degats-lies-a-l-attaque-notpetya-68955.html

This issue is global. The UK government is not the only State with services carrying out CNEs, CNAs and other types of IT equipment disruption.

The resort to CNE, CNA and other types of IT equipment interference by intelligence services is, therefore, a growing concern for the international community.

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression already raised substantial concerns. In his 2013 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."[8]

This was latter echoed by a 2017 report (CCPR/C/ITA/CO/6) of the UN Human Rights Committee expressing the Committee's "concer[n] about reports alleging a practice of intercepting personal communications by intelligence agencies and the employment of hacking techniques by them without explicit statutory authorization or clearly defined safeguards from abuse". In its report the UN is urging "that such activities conform with [...] the principles of legality, proportionality and necessity, [...] that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse,including, where possible, an *ex post* notification that they were subject to measures of surveillance or hacking" be provided for.[9]

In light of the consequences of CNEs and CNAs by State actors, and taking into account the call for robust legal safeguards from the international community, Interveners are of the opinion that the enforcement of the right to an effective remedy, including the right to pecuniary compensation[10], as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (the "Convention"), is paramount.

Interveners therefore respectfully wish to contribute to Court's determination of this Case, first by providing general principles for respect of rights under the Convention, and then by providing some context and analysis on France's legal framework, to support a comparative understanding by the Court of State intelligence services uses of CNEs and CNAs.

2. European Convention On Human Rights (ECHR)

Interveners fully uphold Privacy International's arguments on that matter, in particular on articles 8 and 10 of the ECHR.

In addition, Interveners think that the consequences of State use of CNEs and CNAs interfere with the right to property, and that the right to effective remedy shall include the right to compensation with respect to such consequences.

2.1. The Right To The Protection Of Property

The first protocol of the European Convention of Human Rights (ECHR), entered into force in 1954, enshrines the right to the protection of property.

[8]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

[9]Report of the UN Human Rights Committee expressing the Committee, U.N. Doc. CCPR/C/ITA/CO/6 (2017)

[10]See e.g. with respect to breaches of Article 3 of the Convention, *Torreggiani and Others v. Italy*, App. No. 43517/09, pilot judgment of 8 January 2013 §97

The cases of Belgacom's 5,000 infected machines by GCHQ illustrates the need to ensure that if caught in the net of services hacking, a business undoubtedly incurs costs to fix their property. The Intercept indicates Belgacom had to pay "several million dollars"[11], while stressing that the company is unwilling to give clear numbers.

Although there is an unfortunate lack of estimates regarding costs, Saint Gobain's 250 million euros losses after three days of infection is a show stopper. Moreover, for Saint Gobain as well as for Belgacom the losses in terms of users' confidence is impossible to translate satisfactorily into numbers, even if it is probably the greatest harms of all: trust is often presented as the most precious ingredient for a business to thrive.

All property and reputational costs, in turn, threaten a business' ability to remain competitive. Ironically, the more intelligence services will develop or finance the acquisition of new hacking tools, the more they will become a target of choice for black hackers aiming for high scale extortion and property damages.

As a consequence, the right to the protection of property steadily becomes a central stake in the context of the use of intelligence hacking tools by intelligence services or their subsequent attackers. This right can only be upheld in courts. It is hence inherently dependent on robust effective remedy guarantees.

2.2. The Right To Effective Remedy

The threat posed by intelligence services' recourse to hacking tools requires our analysis to go in a greater level of details to shine a practical light on the questions sent by the court on July 15 2019.

Pursuant to its Article 13, the ECHR ensures the protection of the right to an effective remedy. The ECHR emphasizes that effective remedy shall be assumed, "notwithstanding that the violation has been committed by persons acting in an official capacity"[12].

In terms of case law, the acute threat posed by secret surveillance to redress avenues was highlighted in the *Klass* case, where it held that secret surveillance inherently threatens one's ability to obtain any form of remedy (*Klass and others v. Germany* (5029/71) ECtHR, Plen., Sep. 6, 1978, para. 36).

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).

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 effectiveness of the safeguards was to be assessed, *inter alia*, on the kind of remedy avenues provided by national law. 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 your jurisdiction takes a clear stance requiring that national legal frameworks must have remedy avenues that can be proven to be effective and associated with a fair reparation of the plaintiff(s) when an encroachment was found. Hereby setting a requirement for States to demonstrate how remedies were effective *in concreto*. This building block becomes particularly vital in the wake of unprecedented espionage and sabotaging hacking tools acquired and deployed by intelligence services throughout Europe. The French legal framework is no exception, as Interveners will illustrate below.

[11] Op. Cit., Gallagher 2014

[12] 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."

3. French Law On Intelligence Services Hacking

As seen supra, the effective remedy principle is of particular importance in surveillance cases. It shall now be confronted to a national framework as, despite the ratification of the Budapest Convention, countries' legislations regarding CNEs and the provision of an effective remedy remain fragmented.

3.1. French Law On CNEs And CNAs

Under French criminal law, use of CNEs and CNAs fall in the prohibitions of Articles 323-1 et s. of the Penal Code[13], in line with stipulations of the 2001 Budapest Convention on Cybercrime[14]. These prohibitions aim to prevent and fight against acts exploitation of computer networks by way of, *inter alia*, fraudulently accessing systems, remaining into systems, and modifying, interfering, extracting or transmitting data in such systems, but also the offer, export, design of tools designed to exploit vulnerabilities or carry out CNEs and CNAs.

However, intelligence services are expressly, or implicitly, permitted to use certain forms of CNEs and CNAs under Article L853-2[15] of the Internal Security Code ("ISC") and, more generally other forms of CNEs and CNAs, under Article 323-8 of the Penal Code.

3.1.1. The Unclear Legal Framework For Exceptions For Intelligence Services

Article L853-2 ISC, in particular, allows services to resort to techniques such as keyloggers recording every key pressed by the target, or tools similar to the ones used by the GCHQ like "Flame" to take computer screenshots[16], "Captivatedaudience" to hijack computer microphones[17], "Gumfish" to activate computer webcams and take pictures[18], or "Tracker

[13] 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.

[14] 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

[15] 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*]

[16] 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

[17] 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

[18] Ibid.

Smurf" activating the GPS tracker of a phone, even if it is switched off[19]. In an intelligence service hacking context, any tool is meant to either generate, intercept, modify or delete data.

Article 323-8[20] of the Penal Code provides an exemption in favour of intelligence services that sets particularly 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 ambiguous from the Code whether these measures may be implemented from within the national territory as well as from outside of it - as long as they protect interests "outside" France's territory.

In addition, intelligence services may transfer CNEs and CNAs data or programs, as defined by Article 323-3 but again, the authorisation to do so is merely implied by Article 323-8.

Transfers within or across French borders are further depicted at Article 323-3-1[21]. 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.

In these circumstances, a possible interpretation of the derogation created by 323-8 could lead one to use the liberty given by this article to justify that to exchange hacking tools, intelligence services would not always have to invoke France's interests outside the territory. Such transfers could for instance be done to render a favor to the intelligence service of an allied State.

This is not an hypothetical situation. It has already happened with the Stuxnet hacking tool for instance, as it was 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 favor to the later[22]. It seems to have been the case for the hacking of Belgacom as well, whereby GCHQ would hack Belgacom to share its data with its allies of the five eyes (USA, Canada, New Zealand, Australia).[23]

Incidentally, the compatibility of these provisions with international law also comes into question. In order to harmonize and build up confidence between countries the Budapest Convention's Article 32 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". Then again, French provisions above appear to be in contradiction with France's obligations towards other Parties to the main international law instrument pertaining to hacking.

3.1.2. The Lack Of Control Of Sharing Between States Of CNEs And CNAs Tools

Article L. 833-2 ISC sets out the missions of the French Intelligence oversight body, the Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR)[24]. The

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

[20] Article 323-8 (amendment of 2015 - translation by Lori Roussey 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."

[21] 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."

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

[23] Op. Cit. Gallagher 2014

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

fourth point of this article expressly provides that "elements provided by foreign agencies" shall not enter the material scope of its oversight. Despite the fact that as seen supra with the Stuxnet example, hacking tools are and may very well continue to be passed on among national services. Even when they are made of a succession of exploits that could cost thousands of millions to the private sector if not handled with care or associated with principles of accountability.

This in turn begs for the question - can an effective remedy be deemed to exist in the context of intelligence hacking legal frameworks?

The sixth article of the Budapest Convention on 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 ISC - imply or infer transfers of hacking tools without setting out a clear legal framework in order to provide accountability or oversight.

3.2. Lack Of Effective Remedy Under French Law

As seen above, the most robust legal safeguards would remain walls of hay if not built on top of solid remedy avenues for litigation against intelligence services' techniques, and proper compensation.

3.2.1. Avenues For Administrative And Jurisdictional Control

When the French Intelligence Act and the French International Surveillance Act of 2015 were codified in the eighth book of the Internal Security Code (ISC), Article L801-1 ISC gave exclusive jurisdiction to the Council of State on any dispute or complaint that may arise. Proceedings are before a special court of the Council of State (called "formation spécialisée du Conseil d'État") whose members receive special accreditation for national defense secrecy purposes.

Proceedings before this court may be brought by any person - after having filed a complaint to the Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR)[25], except in matters subject to the International Surveillance Act (see below).

Proceedings before this court may also be brought 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.

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[26], and then by filing a case before the special court of the Council of State via Article L. 841-1[27].

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

[26]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."

[27]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:

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."

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 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.

3.2.2. Redress Mechanisms
Redress offered by the CNCTR:

- The oversight body will neither confirm nor deny the unlawfulness of any measure or whether any surveillance technique has been used at all;
- 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 or three of its members may bring the case before the Council of State.

Regarding redress via the Council of State, while the law provides that it can order the State to provide reparations to persons when surveillance has been found illegal (L. 773-7 ISC), the specific procedural derogations are so great that the right to a fair trial (when avenue for remedy is available, which is not always the case) is greatly affected.

3.2.3. Lack Of Remedies Or Control
The general principle under French law is that remedies are available to private persons via the Council of State for any intelligence measures under the ISC that is subject to Prime Minister's authorization. There are however many exceptions, the justification for which is questionable (as has been pointed out in its 2018 report by the CNCTR[28]).

Redress via the Council of State excludes international and wireless surveillance, as well as transfers of tools or data between countries.

Indeed, firstly, wireless surveillance remedy is excluded by Article L821-1 of the ISC.

Secondly, it is inferred by Article L. 833-2 setting out the missions of the French intelligence oversight body that there is no remedy avenue for claimants fearing that a set of their data or a hacking too was transferred to French intelligence services by or to "foreign agencies".

Such a legal loophole incentivises services to obtain hacking tools or data through other agencies to avoid accountability.

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."[29]

Moreover, the 2015 International Surveillance Act creates a derogatory regime where proceedings before the Council of State in matters of surveillance of "international communications" may only be brought by the CNCTR. This hereby prevents any person or any judge from seeking any remedy in international surveillance cases.

In the same way, Article 323-8 of the French Penal Code poses a serious threat to the principle of legality when used to to protect Frances' interests abroad.

[28]available here https://www.cnctr.fr/8_relations.html
[29]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

In addition, this Article bypasses the fragile possibility that hacking and the transfer of hacking tools could be sanctioned in case of abuse by the services. Yet, Article 323-8 is the only article of the Penal Code referring to services, even if only to create a derogation from sanctions in case of use - or abuse. It could be seen as implicitly acknowledging that other articles do cover the services' activities.

Either way, this would confirm that in the case of hacking and transfer of hacking tools, no article provides for their the sanction of abuse. Which implies a broad impunity of services. A spin chilling fact considering the sacrosanct criminal law principle that any wrongdoing shall not be sanctioned if not expressly associated with sanctions in the law.

To summarise, the Penal Code articles on hacking create a blanket impunity for services' transfers of hacking tools or their resort to such tools to gather, modify or sabotage data in case of abuse. This is accompanied by an absence of remedy avenues when tools were shared by other services or that the surveillance was wireless or deemed international, or that hacking was done to protect France's interests abroad.

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

In short, under many aspects the French legal provisions pertaining hacking blatantly contravene the ECtHR's interpretation of the European Convention on Human Rights on the right to an effective remedy and the right to reparation.

Past national cases involving the Interveners allow some insights on how remedies are implemented in practice. One caveat: to our knowledge, no proceedings relating to intelligence services in France have targeted these specific and new hacking measures yet, but proceedings brought through the remedy avenues created by the 2015 Intelligence Act shed light on the process.

In a first international surveillance case, an *ad hoc* coalition of lawyers, including the Interveners, volunteered to help a citizen bring a claim before the CNCTR. On November 23 2015, the CNCTR answered by asking for the numbers of all the claimant's phone lines to check. It did not make 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. This means that in less than 24 hours, the notoriously underresourced CNCTR[30] checked with the international surveillance agency and other intelligence services who may retain data resulting from the international surveillance apparatus (there are currently six 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. After this, the claimant filed a suit before the Council of State relating to their complaint before the CNCTR. In its "Mme A." decision[31], the Council of State rejected the claim, stating that since the claim pertained to international surveillance, the claimant had no mean to appeal the CNCTR notification.

This portrays a gloomy insight of what the sole remedy avenue provided to natural persons 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. What's more, the claimant discovered that its had been sent proactively by the Council to newspapers with no form of anonymisation whatsoever. In the context of proceedings against hacking techniques, this could mean the reckless unveiling of hacked individuals or corporations, or the exposure of vulnerabilities. This may be the sign that

[30] Declaration of the head of the CNCTR at the time, 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.".

[31] *Mme B... A...* (397623) French Council of State, Formation spécialisée de la Section du contentieux, Oct. 19, 2016, 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

the handling of Intelligence and hacking related cases should be subject to strict official guidelines.

Another case to the CNCTR and the Council of State shed light on the effectiveness of the right to remedy with regard to French intelligence measures.

A complaint filed by the Member of the European Parliament (MEP) Sophia in 't Veld challenged the legality of France's international surveillance apparatus set up since 2008[32]. Mindful of the Constitutional Council's decision of November 2016[33] openly noting that the French legal framework offers no possibility for persons to go to a judge in case of international collection of information, Ms in 't Veld chose to bring two cases before the Council of State.

One to appeal the CNCTR - absence of - notification, and one based on the general French administrative law instrument of the recours pour excès de pouvoir (REP), on the ground that the French authority had exceeded its powers.

The REP was intended to prove the complete absence of remedy before French jurisdictions in international surveillance cases. Either the Council of State was recognizing victims of international surveillance an ultimate remedy avenue in the REP, or it would enshrine the complete absence of remedy for potential victims of international surveillance. It is important to note, in particular, that the REP was not only targeting international surveillance measures made under the International Surveillance Act of 2015 (which removes the right to jurisdictional control of the special court of the Conseil d'État for these international measures). It was also targeting the international surveillance apparatus implemented in France since 2008, as revealed by many official sources and press articles.[34]

Although the 2008 surveillance apparatus was not provided by any legal framework whatsoever until November 2015, MEP In 't Veld's proceedings targeting this system was deemed inadmissible on grounds of the November 2015 International Surveillance Act.

In a nutshell, there is no denying, as multiple sources aboveshow, that France among other states rely increasingly on CNEs and CNAs and other forms of technological surveillance.

Jurisdictional control has however been insufficient to offer effective remedy to claimants.

September 11, 2019, Oxford/Paris

Lori Roussey

On behalf of FDN
Hugo Roy

[32]The briefs submitted in MEP in 't Veld's case are available at https://exegetes.eu.org/dossiers/intveld/

[33]See recital 18 of *Décision relative à la Loi relative aux mesures de surveillance des communications électroniques internationales* (n° 2015-722) French Constitutional Council, null, 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

[34]See, on this topic the list of sources provided in MEP In 't Veld's case, available in French at https://exegetes.eu.org/dossiers/intveld/2018-02-12-observations-sur-duplique-sans-coordonnees.pdf, paragraphs 2 et s.