April 2016

ASSESSMENT AND PROSPECTS OF SECURITY THREATS

Synthesis report for
The International Forum TAC (Technology against Crime) 2016

Edited by Jean-Pierre Maulny and Sabine Sarraf, IRIS

Assessment and Prospects of Security Threats

Synthesis report for the International Forum TAC (Technology against Crime) 2016

This report presents a comparative cross-analysis of the national strategies in terms of security and, beyond, envisions the possible European convergences. Its purpose consists in evaluating the security threat for the decades to come, and assessing the way new technologies can represent a challenge and a response to provide. Various legal instruments, existing or contemplated, are listed in this report, in order to reduce potential risks. All these aspects are observed within the context of correlated societal debates. Four questions are therefore addressed successively:

Edited by Jean-Pierre Maulny and Sabine Sarraf, IRIS

***Contributors**:*

Felix Arteaga, The Elcano Royal Institute (*Real Instituto Elcano*), *Spain*
Caroline Baylon, Chatham House and the International Institute for Strategic Studies, *Great Britain*
Eline Chivot, The Hague Centre for Strategic Studies (HCSS), *the Netherlands*
Anja Dahlmann, The German Institute for International and Strategic Affairs (*Stiftung Wissenschaft und Politik*, SWP), *Germany*
Marcel Dickow, The German Institute for International and Strategic Affairs (*Stiftung Wissenschaft und Politik*, SWP), *Germany*
Artur Kacprzyk, The Polish Institute of International Affairs (*Polski Instytut Spraw Międzynarodowych*, PISM), *Poland*
Alessandro Marrone, The International Affairs Institute (*Istituto Affari Internazionali*, IAI), *Italy*
Jean-Pierre Maulny, The French Institute for International and Strategic Affairs (*Institut de relations internationales et stratégiques*, IRIS), *France*
Rui Carlos Pereira, The Security, Organised Crime and Terrorism Research Centre (*Observatório de Segurança, Criminalidade Organizada e Terrorismo*, OSCOT), *Portugal*
Sabine Sarraf, The French Institute for International and Strategic Affairs (*Institut de relations internationales et stratégiques*, IRIS), *France*

HOW WILL SECURITY THREATS EVOLVE OVER THE NEXT FEW DECADES?

The definition of what can constitute a security threat is subjective and scalable. It depends on the point of view from which it is determined. It is noticeable that different countries do not tackle security in the same way. Whereas **France** and the **Netherlands** favour an approach based on the intended security objective, such as territorial protection, economic stability or health security; other contributing countries take an interest in security on the basis of identified threats. Consequently, the Dutch and the French consider that security covers a broader range of hypotheses, taking into account unintentional threats such as major natural disasters or technical failures. It is an exhaustive definition that does not exclude a prioritisation of the threats, even though this exercise is not necessarily codified in a text. However, a majority of countries understands the notion of security as meaning safety, that is to say the fight against a malevolent intention or action.

Germany and the United Kingdom, for their part, specifically consider security from two perspectives: public and individual safety. The first expression denotes the main objectives that need to be achieved, the prevention of terrorist threats and serious criminality, the protection of vital and critical infrastructures, or, for instance, cyber crime. Regarding individual safety, the writers stress the importance of privacy breaches or all the other rights related to personal data processing and mass surveillance.

Before even prioritising the potential security threats, all **States put an emphasis on the fact that there is a progressive disappearance of the demarcation between external security and internal security**. External security threats are becoming internal security threats, and nowadays, they are starting to overshadow "traditional" threats of delinquency and criminality. **Spain** puts forward a structural cause to explain this development. For this country, globalisation plays an important role in the development of the security environment. This results in a dematerialisation of borders, which increases "the attack surface creating unpredictability regarding the source, the territorial origin of the security threat". Non-State actors can operate beyond national borders, removing the traditional distinction between internal and external security, and thus compelling law enforcement agencies from different countries to cooperate in order to take effective action on a supranational level.

For other countries, both notions of internal and external security are even completely amalgamated. In Poland, one finds that the major cyber security risks include actions conducted, sponsored on encouraged by actors, which reside outside of its territory, be it cybercrime units or state-run groups of hackers. Response to such activities often fall within the competence of internal security agencies, particularly if the attacked systems constitute parts of the critical infrastructure, like governmental communication networks, electric grids or transport management systems.. For a lot of countries, starting with France, international and transboundary terrorism has become the main threat in 2015.

If there is indeed a prioritisation of threats, it is often implicit, and does not ensue from a internal security policy that would globalise the States' action in that field.

Accordingly, in 2015, **Germany** has focused on the violations of individual freedoms that can be committed, in particular the violations related to the protection of personal data and the right to privacy. The reasoning for this is the German society's extreme sensitivity on these issues. Germany also puts an emphasis on issues regarding cyber security or the supply of energy and ores, two sectors which have recently been subject to a new strategy (2015 for the first, 2016 for the second), and are notably linked to concerns with regard to vital infrastructures protection[1].

As a general rule, cyber space faces a phenomenon consisting in the proliferation of malicious tools particularly difficult to grasp and understand. It is widely accepted that the cyber security threat is a priority that is arduous to pinpoint, and that is assessed differently from one State to another. Germany emphasises potential violations of individual freedoms associated with the development of cyber space, but Germans also establish a link between terrorism, threats from third States and cyber attacks. **Poland** directly links together the cyber threat and the external threat, due to the fact that vast majority of cyberattacks originate from sources outside of the territory of the attacked country. Poland is concerned with malign use of cyberspace for intelligence and military operations and terrorist acts, both by state and non-state actors.

In the United Kingdom, cyber space is also regarded as the main threat, regardless of its origin. From the British point of view, it is the multiplicity of possible effects, namely the plethora of potential targets for a cyber attack, that represents the threat. On that account, the list includes attacks on the infrastructures or the banking system, the denial of Internet access, the possibility of attacking unconnected networks which are starting to develop, and violations of various public freedoms and the right to privacy.

Furthermore, the attacks' objectives may be diverse in their nature. It may be espionage perpetrated by State actors. The attacks might aim at paralysing a country by targeting its vital infrastructures. Lastly, the goal might be to strike the country's political sphere or its economy, for instance by attacking an industry which activities are essential to the State's survival. The cyber threat that arises from non-State actors is even more difficult to discern. It is almost unpredictable, for it is not based on known diplomatic channels, contrary to those forged between one State and another.

As for **Italy**, the hierarchy of threats positions terrorism at the top of priorities, followed by the migratory issue and the cyber threat. Italy's perception of the migratory issue is

[11] Cf. German Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011), retrieved 12.10.2015, at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.html; and German Government, *The German Government's Raw Materials Strategy* (October 2010), retrieved 18.01.2016, at http://www.bmwi.de/English/Redaktion/Pdf/raw-materials strategy,property=pdf,bereich=bmwi2012,sprache=en,rwb=true.pdf

interesting, because this phenomenon results in three potential or proven threats: terrorism, the issue of public order relating to the increasing congestion of centres dedicated to migrants, as well as the opportunities for organised crime through human trafficking.

Terrorism is also at the very top of the security threats list for **Spain**, with cyber risk and organised crime. In this State, the migratory issue holds less relevance, but it comes from the fact that, geographically, the country is less affected by Syrian crisis-related migrations than countries from Southeast and Eastern Europe. This prioritisation does not result from an official document, but from observed perceptions in conjunction with public discourses.

Migratory issues are subject to specific attention, and are particularly emphasised by **Italy** and **Portugal** in the various reports. **Italy** is, with Greece, the European Union (EU) country most affected by migratory flows coming from third countries, and identifies migration as a threat to its security. The same applies for **Portugal**, which attests to the fact that Southern countries are more concerned with these issues than Northern European countries. Of course, migration is not a security threat in itself, as the Italian reports underlines. However, the mass arrival of migrants as it is experienced today prevents an efficient management of European borders. Thus, the migratory flow serves to facilitate the free movement of criminals, who take advantage of the malfunctioning control systems to enter the European territory despite the increasing use of ever more efficient security measures, notably biometric technologies used by border guards in Greek and Italian accommodation centres. Moreover, the significant number of refugees creates political and social instabilities within States where the population is hostile to welcoming them, stirring some tensions between communities and hindering their integration, however temporary. The Portuguese report highlights in particular the need to establish a political consensus about the societal implications of the phenomenon within the States, before implementing any policy whatsoever. Yet, it is quite clear that such a consensus, difficult as it is to find on a national level, is even more difficult to reach at European level, the German Chancellor's rhetoric on the necessary reception of refugees being far from shared by everyone, especially in Northern Europe or in some Eastern Europe countries.

In point of fact, Southern and Eastern countries are the most affected by the magnitude of migratory flows. The relocation and resettlement of migrants in other Member States than those through which they entered the Schengen area aims at sharing the burden of managing external borders, burden left to the exclusive jurisdiction of national authorities, in all of Europe. Although at the present time, this measure has only been very partially implemented, it perfectly illustrates a trend towards the *Europeanization of threats and risks*, depending as much on the factors outlined above – technological evolution and globalisation – as on the integration of the management of security issues in the European Union.

In the **Netherlands**, priorities are different. The fight against terrorism and extremism represents a significant threat, but it is less urgent than the manipulation of public administration, the ore supply shortage and cyber espionage[2].

In **France**, the 2013 White Paper on Defence and National Security (*Livre blanc sur la défense et la sécurité nationale*) identifies as strategic priorities the means that need to be deployed to ensure the protection of the Nation's fundamental interests, namely, aggressions against national territory, terrorist attacks, cyber attacks, infringements of technical and scientific potential, organised crime, major natural or manmade crises and attacks perpetrated against nationals abroad. These threats are listed in strategic French documents, in a non-prioritized manner. However, ever since the 2015 January attacks and subsequently the 2015 November attacks, terrorism has become the top priority, while the migratory phenomenon is reflected in real occasional tensions geographically concentrated in certain locations: Calais, Ventimiglia, at the French-Italian border, and Paris to a lesser extent. If the cyber threat is less highlighted, it is primarily because France has reacted and fought back, in particular since the publication of the 2013 White Paper on Defence and National Security, with a National Strategy for digital security being published in October 2015, and the National Defence creating the position of General Officer of cyber defence.

Other existing or proximate threats are listed in the **Dutch, Italian, English and Spanish** reports, and include radicalisation, religious conservatism, the integration of Muslim communities, inequalities in wealth on the international level and corruption.

In conclusion, if a certain harmonisation of the perception of threats can be observed on a European level, by globally drawing attention to the triptych terrorism, migration, cyber security, it must not conceal differences in the very treatment of the response provided.

Regarding terrorism, the perception of the threat is clearly more intense in the South compared to the North of Europe. If the cyber threat is generally linked to the external threat, whereas other countries will lay emphasis on the private – with cyber crime – or terrorist source of such a threat. Germany stands out in this regard, by putting an emphasis on the risks of violations against public freedoms and the right to privacy, in osmosis with civil society's preoccupations. The migratory issue, which is not a threat in itself but can reinforce some threats, needs in any event responses in terms of security, and is without a doubt the most likely to bring about disagreements, not over the recognition of the phenomenon but over the attitude to adopt towards it. This entails some divergences in the responses provided, which are reflected in the European Union's difficulty to enforce the measures that it advocates. In this context, the issue is indeed addressed at European Union level, but the responses are only very imperfectly provided.

[2] According to the National Coordinator for Security and Counterterrorism, attached to the Dutch Ministry of Security and Justice, which recently published a National Risk Assessment as part of the National Security Strategy.

In view of these observations, the new Dutch Presidency of the Council of the European Union has nevertheless tried, immediately upon beginning its term in the first semester of 2016, to set a common agenda emphasising the importance of the fight against terrorism and cyber security – which are therefore two of the threats most commonly mentioned by the States and which are not subject to major divergences between them – for these next few months. These priorities are not exclusive to the strategic orientation of European institutions, and States maintain a measure of discretion both on their definition and on the ways to combat security threats.

HOW CAN NEW TECHNOLOGIES CONSTITUTE A RESPONSE TO SECURITY THREATS?

Security technologies are designed, produced and marketed to respond to existing threats and risks, or from a prospective point of view, foreseen. Yet, by solving a problem, security technologies can sometimes create new ones. For all, information and communication technologies have a peculiar characteristic: they are likely to generate both advantages and disadvantages. Indeed, technological progress is accompanied by new risks quite often related. The writers of the various reports agree on the implications resulting from this progress.

First of all, comes the *universalization of the Internet*. Internet accessibility and its democratisation are objectives pursued by the European States, with the following goals: to allow individuals to exploit the web's potential in terms of marketing and the acquisition of goods and services; to offer companies and governments alike an effective way of using digital tools; and to ensure that digital companies and start-ups will have a horizon as broad as possible to develop their activities. However, as the **Dutch, Italian and Portuguese** reports outline, in facilitating everyone's access to networks, we also facilitate the access of malicious individuals, whose skills in the digital field can create risks of varying severity. One of the best illustrations is that of identity and banking data theft. The mass use of the Internet for commercial purposes, combined with the users' carelessness in naively communicating their personal data, provide the usurpers with a tremendous potential for the achievement of their tortious or criminal intents.

For **Spain**, technological development and innovation create new threats unknown up until this point. Progress made in the fields of chemistry, nuclear energy, biogenetics, as well as in the field of digital technology is essential, and yet it creates new challenges for the integrity, prosperity and welfare of societies, as well as for the protection of the people and of their property.

In **Poland**, surveillance systems and software solutions to detect cyber attacks are listed among the most promising technologies.

Another phenomenon is that of data accumulation and storage. It is indeed an invaluable tool for intelligence agencies for purposes of prevention and detection of criminal offences, or simply on the basis of data storage from computer users' profiling. If the use of digitised data provides the opportunity to expand the capacities and efficiency of the authorities in charge of public security, it can just as well prove prejudicial to the fundamental rights and freedoms of the individuals concerned by an abusive processing of their data. The notion of abusive processing is something that may the subject of interpretation, in particular by the judge in the case of a dispute. The notion is however assessed in the light of established criteria based on the principles of proportionality

and necessity. The processing of personal data must fulfil a very clear purpose, and the means being used must be limited to the minimum necessary to fulfil that purpose. It is important to opt for a restricted interpretation of these criteria, in order to ensure the best possible protection of the fundamental rights and individual freedoms that are the protection of personal data and the right to privacy. Infringing them is only possible in very limited cases, reserved for extremely severe and imminent violations of public order, as set out for instance in the **German** Constitution.

In addition to the violations that it is likely to create regarding the respect of individual rights, the massive storage of sensitive data, in particular data held by public authorities, constitutes a target of choice for State-to-State cyber espionage.

Connected objects or the "internet of Things" are also a product of technological innovation, which induces implications of two kinds. **Italy** states that, in a perspective of increasing individual comfort, they have proved to be very popular and are flourishing, occupying an increasingly important place in everyone's daily life. Led by the allure of the potential optimisation of time management or organisation, individuals, businesses, public administrations use connected objects more and more to carry out routine tasks. Be that as it may, these devices' cyber resilience is far from optimal. The risks can spring from a technical failure or a malicious intrusion in the systems. The vulnerability of these objects brings about, in turn, the vulnerability of the objects they are connected to, multiplying risks factors. The **British** report even brings to light the future risk that objects behaving more and more like automatons could present, as they could escape from all human control.

For everyone, *social medias* are nowadays some of the best collaborative platforms of communication and information sharing. They provide users with a continued and instantaneous access to information, which they communicate and share themselves. Unfortunately, the mass use of these tools prevents an effective control of the remarks and comments being made, of their veracity and of their hateful or discriminatory nature. In consequence, they are at the same time the most efficient tool for propaganda and, with regard to terrorism, for recruitment and radicalisation, as the British report highlights.

Notwithstanding, technological progress in security is just as much a response as it is a potential threat in a dialectic borrowed to a defence that would perpetually confront the sword and the shield.

One can mention the research carried out in the field of quantum computing, which besides the multiplying speed of computers, should allow for the identification of cyber attacks.

The **Italian** report indicates that there is a form of *private sector monopoly on research orientation in the field of communication and information technologies*. In the field of research, one can observe that these technologies are indeed at the very heart of many

programs within companies. Innovation benefits all the actors of security, public and private alike but also, within public security, police forces and military forces alike. These technologies' duality, that is the fact that they can have civil applications as well as military applications, is beneficial in terms of synergy and mutualisation of resources earmarked for research. Nevertheless, in the field of information and communication technologies, the civilian sector occupies an increasingly important place compared to the public sector. Thus, although these new technologies are closely linked to security, and in particular cyber security, the authorities in charge of ensuring public security are dependent on the civil operators' choices in terms of research and innovation orientation.

Spain lays emphasis on the new technologies which have been put into service and which bring substantial progress in the field of security. The report lists the integrated border surveillance system used for ship detection and recognition, the simulation systems used by security forces and the technologies used for IED (improvised explosive device) recognition.

All reports bring to light the progress made in the field of information technologies, which allows for the collection of data on individuals through their telephone or their computers, or for the development of the capacity to fight against a number of crimes, starting with terrorism, which ranks at the very top of preoccupations. However, these technologies, which are aimed at increasing security, also carry two potential threats: a growing vulnerability to cyber attacks and the violation of public freedoms. Thus, the British report lays emphasis on the fact that the possibility of developing a quantum computer would enable access to any encrypted information, which would represent a progress as well as a threat against the interests of the States.

Aside from the information and communication technologies mentioned in the various reports, other technologies are a focus of concerns as well. Indeed, for **Italy**, the attention must be drawn to surveillance software programs, to micro cameras and facial recognition, as well as drones. For **Germany**, the evolution of technologies allocated to the retention of metadata, software programs encrypting electronic communications, and mobile data collection should be closely monitored. For the **Netherlands**, key challenges ahead involve biometric technologies, for authentication and identification, and the technologies used for behavioural analysis. Other debates, current and future, focus on the robotisation of security, as the **Dutch** report raises. Drones and armed robots are the main systems concerned. Drones, aside from the challenges that derive from the issue of privacy protection related to their surveillance function, also prove dangerous for physical and aviation security, more precisely in case of a technical failure or highjacking. As for robots, they can raise public debates about the dehumanisation of security or war in the field of defence.

WHAT LEGISLATIVE PROVISIONS COULD PROVIDE SUITABLE RESPONSES TO THESE THREATS?

All States included in the study have security documents on particular aspects, such as cyber strategies. It can be added that the same goes for the European Union, which has had a European security strategy pertaining to the Union's external security since 2003. Its definition and its implementation fall within the competence of the European External Action Service and, as of 2010, of an internal security strategy. The European Union's security strategies preceding those of the Member States, they have had an impact on national approaches, since these approaches have relied on what existed before. The legislative process towards the implementation of strategies translates into the adoption of more specific laws in order to reach the objectives pursued by these strategies.

The States covered by the study focus as a priority on three subjects: cyber space, terrorism and migration management, which is not surprising since those three subjects are among the priorities in terms of security.

In the field of cyber space, regulations are almost non-existent or very recent. In **France**, a draft legislation on digital technology is under development in the beginning of 2016. It is not only the first law on the matter, but also the first text for which citizens have been able to contribute to the drafting, by suggesting amendments *via* an online public consultation, in a direct democracy rationale.

The other European countries admit to not possessing any laws of general application, but they do have strategies on this subject, as France and the European Union do. As asserted in the **Dutch** report, for over ten years, the only text regarding cyber space was the Budapest Convention of 2001 against cyber crime. Yet this international agreement has not been ratified by the large majority and so far, has never demonstrated its true effectiveness. In order to fill the void in the field of cyber space, the majority of the countries included in the study have since 2013 resorted to the use of a strategic document on the matter, as well as structures dedicated to the management of those issues. **France** and **Germany** have differentiated themselves from the other countries since they have started public works programs on the challenges of cyber space a soon as 2011, which is two years before their partners.

In **Germany**, the adoption of the cyber security strategy has been accompanied by the creation of several new organisations in charge of its application. In the military field, Berlin has had since 2002 a Computer Emergency Response Team (CERTBw) at its disposal. As for the non-military side of cybernetic security, a National Council of Cyber Security has been created in 2011, after the publication of the Cyber security strategy, which serves at a platform where the users can share their experiences and strategies. A

National Cyber Response Centre has also been created in 2011, serving as a collaborative platform for governmental agencies such as the Federal Office for Information Security, the police and intelligence agencies.

In **Spain**, the cyber security strategy was adopted in 2013, in accordance with the ambitions stated in the 2012 National security strategy. The governance is ensured, for internal affairs, by the National Police and Civil Guard, in charge of the security of critical infrastructures, as well as the fight against cyber crime and cyber terrorism. The Ministry of Industry has developed a culture of cyber security *via* the National Institute for Cyber Security (*Instituto Nacional de Ciberseguridad*, INCIBE). The Ministry of Defence, for its part, has set up a Joint Cyber Defence Command and a National Centre for Intelligence (*Centro Nacional de Inteligencia*, CNI), respectively for the management of cyber defence operations and the protection of information and communication systems used by public administrations.

Italy adopted in 2014 a national framework for the protection and security of cyber space. Strategic documents establish the institutional architecture and identify the administrations in charge of the implementation of national cyber security policies. Among them, the Interdepartmental Committee for the Security of the Republic suggests new legislative action, the Cyber security Unit is designed to respond to cyber incidents, and the Security Intelligence Department, among other things, acts as a coordinator on a national level.

The European Union has itself set a European strategy for cyber security in 2013. Although it does not have binding legal value, it can be noted that it has had an impact on national policies, since following its publication, the States have adopted their own measures.

For the time being, national legislations in the field of digital technology are intended to cover the following issues: personal data processing and the obligations of the organisation responsible for their processing; the powers of judicial and police authorities; and the protection of the rights and freedoms of the citizens.

In **France**, the 1978 Law should be amended.

In **Germany**, the Parliament adopted in 2015 a law on data storage and data processing, making it mandatory for Internet service providers and telecommunications operators to provide the data relating to the telephone user, the person they called, the date and time of the call, its location, and in the case of Internet, the IP address and the date of the connection. This law applies when there is presumption of a serious crime, such as those provided in the Constitution (§ 100g StPo). The data will be processed by the Federal Communications and Internet Networks Agency (*Bundesnetzagentur*).

At **European Union** level, the European data protection package should be formally adopted in April 2016, after over four years of debate. This package consists of a

regulation regarding the data processing carried out by economic operators, and a directive regarding the data processing carried out by police and judicial authorities. Within two years, unless otherwise specified, the States should have adapted their national legislation to the content of these two texts.

It must be noted that these propositions are more suited to ensure individual safety in the context of cyber activities rather than cyber security strictly speaking. One will have to wait for the official adoption of the European directive regarding the minimum security level of information networks, which should occur in 2016, for the States to enact legislation relating to cyber security *per se*. This means that the States will have legislation within the next two years at the latest, a time period set to allow the transposition of the directive in domestic law. Consequently, the States will not want to enact legislation on the matter before that date, since their legislation will have to be compatible with that directive.

In the area of counter-terrorism, all the States have adopted national legislations relating to counter-terrorism and the incrimination of terrorism. These laws condemn propaganda, training, the preparation of attacks and their funding. These activities are considered criminal offences. The definition of a terrorist offence is based on two types of elements. The action must include objective elements – for instance a homicide –, bodily injuries or hostage taking. The action must also include subjective elements, such as the intimidation of a population or the destabilisation of the country. This decision also recognises the condemnation of intention, preparatory acts, offences connected to terrorist activities. In other terms, this decision does not require the offence to be consummated to be condemned. The assessment of the intent is based on a subjective interpretation.

Italy also adopted a law, in April 2015, which extends the legal framework for the surveillance conducted by intelligence authorities in the context of their fight against terrorism.

In the **United Kingdom**, David Cameron proposed in July 2015 a law relating to powers of investigation, the Investigatory Powers Bill, which makes it compulsory for businesses to keep recordings for a minimum of one year, in order to be able to make them available to security forces if necessary. The draft law also provides the possibility to have "backdoor access" from the operators, in order to have access to encrypted information.

Even **Poland** is preparing its first anti-terrorist law - *Ustawa antyterrorystyczna* – in the wake of the attacks perpetrated in France in November 2015. It should provide a legal framework for counter-terrorism activities, which are mapped out in the National programme of counter-terrorism 2015-2019. In consequence, this could be interpreted that the fight against terrorism is gradually becoming more of a priority for the country, which had until that point stayed in the background on this matter. The consultations on this new law should continue in the spring of 2016.

In **Spain**, the organic law on the protection of public security, which replaces the 1/1992 organic law on the same subject, was adopted on March 30th 2015. This law provides a number of provisions considered more restrictive than the ones existing previously with regard to public freedom. In this manner, a call to protest *via* social media can henceforth be penalized, as well as taking pictures of police officers or opposing an expulsion.

Struck by two series of attacks in January and November 2015, **France** has furthermore suggested, as early as the summer of 2015, several legislative projects to fight terrorism, notably with a law on intelligence. This law, adopted in July 2015, has admittedly allowed for a control of the activities undertaken by intelligence agencies, which wasn't a possibility beforehand – but it has also legalised practices which may be regarded as harmful to human rights, in particular techniques used to collect intelligence. The law provides for the possibility to coerce Internet service providers into detecting a terrorist threat based on automated processing and by monitoring all the traffic. Black boxes are in charge of reviewing the metadata relating to all communications: the origin or recipient of a message, the IP address of a visited website, the duration of a conservation or of the connection, etc. The Constitutional Council (*Conseil constitutionnel*) has nevertheless verified most of the law, underlining that the decision to resort to such techniques of collecting intelligence, and the choice of these techniques must be proportionate to the intended purpose and to the grounds invoked. The National Committee for the Control of Intelligence Techniques and the Council of State [*Conseil d'État*] are in charge of ensuring that this proportionality imperative is respected[3].

Politically and legally, this decision is important, for it does not call into question the principle of collecting private information in order to fight terrorism. However, it sets limits for public authorities in terms of the proportionality of intrusive procedures with regard to intelligence, in view of the risk involved. The debate should accordingly shift to the subject of the organisation in charge of the control, as well as the potential techniques of personal data self-protection, with the concept of privacy by design.

At **European Union** level, the European data protection package should be formally adopted in April 2016. As mentioned previously, this package consists of a regulation regarding data processing by economic operators and a directive regarding data processing by police and judicial authorities. The directive pertains to the protection of individuals in the face of their personal data being processed within the context of police or judicial activities, while the regulation sets out to strictly monitor data processing by economic operators – businesses. The frameworks for processing, applicable to private or public operators alike, are in fact closely linked. Businesses established on the territory of the Union regularly transfer, in the context of their commercial or human resources activities, data towards American companies. This practice was carried out in the legal framework of the *Safe Harbor* decision (an agreement between the EU and the USA on the transfer of data), recently invalidated by the Court of Justice of the European

[3] Constitutional Council, Decision n° 2015-713 DC, July 23rd 2015 – Law on intelligence, Press release, July 23rd 2015.

Union on the grounds that citizens of the Union could not have their right to privacy and to personal data protection guaranteed by the American authorities, and that it was impossible for them to be entitled to a recourse before the American courts[4]. The American police authorities can indeed, thanks to the *Patriot Act* 2001, have access to all data held by private American operators within the context of their security mission, and in particular the fight against terrorism. The adoption, as of today still informal, of the European data protection package, combined with the invalidation of *Safe Harbor*, offers EU citizens the guarantees deemed necessary by Community public authorities. Again there, it can be noted that these propositions are more meant to ensure individual safety within the context of cyber activities rather than cyber security strictly speaking. The data protection package should be officially adopted in the spring of 2016, while *Safe Harbor* has just been replaced by the Privacy Shield, which proposes clearer guarantees and requirements of transparency regarding the role of the United States government. If the European directive and regulation are adopted in 2016, the States will have to adapt their national legislation to the content of these two texts, which could translate into a calling into question of some laws already adopted.

Simultaneously with the adoption of new laws, **France** has suggested to revise its Constitution in order to include in it the principle of deprivation of nationality for the perpetrators of terrorist acts. However, it is not certain that this constitutional revision, which necessitates a three-fifths majority of the Parliament meeting in joint session, will be adopted. Some do not wish this provision to be included in the Constitution. Furthermore, restricting the scope of this provision to dual nationals would risk leading to a breach of equality with respect to the law, while extending it to all citizens could prove contrary to the 1954 New York Convention designed to combat situations of statelessness.

Migration management is an exclusive prerogative of the States, although the creation of the Schengen area leads to relativize its principle.

The Schengen area is a space without internal borders, which means that only the external borders of the territory are monitored. The free movement of goods, persons and commodities is ensured within that space. Although freedom of movement is a fundamental principle, the "Schengen Borders Code" allows Member States to temporarily restore the borders for reasons of public order and security (Article 26 and seq.). Yet, the number of border control measures has multiplied since 2015 for the first time since the establishment of Schengen.

It is on this legal basis that **France** has reinstated border control since November 13th, following the attacks that struck its capital, and to ensure the smooth running of the COP21. The other cases of border control, which have multiplied since September 2015, aim at allowing States to control migratory flows. It is in particular the case for Sweden, Italy and Belgium. Germany concentrates on its own a significant part of this issue, since

[4] CJEU, October 6th 2015, Max Schrems, C362/14, not yet published in the reports.

after announcing its will to welcome migrants, it had to take corrective measures in the form of border controls to be able to face massive and uncontrolled flows.

A certain number of laws are adopted in European countries, in an effort to dissuade migrants and to contribute to their reception in their host country. A Danish law voted at the end of January 2016 stipulates that the migrants' belongings will be confiscated if they are valued above 1340 euros. In Germany, a certain number of *Lander* also implement such a policy for asylum seekers. It is the case for Bavaria and Baden-Württemberg, the threshold for confiscation being respectively 750 euros and 350 euros.

In France, the state of emergency – which notably allows to conduct administrative searches, vehicle searches and to order house arrests – was declared for three months following the attacks on November 13th 2015, then was extended for three additional months. The provision should be included in the reform of the Constitution examined at the beginning of 2016. In addition, the reform of the Criminal Procedure Code envisages the implementation of other measures, such as four-hour-long administrative detentions during identity checks, vehicle searches in the vicinity of sensitive locations or house arrests for people suspected of coming back from Syria.

The **United Kingdom** is not a member of the Schengen area. It remains nevertheless true that the country is extremely preoccupied with migration issues. The very restricted access to the British territory has repercussions on French territory, where a large number of migrants are staying in precarious conditions on the Opal Coast (*Côte d'opale*), hoping to be able to reach the British territory.

The Europeanization of migratory risks has forced to reconsider management methods. In 2004, the **European Union** has created the Frontex Agency - European Agency for the Management of Operational Cooperation at the External Borders – which role is essentially to coordinate and support the action of the Member States. The added value of this agency has been called into question since the beginning of the migration crisis. The own resources of the peripheral States in charge of external borders control are not sufficient, and although Frontex has, since 2004, the capacity of acquiring additional supplies, it has not been enough to grant the necessary equipment to the States concerned. Moreover, in spite of the numerous calls for donations launched by Frontex to the Member States, few were inclined to provide supplies *ex gratia*.

That being so, with the adoption of successive provisional measures, the European Union has tried to take initiatives as a complement to the Member States' action, deciding to carry out immediate actions to face an unprecedented crisis. Among these actions is the relocation and resettlement of refugees or those who claim refugee status, and the introduction of "hotspots". This latter measure, implemented in the locations most affected by the massive arrival of migrants – Greece and Italy – was meant to control the flows while ensuring an effective control of the people entering the territory of the Union. Setting up these hotspots was long and tedious, and their efficiency still cannot be assessed as of today. Simultaneously, aware that immediate actions and

provisional measures will not be sufficient to resolve the migratory issues, the European Union has proposed in December 2015 a "borders package". This package includes: a draft regulation for the creation of a new European border guards and coastguards agency, which would replace the current Frontex agency; a revision of the Schengen Borders Code; and a draft regulation on a European travel document for third parties illegally staying on the EU territory. This travel document incidentally illustrates the increasing use of biometric data to improve the efficiency of the control of migratory flows in Europe. The adoption of the "borders package" is expected at the end of the first semester of 2016.

New structures dedicated to security

In France, the National Agency for the Security of Information Systems (*Agence nationale de sécurité des systèmes d'information*, ANSSI) was created in 2009, replacing the Central Directorate of Information Systems (*Direction centrale des systèmes d'information*). It assumes the role of national authority in the field of information systems security. More recently, in 2013, the Council of Trusted and Secure Industries (*Conseil des industries de confiance et de sécurité*, CICS) and the Committee of the Secure Industries Sector (*Comité de filière des industries de sécurité*, Cofis) were established in order to strengthen dialogue between public authorities and the security industries, the knowledge of public demand in the sector being essential to the efficiency of the implementation of security public policies.

In terms of training, the creation of an internal security campus in Lyon was suggested in 2013. This proposition fits into the logical continuity of the city's implications in the field of security. Lyon is an international security actor, particularly active and important. The city is host to Interpol's headquarters, the National Forensic Science Institute headquarters (*Institut national de la police scientifique*), the judicial police's technical and scientific police department and the National school of the police headquarters (*École nationale supérieure de police*). The campus would offer a sharing platform for the various schools, academies, European colleges, institutes and police research centres, with the purpose to gather and harmonise the development of internal security activities and to bring the training programs together. This ambitious initiative, supported by the French Ministry of Internal Affairs and Interpol, meets the needs of coordination to fight against the new security threats, and is destined to become a European centre of excellence.

WHAT ARE THE PUBLIC DEBATES, EXISTING OR FUTURE, THAT CAN INFLUENCE THE MEASURES COMBATTING SECURITY THREATS?

The main public debates lie in the opposition between the exercise of security prerogatives and the exercise of individual freedoms, often summarised by the expression "security vs. privacy". The various reports agree that it is important to bring light on the fact that Edward Snowden's revelations, focusing essentially on the abusive use of data relating to individuals by the American intelligence services, have led the civil society to mobilize against breaches of their privacy. The same applies to the protection of personal data, the people denouncing the practices of law enforcement authorities deemed too intrusive with respect to the pursued security objective. But simultaneously, the very same civil society will accept – or even request – security responses that may translate into a restriction of public freedoms. This paradox is sometimes inherent to technological progress, and this even without public authorities taking restrictive actions.

The digitalisation of societies indeed creates two correlated phenomena. First of all, the possibility for citizens to benefit from online services on which they provide their personal data – such as the data regarding their identity, their banking details, their geographical location, but also their hobbies and interests – allowing to reconstitute the profile of the individuals and to anticipate their actions. At the same time, the communication of all this data allows law enforcement authorities to capitalise on a multitude of new channels, opening a new field to pursue their investigations against criminals or terrorists.

In spite of all those debates and controversies about the abusive use of personal data by police authorities, it is necessary to acknowledge that this trend of citizens deliberately disclosing information concerning them is not regressing, quite the contrary. Thus, to be able to benefit from the comfort of life offered by digital services, citizens themselves put in jeopardy the protection of their privacy and the protection of their personal data.

The **Italia**n report insists on the importance for public authorities to raise the awareness of their nationals on the vulnerabilities they are exposing themselves to because of the use of digital services, even though the respect of the citizens' fundamental rights and freedoms is an obligation of the State, regardless of these individual behaviours. Citizens must be able to rely on some safeguards to limit the risks of abuse.

Then, the question is who, between the legislator and the judicial power, will arbitrate between the security preoccupations and the freedom preoccupations. In any event, the debate stretches over all the countries within the **European Union**, but the responses to it are not identical everywhere.

One can notice that in **Germany**, the judicial power is very present in the debate. It is, as elsewhere, the guarantor of public liberties, but the question is becoming particularly important in this country. The report sheds light on this role. For instance, the German Federal Constitutional Court (*Bundesverfassungsgericht*) found in 2008 that the automated license plate recognition was a violation of the right to privacy, for it did not fulfil a determined purpose, thus criticising the concept of mass surveillance. Closer to us, the law on the storage of data relating to people having committed a serious crime, voted by the *Bundestag* in 2015, has in turn been referred to the German Constitutional Court.

If the judge can limit the risks, the legislator can create them. In **Italy**, a decree on counter-terrorism has been amended to allow public authorities to access personal computers, raising a heated debate within the civil society. This amendment was eventually removed by Matteo Renzi in April 2015.

In the **United Kingdom**, the debate about the Investigatory Powers Bill – nicknamed Snooper's charter by its opponents – has not ceased ever since the bill was introduced. It is perceived negatively by the civil society, which sees it an anti-Snowden law, as it extends tremendously the capacities of accessing telephone communications and Internet connections for police forces. But it is rejected by operators and digital services providers. They believe that the Investigatory Powers Bill won't allow them to protect their clients' personal data anymore. Apple has notably denounced the possibility for public authorities to benefit from a "backdoor access" to encrypted data, which according to the company weakens all data protection devices in general. Petitions are multiplying in the United Kingdom, without the bill being significantly amended so far.

The new law on security in **Spain** has brought about protests as well. In this case, the legislation does not aim at extending the collection of personal data in order to fight terrorism, but rather at limiting advocacy actions on public roads – which has led the opponents to describe it as a "gag law". The aim is thus rather the social movements that have arisen following the economic crisis in Spain.

In **France**, the law on intelligence has also provoked heated debates relating to the extent of the powers granted to police authorities regarding the collection of information. Nonetheless, the debate does not seem to have reached the intensity encountered in the United Kingdom, even though the petition "*ni pigeons ni espions*" ("neither dupes nor spies") has federated several host companies and Internet service providers, as well as the National Digital Council (*Conseil national du numérique*). The National Committee for Computing and Freedoms (*Commission nationale informatique et libertés*, CNIL) itself has expressed reservations when providing its opinion on the subject, in particular regarding the use of data and its retention period.

The protection of privacy is subject to the evolution of the security environment. The more vulnerable a country is, or the more it feels threatened, the more it is likely to enact legislation at the expense of individual freedoms. These violations of freedoms are,

in this hypothesis, legitimised by the threat and the need to have the necessary resources to face it. In this way, the governments hope to obtain the support of their nationals. On this subject, the media also play a very important role. They have a serious power of influence at their disposal and can, by this means, raise the awareness of the citizens about the risks related to the use of Internet or legitimise new legislation enacted for security reasons.

The **Italian** report states that the awareness towards security issues is not equivalent in all of Europe. Western Europe, **France**, the **United Kingdom** and the **Netherlands** are countries where the citizens are the most aware of these questions. By contrast, Southern countries are more preoccupied with migratory issues, while Eastern countries are primarily involved in the protection and integrity of their territory.

The way in which the States enact legislation with regard to data protection varies within the European Union, and reveals different perceptions of the protection that must be ensured for each individual against intrusions into their privacy, whether these intrusions come from State authorities or from private entities. In the South and East, the challenges relating to the protection of personal data seem to be more accessory, without being ignored either.

For the protection of personal data, which is correlated to police and intelligence activities being carried out, the European States also have dedicated structures at their disposal.

Italy, for instance, has had since 1996 an administrative body dedicated to the protection of data, which role is to advise the public authorities and to ensure the respect of the right to data protection and to privacy when new legislations allowing the exercise of repressive activities are drafted.

In **Germany**, at federal level and for each of the sixteen *Lander*, there is a commissioner for the protection of personal data. Their role is to monitor compliance with regulations regarding data processing to which private operators are subject. They can also act as a mediator.

In the **Netherlands**, the creation of an administrative body dedicated to the protection of data also dates back to the 1990s, directly in line with the recommendations of the 1995 European directive. It has power to investigate in order to assess the compatibility of the processing and of the laws relating to personal data processing with respect to fundamental rights and freedoms.

In **Poland**, the Data Protection Authority (*Generalny Inspektor Ochrony Danych Osobowych*, GIODO) was created in 1997. There is a universal legal duty to handle personal data with due diligence. The obligation for registration of personal data sets contains a number of exemptions, including on classified data acquired during preliminary investigation activities, and applies mostly to commercial entities. GIODO can launch a control procedure on its own initiative or after receiving a complaint from

legal entity or private person on the misuse of personal data. GIODO also gives its opinion in the event of a new law on the subject.

In **Spain**, the issue of the protection of personal data is dealt with by the Spanish Agency for the Protection of Personal Data (*Agencia Española de Protección de Datos*, AEPD), which is an independent agency. It has its origins in the Spanish Constitution, in the convention No.108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data, and the directive 95/46/CE relating to the protection of the European citizens' personal data. Following the creation of this agency, the government presented in 2007 a law on the detention of data related to telephone and digital communications, which allowed the use of data banks by security services under the control of the judiciary. The Spanish legislation seems to be cause for satisfaction, since there are very few complaints about a violation of civil rights. The debates that one can witness today in the media about mass surveillance within the context of espionage activities and the fight against terrorism do not lead to repercussions on a national level in Spain.

The precursor in this field remains **France**, which has had a data protection authority ever since the adoption of the 1978 "Computing and Freedoms" law. The CNIL (*Commission nationale informatique et libertés*) currently serves as Chairman of the Article 29 Working Party (Art. 29 WP), which is the European grouping of all the European data protection authorities, and which works on the harmonisation of the protection guarantees on the territory of the Union.

In addition, the **European Union** has an independent supervisory authority for data protection, which role is to monitor personal data processing carried out by the institutions and authorities of the EU, to give advice on policies and legislation relating to privacy, and to cooperate with homologue national authorities to ensure a coherent protection.

Portugal puts an emphasis on the informative role played by the media within the context of societal debates, which is likely to compromise the smooth running of some interventions conducted by law enforcement authorities and to call into question their efficiency. As a matter of fact, it was the subject of intense debate in France at the moment of the 2015 January attacks, when the media had broadcasted some images and communicated information in real time about the conduct of operations, without any concern as to whether or not the terrorists had access to those images and to that information.

Finally, other social issues, notably mentioned by the **United Kingdom** and the **Netherlands**, such as radicalisation, religious conservatism, the integration of Muslim communities, inequalities in wealth on the international level and corruption are listed in the reports as future issues that will instigate public debates.