INHESJ
INSTITUT NATIONAL
DES HAUTES ÉTUDES
DE LA SÉCURITÉ ET DE LA JUSTICE

NATIONAL INSTITUTE FOR ADVANCED STUDIES IN SECURITY AND JUSTICE

TEAMWORKS

27th National Session «Security and Justice» 2015-2016
Strategic Diagnostic Group (GDS) n°3

TOWARDS POLICING 3.0 :

DIGITAL TRANSFORMATIONS IN POLICING TO 2025: ANTICIPATION AND PERFORMANCE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

JUNE 2016
ISSN 2265-447X

Members of GDS 3 :

Chair: **Claire BERNIER,** *lawyer, Partner at Adsto*

Vice-Chair: **Paul-Mathieu LE GAL-OTTAVIANI,** *City of Paris*

Coordinating Editor: **Alain IMBERT,** *Director, Research & Analysis Department, McKinsey & Company*

Alain PERRAUD, *Senior Manager, Compliance, Assessment & Control, Renault*
Céline BRUNEAU, *journalist, i-Tele*
Didier CANNESSON, *Regional Sales Manager, Criminal Justice and Public Security, Morpho*
Philippe CORREOSO, *Colonel, Military Personnel Directorate, French* Gendarmerie
Fadi DAHDOUH, *City Councilor, Troyes, France; osteopath*
Jean-Luc FAIVRE, *commissaire divisionnaire, National Directorate of the French police*
François GARNIER, *Deputy Chief of Staff, Prefecture of Essonne, France*
Christian GRAVEL, *Prefect, Director of France's Government Information Service (SIG)*
Christophe GUEGUEN, *CIO, Securitas France*
Denis LAURETOU, *Head of Security, Banque de France*
Thomas LEGRAIN, *Managing Partner, Thomas Legrain Conseil*
Kristof DE PAUW, *Chief Superintendent, General Director of SAT Justice, Belgian police*
Emmanuel MAGNE, *Director of General Surveillance, City of Lyon*
Olivier ZAMPHIROFF, *magistrate*

This document cannot be considered as an official or unofficial position of the institute or other state authorities. The inputs and recommandations expressed reflects only the views of the authors. It is published under the editorial responsability of the Director of INHESJ.

Publication Director M. Cyrille SCHOTT, director of INHESJ

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

TOWARDS POLICING 3.0
DIGITAL TRANSFORMATIONS IN POLICING TO 2025: ANTICIPATION AND PERFORMA

27th National Session «Security and Justice» 2015-2016

Contents

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

EXECUTIVE SUMMARY

Between now and 2025, a host of disruptive technologies–advanced robotics, autonomous vehicles, the automation of knowledge work, quantum computing, augmented reality and others–will change the face of society and, with it, the security forces. France has begun to make preparations, with a security modernization plan allocating 108 million euros to five priority challenges for the period 2015-2017, but many issues still need to be faced: information gathering and monitoring on the internet, Big Data, the Internet of Things, smart video surveillance, productivity, and numerous others.

Meanwhile, the underworld (whether isolated criminals or terrorist organizations) has been quick to identify the "opportunities" offered by the digital revolution, spawning cybercrime, with new resources and new *modi operandi*. The behaviors and expectations of our fellow citizens have also changed, obliging police forces to develop a new internet presence and to enter into a new era of communication. Even the security forces' relationship with the private sector is affected by these technological developments (collaborating jointly in companies' R&D efforts, bringing experts in on investigations, and helping–in a limited way, so far–to build a French homeland security industry).

How are our security forces approaching this digital revolution? In the past, a number of large-scale technological transformation projects (such as ACROPOL, Embedded Computing Systems, and CHEOPS) ran into considerable difficulties, due mainly to the excessive organizational complexity of the structures tasked with their implementation. The same lack of visibility is found in the management of human resources, where the transformation culture is still insufficiently prevalent despite a number of interesting, but limited, initiatives (commissioned officers in the gendarmerie, training of cybercrime specialists, etc.).

Nonetheless, the digital revolution provides a twofold opportunity: the chance to offer our fellow citizens a new "experience" (new services, new proximity to security forces, etc.), but also an opportunity to optimize ways of working (making the task of the police and gendarmes more enriching, more relevant, and more connected to the populations they serve). France's security forces could strive *"to become–through the use of digital technologies–one of the world's three leading security forces in terms of efficiency and the quality of service provided to all"*.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

To help realize this vision, we put forward an eight-pronged set of recommendations.

- Transform structures by building on a long-term vision: a new orientation and programming law, supporting change, breaking down silos...
- Develop the talents already present in each institution: forward planning of jobs and skills, a dedicated digital investigation branch...
- Attract new talents: a broader recruitment process, an expanded field of commissioned officers, greater interaction with the outside world...
- Implement the digital strategy: a position of Digital Director at the Ministry of the Interior, dematerialization of processes, unification of identification and authentication systems...
- Beef up digital investigation resources: leverage market intelligence to identify digital investigation solutions, acquire solutions, develop a cyberpolice...
- Accelerate and lock in predictive approaches: scale up experiments, including in priority security areas, instill a predictive analysis culture in the organization...
- Modernize command centers: integrate digital functionalities into emergency calls, break down silos; integrate drones, image walls and social networks...
- Initiate a new relationship with the population: reinforcing digital services, encouraging citizen engagement, etc.

The profound digital changes for which France's security forces must now prepare highlight the absolute necessity of putting the human factor—in the form of citizens as well as members of the security forces—back at the heart of the system and at the center of government action.

INTRODUCTION

Like the invention of printing, electricity or computing, the digital revolution is reshaping our society, and will continue to do so, deeply and lastingly. And because it creates new ways of relating to the general public, optimizes the impact of actions by making massive use of data, frees up time (or cuts costs) by overhauling processes, and enables services to be better tailored to needs, the "digital big bang" promises greater efficiency and effectiveness in every type of organization, whether in business or government. It can also represent a positive aspiration for all who implement it or who become its future users.

Policing is no exception–it, too, is being reshaped. Digital initiatives are multiplying throughout the world: in New York, with predictive policing tools; in London or Madrid with the use of the internet and social networks to communicate with citizens; in Tel Aviv, with smart surveillance cameras; or in Singapore, where Interpol inaugurated its Global Complex for Innovation in April 2015.

In a speech to the French security forces on September 30, 2013, Manuel Valls, then minister of the Interior, called for work to begin on "*a new frontier*", that of "*the police and* gendarmerie 3.0", declaring his determination to anticipate and prepare for the future through forward-looking thinking on topics such as intervention equipment, the Internet of Things, online public services, mapping tools, Big Data forensics or, more prosaically, ways for France's police and gendarmerie to share knowledge and resources.

Wherever we look in the world, and at whatever period in time, the history of the police shows that it has always been in a position of reactive adaptation rather than proactive evolution. Could it be otherwise with the digital revolution–of which criminals, gangs, and terrorist networks have already shown themselves to be early adopters?

In the course of their research and interviews with experts, the authors of this report have acquired the conviction that the digital revolution is not some kind of massive technology upgrade; it is–as Part One of this document shows–a paradigm shift. To which the response can only be a cultural and organizational revolution, as described in Part Two. To spark that revolution, we make 30 recommendations, organized into 8 broad themes, in Part Three. A third of these recommendations could usefully be implemented in the short term.

Because it accelerates time, digital obliges police forces to adapt even faster than before.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

DIGITAL REVOLUTION: DIAGNOSTIC AND OUTLOOK

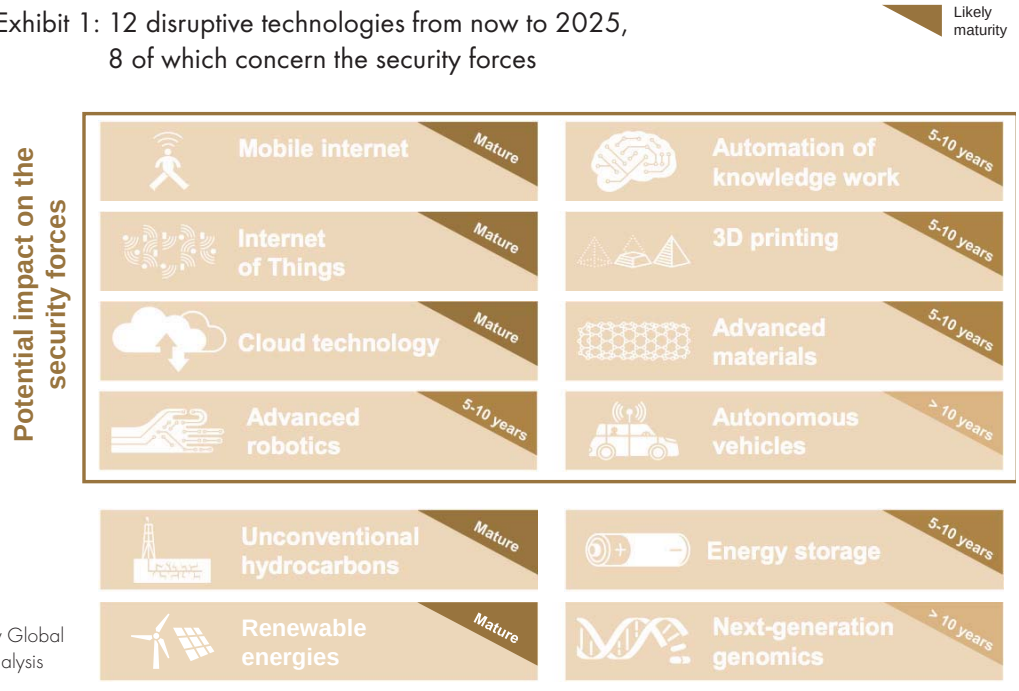
Towards a world reshaped by disruptive technologies

In a report published in May 2013,[1] the McKinsey Global Institute identified twelve disruptive technologies likely to bring about radical social transformations by 2025. Some of these will affect the security forces, directly or indirectly, and examples of possible uses are limited only by our imagination:

- Mobile internet will enable remote access to databases or business applications that consume ever more bandwidth;
- The Internet of Things could become a source of intelligence or even surveillance, just as telephony is today;
- Advanced robotics could enhance the capabilities of intervention forces (carrying heavy loads, neutralization, etc.) and lead to new forms of collaboration between humans and robots (bomb disposal, surveillance, etc.);
- Autonomous vehicles will modify the approach to road checks;
- Etc.

(1) Disruptive technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute, May 2013.

Exhibit 1: 12 disruptive technologies from now to 2025, 8 of which concern the security forces



Source : McKinsey Global Institute, authors' analysis

Augmented reality[2] will also open up new fields. For example, it will allow intervention forces to exchange information in real time (e.g. location, suspicious presence, physical state of operatives, etc.).

(2) The creation of an environment where information from various sources–Google glasses, Thales 6W4U connected watch, etc.– is superimposed over our own vision or preception of a scene.

Finally, quantum computing will bring further disruptive change. Computers will acquire a processing power 100 million times greater than that of today's computers, making current encryption techniques, for example, obsolete.

Homeland security actors and decision-makers must, of course, reflect carefully on these prospects and what they imply not only in terms of resources, but also of work methods, capabilities to be acquired, or training to be developed.

Security forces, criminal networks and civil society: the applications and implications of digital

The internal security modernization plan

Origins and ambitions

In September 2013, France's Interior Ministry set up a Working Group on Internal Security Technologies (French acronym GTTSI), to accelerate the uptake of technological advances and digital innovations by the police and gendarmerie. Its findings (five-year strategic outlook and forward vision to 2025) culminated in the submission of a report in June 2014,[3] containing action orientations that were validated by the ministry. The main projects are programmed and overseen in the framework of the three-year budget for 2015-2017, in which they are allocated an envelope of 108 million euros..

(3) Delville Report: *Les défis technologiques des forces de sécurité intérieure*, June 2014.

Five priority challenges

In concrete terms, the Security Modernization Plan (PMS) that emerged from this work centers around five priority "technology challenges", described below. While all of them seem to be moving in the right direction, some (notably online services for citizens and predictive tools) could have demonstrated a more immediate sense of ambition.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

• *Develop "digital proximity" to the public*

Despite its declared intention of pursuing and reinforcing the approach already adopted on the interactive use of new communication supports with the population (e.g. online pre-reporting, etc.), this strand of the modernization plan may seem somewhat lacking in ambition. It is essentially limited to the online reporting of internet fraud and ability to sign up for "*Opération Tranquillité Vacances*"–to have patrols run a visual check on one's home during vacations– on France's e-government site "service-public.fr". The communication strand, aimed at reaching out to the general public, has thus far been totally neglected (attractiveness of the ministry website, visibility on social networks, etc.)..

• *Unify emergency call platforms*

This aspect of the PMS is more ambitious, by contrast, in that it aims to unify the emergency call platforms (for emergency numbers 17, 18 and 112) within each of France's *départements*, in line with an experiment under way at the Police HQ (Prefecture) in Paris since the spring of 2016. The objective is to achieve more effective coordination between services (police, *gendarmerie* and firefighters), ensure better response to life-threatening emergencies (including *via* stronger filtering of non-urgent calls) and guarantee more efficient crisis management, while diminishing financial and personnel costs through the pooling of resources..

• *Implement mobility solutions (digital equipment)*

The aim here is to equip every ground-level police officer and *gendarme* with a secure mobile terminal capable of carrying the necessary tools: access to files, messaging, certain strategic applications (electronic fines and reports, OCTET for dealing with traffic offenses, etc.) and also the internet. These terminals take the form of tablets and smartphones using a version of Android secured by ANSSI (SecDroid).

Mindful of this goal, and of the obsolete character of the existing embedded computing system (TIE), the *gendarmerie* in the Nord *département*, in liaison with the national police force, has been road-testing a new digital device called Neogend (or simply Neo for the police version) since the end of 2015. The gendarme or police officer is no longer tied to his or her desk for every single activity, and so enjoys greater freedom of action. With their integrated tools, Neogend and Neo enable interaction with internal and external correspondents, and make it easier to signal offenses, look up files, access various mail clients, draw up incident reports and take notes. It can also perform optical MRZ scans (on identity cards, passports and vehicle registration documents). The "*Opération Tranquillité Vacances*" application helps keep track of registered users. The built-in camera can be used for anthropometric images or photographs of incidents, which can then be easily inserted into the paperwork. Finally, an operational mapping application can geolocate nearby patrols and on-going incidents, acting as a decision aid and facilitating the operational handling of interventions.

After collating the feedback from these initiatives, the Internal Security Procurement, Equipment and Logistics Service (SAELSI) will be tasked with issuing a public contract at the end of 2016 to equip police and gendarmes with off-the-shelf terminals between 2017 and 2018.

• *Modernize and converge radio networks*

The Interior Ministry currently has two distinct radio networks: Rubis for the *gendarmerie* and INPT (*infrastructure nationale partagée des transmissions*), which is mainly for the emergency services (police, fire and ambulance) and for prefectures.

The objective is to converge the two networks, which will reach the end of their lives by 2025, not only to make substantial savings (their maintenance costs tens of millions of euros every year) but also to increase the efficiency of communications (e.g. in crisis situations where the massive presence of services in a limited geographic area saturates the networks), while at the same time allowing new users (customs, municipal police, etc.) to be included.

• *Introduce predictive and decision-making tools*

The adoption of predictive and decision-making tools should optimize the use of available resources at ground level.

In concrete terms, this involves using advanced statistical analysis techniques to study and analyze the phenomena of crime, public disorder, road safety and emergencies—as described in the police and gendarmerie information systems—in order to anticipate them more effectively. By supporting this "predictive" approach with geo-spatial analyses and mapping tools, the ministry would give the police and *gendarmerie* the means to better allocate their resources on the ground day-to-day, or even hour-to-hour.

To this end, the Internal Security Information Systems and Technologies Service (ST(SI)²) and the Central Criminal Intelligence Service of the *gendarmerie* (SCRC) are currently working on expert systems based on mass data analysis and business intelligence solutions.

What makes this approach so ambitious is that, until now, the services have always had the greatest of difficulty in producing crime or accident maps worthy of the name; they have usually left it up to ground-level units to devise the mapping tools they required, in as far as local resources allowed.

By choosing to focus its predictions on the month or week, the SCRC seeks to work on a long time scale, aiming for a lasting impact in the long term. Drawing up a monthly map of risks is a way of leaving the initiative with the operatives and getting all of society's actors (prefects, the voluntary sector, private players, etc.) more involved in a consultation process. The experiments under way at the start of 2016 in *Aquitaine* (all types of minor crime, in the jurisdiction of the gendarmerie only) and in département of *Oise* (car thefts in both police and gendarmerie zones) will provide a measure both of the relevance of these tools and their take-up in the field.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

The need for the security forces to master the digital universe

The implications of information gathering and web intelligence

The security forces have specialist cybercrime units equipped with considerable human and material resources. While a degree of web intelligence is performed to forewarn of large gatherings of people, which are relatively easy to detect, criminal intelligence gathering has for several years been a constant–and constantly evolving–focus of effort.

Every month in France, some 3,000 complaints from victims of cybercrime-related offenses are recorded by *gendarmerie* units alone.[4] The total loss is put at more than 3.5 million euros a month. Aside from data theft, cybercrime encompasses two families of offense: those that make primary use of digital technologies, such as the dissemination of illegal content (child pornography, promoting terrorism, etc.) and ordinary crimes that make accessory use of the internet, such as classified ad fraud, handling stolen goods online, or selling regulated products.

(4) The corresponding data for the National Police are not available.

In recent years, the *gendarmerie* has developed a network of some 2,000 gendarmes operating in cybercrime-related fields, spearheaded by the 260 investigators of "N'Tech". At national level, the network is run by the territorial coordination foresight department at the C3N digital crime-fighting center, which itself is integrated into the Central Criminal Intelligence Service (SCRC). The C3N is responsible for harmonizing the training, equipment and working methods of these "cybergendarmes".

The national police, meanwhile, have 430 "investigateurs en cybercriminalité" (ICC), who are trained by the DCPJ (Central Directorate of the Judicial Police), where half of them are also deployed.

The DCPJ has also set up a central office for the fight against ICT-related crime (OCLCTIC), which includes the platform for harmonizing, analyzing, cross-checking and referring reported infringements (PHAROS), to which internet users can report any web content or behavior they believe to be illegal. In 2015, PHAROS received and processed 188,055 notifications, covering such varied fields as internet fraud, child pornography, or the promotion of terrorism.

The implications of Big Data

Big Data handles billions of pieces of information in real time. Its analysis and interpretation identifies trends, enables foresight or anticipation, and provides support for decision-making.

In a preventive approach, the goal of Big Data for the security forces is to identify the places and periods where an unfavorable trend in crime levels is likely to surface.

But Big Data can also be an investigative tool. Gathering data from connected objects can, for example, help to improve road safety and reduce the causes of accidents (connected cars). The processing and exploitation of intelligence

in the maintenance of public order (preventing events such as "*rave parties*" or other large gatherings of people) and in the fight against personal abuse (pedophilia), organized crime, terrorism, fraud, economic and financial offenses, or even in cybersecurity (detecting attacks and identifying hackers) are further areas where Big Data will bring real added value.

Currently being developed on a massive scale, Big Data tools open up new horizons for security forces by expanding their scope of action. So much so that public authorities have sometimes taken the initiative in centralizing security data. The city of Turin recently put in place a test platform covering several districts. Shopkeepers can record their video surveillance images on the city's secure servers. The program centralizes information (ensuring easier exploitation) for the benefit of the security services, and enables experiments with smart video surveillance (real time analysis, forensic methods, etc.).

However, the potential collusion between Big Data and Big Brother–fuelled by the place that computers and the internet now occupy in the lives of our fellow citizens–constitutes a threat in the eyes of some (e.g. the digital rights advocacy group "*Quadrature du Net*", etc.). The logic of controlling flows must therefore be counterbalanced by guarantees that every such action will be taken exclusively in the public interest.

The implications of the Internet of Things

There are now estimated to be more than 9 billion web-connected objects in the world, including computers and telephones. By 2025, projections suggest up to 1,000 billion connected objects.[5] Their growing use will have strong implications for data security and privacy. US Director of National Intelligence James Clapper went so far as to state, at a Senate hearing in Washington: "*In the future, intelligence services might use the [Internet of Things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials*". [6].

(5) McKinsey Global Institute, ibidem

(6) Le Monde, February 10, 2016

Electronic component designers are making efforts to integrate the security dimension into the objects they produce, given the multiple risks.

The risk is above all economic. Customer trust must be preserved by ensuring that personal data remains confidential, that transactions are secure, and that systems are protected against computer attacks and malicious software. The risk can also concern public health, notably when it involves devices that are directly related to patient care (e.g. for the remote control of medical equipment).

The responses to these threats are decidedly weak. In France, the "*Informatique et Libertés*" law of 1978 has been amended and updated from time to time in an effort to protect personal data as well as possible, but it applies only on French territory and outside the private sphere. Likewise, at the European level, while a European regulation for the protection of personal data was finally adopted on

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

April 2016, it does not come into effect until the second quarter of 2018, and will only cover the points on which the Member States have reached consensus. The stumbling blocks–sometimes crucial for better protection and management of the data concerned–will continue to be managed by each State through its national legislation. But despite this political will and a number of attempts–and even significant advances–by the authorities to supervise and regulate these exchanges of data, the issue remains unresolved. How can we preserve the confidentiality and integrity of the vast quantity of data collected by connected objects and exchanged with other connected objects, on the internet or with servers dotted around the globe?

There is currently no answer to that question. And international law–less so even than French law–is not geared up to address it.

The implications of smart video surveillance

Its adoption curve was comparable to that of connected objects and it soon became part of the security forces' toolkit in its own right (with fixed, dashboard and body cameras), but "traditional" video surveillance is already evolving, or even disappearing, in favor of "smart" systems.

Aided by a favorable context–ideological and social maturity on the one hand, and technological opportunities on the other–new generations of cameras and algorithms are now emerging. Automatic anomaly detection, people monitoring, reaction to sound signals, facial recognition, vehicle tracking... these will become core features of smart video surveillance systems. These systems will then be even more powerful tools to help prevent, investigate and elucidate crime and intervene when required.

So great is their potential that the ethical, deontological and legal limits that restrict the current use of video surveillance will need to be kept in line with social and societal requirements. And yet the interministerial decree on the technical standards for these systems dates back to 2007; there is already a clear gap with the current capabilities of the equipment. Once again, the law needs to evolve.

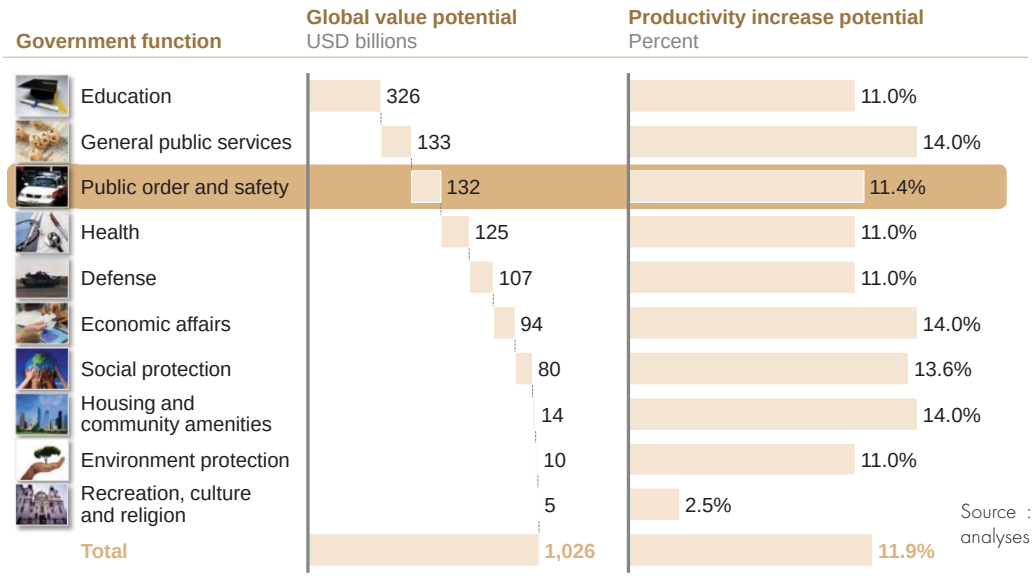
The implications of productivity

In addition to making concrete contributions to the basic policing, the digital revolution also represents, more generally, a significant new source of productivity for all public services. McKinsey experts evaluate the gain at just over 10% for internal security services. Expressed in terms of working hours freed up or reassigned, this represents, for France, the equivalent of more than 20,000 full-time police or *gendarme* posts.

Crime goes digital

Since the 1990s, easy access to the internet and falling technology prices have led to the rapid democratization of information and communication tools and their use–for honest ends or otherwise.

Exhibit 2 : The digitization of public sector services has an estimated productivity impact of more than 1 trillion USD annually on a global basis



Source : UN Statistics: OECD, analyses McKinsey

The characteristics of cybercrime

Two categories of cybercrime threat can currently be distinguished:

- Those where the technologies give rise to offenses that did not previously exist (denial of service,[7] advanced persistent threats (APTs),,[8] website defacement,,[9] etc.);
- Those that use these technologies as a vector to commit "traditional" offenses (scams such as phishing, Nigerian "advance fee" confidence tricks, attacks on automatic data processing (ADP) systems to steal data or files; ransom demands in bitcoins,[10] etc.).

In both cases, thanks to these technologies, the offense is committed remotely and anonymously. Perhaps by a lone individual, with the support of an extended technical and IT network, or acting as part of an organized but geographically dispersed gang. The offense may be local in character (e.g. a desire for vengeance against a former employer, partner or spouse, etc.) or international (geographical, political and economic boundaries no longer exist). It need not necessarily demonstrate a high degree of sophistication (indeed, it may well be committed without any great intellectual or physical effort, so much so that some cyber-offenders fail to realize the seriousness of the crimes they are committing).

(7) Saturating a website by flooding it with simultaneous requests in order to make the service unavailable.
(8) A recurrent attack that exploits complex mechanisms or hitherto unknown vulnerabilities (e.g. the attack on TV5 Monde in April 2015)
(9) Taking control of and modifying a website without permission
(10) A virtual digital currency

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

The offense may be all the more stealthy or undetectable in that it is performed *via* closed networks (virtual private networks or the "Dark Net") or by hijacking PlayStation or similar networks, etc. In every case, its financial, political, strategic or reputational consequences will be almost immediate and may be calamitous (temporary but serious or even irreversible destabilization of the target).

Factors in the development of cybercrime

The growing democratization of technology is not the only fertile ground for the growth of cybercrime. The spread of free or near-free installation and use is, of course, another powerful lever. But its development also feeds on a conjunction of other elements:

- The growing importance of dematerialized IT assets;
- The weak culture—and sketchy practices—of data protection among the general public and, indeed, in business;
- The continuing explosion of websites and web pages, making it almost impossible to keep tabs on them;
- Technological barriers (encryption of communications, onion routing through the Tor network, etc.) that are sometimes insurmountable for investigators;
- A form of commercialization of cybercrime (computer viruses, cyber attacks and even weapons can be purchased in just a few clicks);
- Shortcomings in international police (and even judicial) collaboration, leading to failed prosecutions;
- Legal loopholes: not every country has integrated the various aspects of cybercrime into its legislation (recognition of virtual identity and prohibition of virtual identity theft, data theft, attacks on ADP systems, etc.).

This type of crime may be new in terms of its means and modus operandi, but its motives are as old as the hills: ideology (terrorism, sectarianism), revenge, greed (quick and easy money), the sheer intellectual challenge, or just for kicks (demonstrating technical prowess without financial or malicious intent).

New interactions with citizens

The paradox of privacy in an ever more digital society

In the space of a few decades, new information and communication technologies have radically transformed our fellow citizens' attitudes and behaviors: mobile telephones, the internet, smartphones and tablets have become day-to-day objects. Fast broadband makes it easier to work remotely or on the go. People shop, get information, and even file their taxes online. Social networks are creating new ways of relating to each other. Opinions are volunteered more freely and more spontaneously. "Sharing" and "collaborative" are the buzzwords of the

new economy that is taking shape. The public, meanwhile, is developing new requirements with regard to the internet: quality of goods and services proposed, fluidity and design of applications, secure transactions, histories and tracking, protection of personal data, and so on.

The digitization of the economy is developing the force of a standard, one that will impose its rules, usages and values on the whole of society. Public services–including the security services–will be no exception.

The fact remains, however, that the digital revolution partakes of a profound paradox. With the development of websites like *Dailymotion*, *Facebook*, *Flickr, LinkedIn, Twitter* or *WhatsApp*, our contemporaries have opened up their private lives to public view as never before. So much so that even those who do not have a personal account on any of the social networks may well nonetheless have a substantial online presence, generated by the activity of their partners, parents or close friends. [11] But at the same time, our contemporaries demand total protection of their privacy and are inclined to protest any interference by government, even if it is in the name of counter-terrorism and the defense of freedom. As we heard during our interviews: "*We give the web giants everything; but we refuse to give information to the authorities, although they, at least, are monitored.*"

(11) As in the case of Edward Archer, who opened fire on a police officer in Philadelphia on January 8, 016: his mother's posts on the internet confirmed his links to Daech.

Further progress is required on web-based services

In response to public demand–but also because it holds out real opportunities for transformation–the security forces will be able to capitalize on the benefits of digitization to build a new relationship with citizens, and even reconcile some people with their police force.

There have already been a number of initiatives in this direction, including internet recruitment notices, Twitter accounts, online pre-reporting of incidents, signaling of illegal web content (PHAROS) and a platform for referring cases to the IGPN (France's internal police investigation unit). However, the approach taken could be accused of still being very institutional and overly focused on communication and "image", to the detriment of any real service delivery, making it difficult to create and consolidate a sense of proximity.

A glimpse at the best practices of major foreign police forces suggests several potential lines of progress.

In Spain, the national police decided in 2006 to develop a social network presence. This approach, initially targeted at the media, gradually expanded and then refocused on the general public (institutional communication, prevention messages, operational intelligence gathering, etc.). The eight people who currently run the mechanism have succeeded in creating a genuine dialogue with citizens (young people in particular) and are in effect managing the *Policía Nacional* "brand".

Exhibit 3 : Spain's Policía Nacional sleverages the social networks to develop its proximity with citizens

An active presence on the major platforms…

YouTube:
- 300 videos
- Seen over 6.7 million times
- Largest viewer figures of any Spanish government service

Twitter:
- 2.3 million followers (more than the FBI or the White House; #1 police force worldwide)
- 10 to 15 tweets per day

Facebook:
- 400,000 friends
- Advice, answers to questions…
- 25 to 30 personalized responses per day

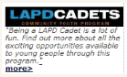
Instagram:
- 100,000 friends

… which host regular campaigns

Source : Policía Nacional, Oficina de Prensa y Relaciones informativas, april 2016.

Exhibit 4 :Numerous channels and services can be used to reach out to the general public

Examples of channels and services available online



Street-by-street crime figures available online

Free mobile apps e.g. to track neighborhood crime, etc.

Raw crime statistics available for download
(open data policy)

Source : McKinsey (Police service line, 2014)

Other international examples suggest further pertinent ideas:

- In Los Angeles, the police use multiple channels to create and maintain proximity to citizens: activity reports, "[monthly] messages from the Chief", security advice, appeals for witnesses, traffic updates, online questionnaires, recruitment notices, pages for the Spanish-speaking community, etc.;
- In London (as in Los Angeles), the Metropolitan Police web pages provide access to crime data with extraordinary geographic precision;
- The Met website also offers pages dedicated to assisting victims and witnesses.

Positive pressure on quality of service and ethics

Regardless of which digital services are deployed, and of how responsive the police officers and *gendarmes* prove to be, the security forces will also have to get used to a form of positive pressure on quality of service, imposed by the digital revolution. One need only *Google* the name of a police station, for example, and one can now rate it and post a review of it. More commonly, police interventions are now filmed on mobile phones and the images circulate at lightning speed, even making headlines, especially if they are "spectacular" or depict inappropriate police behavior. Businesses such as Citizenside have made a specialty of this kind of "participatory journalism" and offer to pay between 20 and 900 euros for a photo or video.

The digital revolution–the first revolution in which organizations lag behind society–is above all a revolution in usage. The challenge for the security forces, therefore, is to take ownership of the more innovative uses. The body camera is a step in that direction. Experience shows that it does indeed reduce tensions. Active, or even proactive, advocacy on social networks would be another positive step.

All the tools and technology aside, the digital revolution also calls for a stronger public stance–and better training–on ethics-related issues, with specific training, where required, in quality of service: what it means, and what form it should take in policing.

Partnerships with the private sector need more work

The standoff between the FBI and Apple at the start of 2016 over access to the content of the iPhone that belonged to one of the San Bernardino terrorists [12] illustrates a phenomenon that could well have increasingly heavy consequences in the coming years. Data security mechanisms–and, in particular, encryption technologies–are now more powerful than investigation techniques. The algorithm used by the Apple encryption engine, AES 256, had never previously been hacked, and only lengthy research (or brute force, i.e. testing every combination one by one) seemed to have any chance of doing so.

(12) A shooting on December 4, 2015 in the USA in which 14 people were killed. Daech claimed the attack was carried out by two of its followers, who were neutralized by the security forces as they were fleeing the area. In the end, the FBI unlocked the device with the help of a third party..

If bypass options (back doors, protection deactivation mechanisms, etc.) are not built into products at the design stage, raising the issue after the event is only going to make matters worse. Conversely, if these solutions exist, or if the ability to create them does in fact exist, then refusing to comply with a judicial requisition would constitute a tier-2 offense under French law.

The development of services and technologies opens up numerous opportunities for collaboration between the security forces and the private sector. Communication tools, two- or four-wheeled vehicles, financial dematerialization, connected objects, domotics and smart electricity meters can all serve as sensors to monitor, detect, or simply foil criminals.

In this context, should private companies integrate the potential needs of the security forces into their product development and their security architecture? We believe collaboration is clearly possible, providing it is organized.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Participating in companies' R&D projects

To be fruitful and enduring, collaboration between the private sector and the police or the *gendarmerie* must be organized by formal protocols, clearly setting out the objectives, the principles, and the modalities of exchange.

In 2012, for example, *Renault* signed an agreement with the national gendarmerie on the fight against auto theft. In concrete terms, the *gendarmes* gain access to the carmaker's technical toolboxes and databases, while *Renault* compiles an up-to-date knowledge base on auto theft techniques as observed by the *gendarmes*. To facilitate these exchanges, the two partners have set up dedicated teams who have developed a close working relationship.

It is the win-win nature of this exchange that enables this collaboration to endure, and to call itself a partnership:

- The private sector needs to be able to draw on the security forces' knowledge of crime in order to gain a better understanding of theft techniques and improve its security devices;
- The police and *gendarmes* need to be able to express their needs upstream and be involved in projects that affect them right from the design phase.

To initiate this type of agreement–ensuring that such agreements are of mutual benefit and that they generate positive emulation between private sector firms–the security forces must join together in a single structure. We believe this could be one of the missions of the Ministerial Delegation to the Security Industries (DMIS). It would be tasked with identifying firms eligible for such partnerships, formalizing the agreements, appointing appropriate contact persons in the police, gendarmerie and General Directorate for Internal Security (DGSI), and supporting foresight activities.

The only way to achieve real advances is through a joint effort of forward planning: the private sector does not know what the security forces need and conversely, the latter know nothing about the development plans of the private sector.

Helping with inquiries

Collaboration within the framework of actual investigations is increasingly common. This may involve the requisition of persons, or official requests for assistance or expert assessment.

Given the rise in the number of requests (particularly onerous for the private sector when they take the form of successive requisitions), these exchanges could be facilitated and accelerated by putting in place a one-stop shop information system, shared by all of the security forces, who would benefit in return from having dedicated contacts in the private firms. Such a system already exists in the world of telephone operators.

There is also the question of the cost of dealing with requisitions: the workload must not be intolerable or persistently disruptive for the requisitioned firm, nor must it be a source of recurrent and disproportionate revenue. Collaboration should take place in a balanced spirit of *pro bono* cooperation.

Finally, it should be possible to mobilize private expertise during the upstream phases of investigations (e.g. detecting suspicious travel or financial movements, using banking transaction data in scoring terrorism risk, monitoring social networks, etc.). The question that often arises in such cases concerns the accreditation of the expert or the person who will be party to the information. One solution might be to operate a strict silo system, such as Interpol put in place for its INVEX [13] program. While national laws do not allow private actors to access data on stolen vehicles, Interpol plays an intermediary role, consolidating data from the countries that adhere to the program and disseminating it to the carmakers, who can then alert the authorities if a listed vehicle turns up at one of their dealerships.

(13) *Interpol vehicles data exchange*

France's security forces could take inspiration from this example to expand collaboration protocols, being careful, however, to protect the status of the expert, whether paid or pro bono. An expert's knowledge of the facts (e.g. a vehicle brought in for repair work is sought by Interpol) should not be allowed to jeopardize his or her position with regard to the customer or to the legal system (in our example, the work on the vehicle is subject to authorization by the security forces. If they are slow to give the green light, the customer will complain about the delay in repairing his vehicle. If the mechanic acts without that authorization, he could be accused of complicity for erasing data or alert messages from the vehicle computer).

France's internal security industry needs to be developed further

While France has managed to develop a world-class defense industry–thanks to the structure and volumes provided by government contracts–the same clearly could not be said of its internal security industry. The government certainly lays down plenty of requirements, but it places relatively few orders. And it isn't just volumes; there seems to be a lack of vision about hardware needs in the mid to long term. Unless demand is structured, it is almost impossible to structure supply, let alone drive the industry's ecosystem and its R&D.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Building a mid- to long-term vision of the needs

To move forward, the manufacturers have broached the idea of defining needs by sector and by core mission (e.g. security forces' needs in urban areas and at protest sites, the needs of the intelligence services with regard to unattended sensors, etc.).

While the UK and US governments are willing to take technological and industrial risks, decided upon by proper investment committees, the French approach consists of demanding demonstrators. This administrative inflexibility slows down the government procurement process and weakens its potential knock-on effect. France would benefit from taking more industrial risks.

Giving more power to the Ministerial Delegation to the Security Industries (DMIS)—which could become the internal security equivalent of the DGA [14] – would enable the expression of needs to be organized by core mission and allow for faster validation of concepts, shortening the time taken to move from PoC to PoV [15].

(14) The *Direction Générale de l'Armement*, France's military procurement agency.

(15) Proof of Concept and Proof of Value, respectively.

Investing in the inIdustry to support its development

If they are to develop a French offering for the export market, manufacturers require an increase—they speak of a doubling "as a minimum"—in the amount of investment devoted to internal security demonstrators. At a time when the country is putting together its third Future Investment Plan (PIA), with a total envelope of 10 billion euros, it is surely regrettable that no credit lines are specifically allocated to sensitive internal security topics such as IT security, encryption and web surveillance. In particular, the government, and even the European Union, would gain by supporting French tech firms Bull and Atos in the development of supercomputers, a promising market disputed by a handful of players: Americans, Chinese, Japanese... and French. The ability of quantum computers to break access codes, for example, will make them a major issue of national sovereignty in a few years' time.

On a more symbolic level, if our country wishes to acquire a world-class security industry, then our government must provide it with technological showcases capable of winning future customers. French manufacturers will then be able to organize visits in France; visits that are currently "offshored" to Abu Dhabi, Dubai, Mexico City or Singapore.

CULTURAL AND ORGANIZATIONAL CHALLENGES: ADAPTATION OR REVOLUTION?

Some lessons from past experience

While large national files such as the automated fingerprint file (FAED) or the national automated genetic fingerprint file (FNAEG) are undeniable successes, many projects implemented in recent years at the Ministry of the Interior have been at best half-successful, and more often significant failures.

Several business applications (though there is no suggestion that all options were tested) failed to produce the expected results, or at least not within the announced timeframe.

In addition to the red tape inherent to public contracts, the organizational structure of the Ministry of the Interior—and in particular of the national police—itself acts as a barrier to implementing and managing technological change.

Depending on their geographic location, police services are placed under the authority either of the National Police Directorate (DGPN) or of the Paris Prefecture, and are then split between various operational departments, each of which is keen to cultivate its own particularities and is jealous of its prerogatives, which are often simply a matter of historical legacy. From this point of view, the contrast offered by the national gendarmerie is striking. In addition to these particularities comes the positioning of the Information and Communication Systems Directorate (DSIC) within the General Secretariat of the Ministry of the Interior: part of its area of competency includes the national police (but not the gendarmerie, which has always had its own resources).

Given the silos inherent in any bureaucratic structure, and an organization more akin to "organ pipes" than to a pyramid, the management of new technology projects is, at the very least, slowed down, when it isn't hampered by inter-service rivalries and difficulties in cooperating. De facto, there are usually significant delays involved in rolling out such initiatives, as is evident from a number of examples:

- ACROPOL (automation of police operational radio communications), the encrypted radio communication system used notably by the national police. This system—essential to the reliability and confidentiality of police

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

radio communications–initially ran into problems with the definition of needs (mainly due to the multiplicity of departments involved) before it began to be deployed, but only very gradually, in 1995. In fact, it was only in 2007 that the last département teams were equipped. According to the assessment in the Internal Security Modernization Plan (see earlier), this network is now obsolete, only eight years after being fully rolled out, despite the fact that its deployment began twenty years ago.

- A similar technology lag was observed with the police intervention management tools (PEGASE – CORCICA) used in the major information and command centers (of which there are currently 48), mainly in public security. While the product delivered in 2004 was well received by its users, its development was costly in terms of time, and its deployment turned out to be particularly slow (the last information and command center, that of the DDSP in Essonne, was equipped with PEGASE in 2015), so much so that it, too, became obsolescent shortly after entering into service.

- Embedded computing systems (known as TIE, terminaux informatiques embarqués) carried on police vehicles offer another illustration of an unsatisfactory product that had already reached its shelf-life by the time it was delivered. Following on from other projects in the 1990s (SITTER and TESA) that never won general acceptance from the services, the TIE is based on a totally outdated technology that fails to meet user expectations. And yet more than 8,000 of these devices are now in use in police and gendarmerie vehicles, without having demonstrated their efficiency at the operational level. Meanwhile, the "4-in-1" component on certain terminals (for automatic scanning of administrative documents such as drivers' licenses and identity cards) resulted in a resounding fiasco and never really worked.

- The CHEOPS portal, a tool developed and maintained by the DSIC, provides Ministry of the Interior officials with secure access to the various police files [16] and to certain professional applications [17]. CHEOPS proved satisfactory at first, but with the gradual addition of new functionalities over the years, and exponential growth in the number of profiles tailored to each user's privileges, the system rapidly began to suffer from saturation, making some files and applications unavailable, to say nothing of the tangle that it now represents for local accreditation managers who need to create or modify the rights of the various users. The migration–once again slow and over-schedule–from CHEOPS (fat client) to CHEOPS-NG (new generation: a web application with ST(SI)² supervision) only went part of the way toward solving the problem.

- The national police report editing software (LRP-PN) had a particularly hard gestation period, weighed down by delays and difficulties. It was originally announced in 2007 under the acronym ARDOISE. All of the report-writing personnel in the national police were given training in 2007 and 2008 to prepare for the supposedly imminent arrival of the new report editing software. Given the sheer immensity of the unresolved technical difficulties, the project was eventually withdrawn without ever having been installed at office level; only in 2011-2012 was a new version delivered to police officers and agents (after training them in its use for a second time). It is telling that the national

(16) FPR, FOVeS, TAJ, SNPC, FNE, ...

(17) PVe, WinOMP, LRP-PN, ...

gendarmerie, faced with the same need to provide its staff with software of this type, was more modest–but more realistic–in its ambitions regarding the tool's functionalities, bringing a community of front-line *gendarmes* in on its development to make sure the expectations of the regional units were heard. This enabled the gendarmerie to deliver their solution several years before the police.

- Despite this greater realism, the *gendarmerie* also encountered difficulties implementing certain applications developed by its own resources. This was the case, for example, with Pulsar, which offers several functionalities essential to the work of the units: managing mail, activity, offense notifications, and privileges (issued by accreditation managers) and creating duty rosters, accident reports, minutes of meetings, and statistics, not to mention community profile and budget monitoring files. In 2005, a consortium of companies developed the first version of Pulsar, without managing to finalize the departmental version "Pulsar Service". The *gendarmerie* then abandoned the project–having already trained its middle-ranking staff–until a group made up exclusively of gendarmes took it over in 2011.
- More recently, in a move to adapt to changes in qualification levels on *gendarmes'* professional ID cards, the ST(SI)² signed a contract to modify the profile of the microchip embedded in the cards. But these cards are used for access to certain applications, and the adjustment will affect the way those applications work. In the summer of 2016, 40,000 *gendarmes* will no longer be able to use the notification terminals installed in their units.

These examples illustrate the difficulty of the task of implementing new IT systems, or any kind of innovation, within the Ministry of the Interior.

The central administration, in its broadest sense, seems to get embroiled (and sometimes bogged down) in projects that inflate to mammoth proportions, while overlooking more modest initiatives that nonetheless correspond to the day-to-day needs of front-line services. This particularity explains why, for so long, decentralized services resigned themselves to developing their own tools by calling on the IT skills of their personnel, rather than waiting for solutions to come down from on high, which led–probably quite unnecessarily–to a multiplicity of parallel solutions. Even if these practices no longer continue unbeknownst to the central authorities (which remains to be seen), the excessive multiplication of similar IT applications clearly does not contribute to efficiency or to the careful management of limited resources.

In this respect, it is interesting to note the decision taken by the Director General of the national police who, in a memo dated April 3, 2014, set up a "national police development community" with the aim of prohibiting the unregulated practice of IT development in regional services. This "community" was to be made up of developers present at ground level, who would volunteer to integrate a structure federated by the ST(SI)², which would in turn supply the appropriate collaboration tools. The twofold objective was to gather feedback about specific needs and to mobilize readily available resources (subject to approval from heads of department). Two projects were proposed from the outset: the

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

management of police custody and the management of sealed documents and exhibits (two old "ogres" that had spawned an almost incalculable number of local applications). Two years later, the record of this development community is less than encouraging. On the one hand, few volunteers have stepped forward and on the other, the two initial projects have made little progress; no further projects were mooted until the spring of 2016.

Diagnostic of the existing change governance structure

A need for simplification and greater organizational transparency

The digital landscape—and the challenges it poses for the security forces—obliges us to reconcile three fundamentals: organization, human resources and strategy.

Far from focusing solely on the development of tools, successful change will emerge mainly from the mobilization of personnel (recruitment, functions, continuing training). Additionally, the great technology rush must not be allowed to distract the authorities from their task. Due consideration must be given to the initial difficulties generated by the multiplicity of actors (national police, national *gendarmerie*, municipal police, private security firms, citizens), the heterogeneity of structures and practices, the rigidity of certain rules (the frameworks that govern recruitment, budget practices, etc.) and finally, a damaging lack of managerial leadership.

The first question concerns the organizations. When one examines the major directorates concerned (DGPN, DGGN, DGSI, DGSCGC), the HR mission is clearly under-sized and its management resembles a layer cake. That fact is that even when their missions and objectives are identical, the police and the *gendarmes* do not operate in the same way. There are, however, some initial signs of a rapprochement: the gendarmerie is now placed under the functional authority of the Minister of the Interior, and the police and *gendarmerie* pool some of their resources, and even set up joint working groups. But the information systems of the security forces do not yet form a common entity. Another problem is the coexistence of separate tools for the same use (report editing software: LRP-PN and LRP-GN) resulting, moreover, in different sets of statistics.

Finally, there are indications here and there of a total lack of any transformation culture—a major barrier to the changes that need to be made in both institutions. The ability to instill a culture of change, and to evaluate performance, is an essential component of leadership.

An evolving recruitment policy

Clearly, civil society is brimming with individual IT talent. The administration cannot but try to attract this potential into its ranks. Open innovation, for example, is a topic for the DGSI. Given the tensions that surround the recruitment of these profiles, and the speed of change in the markets, is it time to prioritize short-term contracts? This option, founded on pragmatism, involves at least one difficulty: the accreditation of staff without official status. But in any case, the ministry must avoid relying solely on engineers and consultants from service providers.

The absence of a well-managed technical branch and of well-defined recruitment profiling is keenly felt. Likewise, opening up the police officer corps to scientists would be a welcome move, as would personalized support for agents looking for a change of career path.

The recruitment of operators from outside the ranks, and from civil society–along the lines of the counter-terrorism unit set up within the NYPD [18] –would bring in fresh pairs of eyes: not always comfortable, but definitively constructive.

The attacks of January and November 2015 spurred the French authorities to declare a significant recruitment drive, which will mainly affect street-level and intelligence missions. In the latter field, the Prime Minister also plans to open up a specific recruitment path for civilians.

For the 2,731 police officers recruited, easier entrance tests and shorter training–one year instead of two–illustrate that the change is more than just symbolic. Meanwhile, the national gendarmerie, where 1,763 new positions are to be created in 2016, is also overhauling its methods by focusing instruction on operational aspects, with theory lessons being dispensed remotely (notably via e-learning). In practice, a form of simplification is being adopted.

In municipal police units, a significant professionalization effort is indispensable in every area; IT skills, in particular, are uneven.

(18) In the wake of September 11, 2001, the New York Police Department (NYPD), at the instigation of Raymond Kelly, set up a unit dedicated entirely to counter-terrorism. Directed by a former CIA head of counter-terrorism, one half of the unit consists of police officers, the other half of academics, scientists, lawyers, journalists, etc. All are strongly encouraged to work in pairs, to report information (to be analyzed and filtered by others), and to create and maintain networks of informers (35,000: subway workers, officials from housing and employment services, etc). New operating principle: from now on, those who uncover information justifying the opening of an inquiry will be associated with the inquiry.

Adaptations must take account of changes in the private sector

In parallel, areas of collaboration are being opened up with the private sector (internet giants, the security industry, etc.) so as not to isolate the public sphere from this digital reality.

While the Ministry of the Interior has only recently defined its industrial policy, there is still the hope that a French "Palantir" [19] will be created. The transition to Policing 3.0 might even justify the creation of "instant upgrade sensor" personnel, qualified to follow up any technological development without delay. To date, there is not yet been a proactive initiative by the administration at electronic trade events. A permanent horizon-scanning cell should be considered.

Finally, the organizational and methodological disparities already mentioned, and *a fortiori* the shortcomings in transversal action and coordination, reinforce the need for a shared diagnostic. A coproduced vision must be defined, henceforward avoiding the risk of having too many projects.

(19) A Californian company created in 2004, specializing in data analysis, and a regular subcontractor for the US intelligence and police services. Palantir is currently establishing a foothold in Europe.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

The need to open up recruitment

In addition to the technological tools supplied to the security forces, there is the question of the human resources required to properly utilize those tools, whether for specific, permanent, or one-off needs.

Harnessing internal resources

Faced with growing technological and operational challenges, the security forces have sized up their internal resources, and a number of initiatives have been piloted, of which two seem particularly significant.

For the last fifteen years, the Anti-Cybercrime Subdirectorate (SDLC) at the Central Office for Combating Information and Communication Technology Crime (OCLCTIC) has offered an eight-week training course designed to turn investigators in into specialist cybercrime investigators (investigateurs en cybercriminalité, ICC). Every year, some fifty ICCs are trained up and equipped with the hardware and software essential to their mission. [20] On completing the course, the new "experts" return to their department of attachment to intervene, as required, in specific cybercrime cases.

(20) A pack worth 11,000 euros, entirely financed– we are told–by the DCPJ, regardless of the future ICC's department of attachment; a budget approach that is, to say the least, surprising.

The absence of any real selection at the initial level (minimal IT or office skills, etc.) or in the territorial distribution of these new specialists suggests that the approach undertaken could certainly benefit from further improvements.

Since 2005, the national *gendarmerie*, which lays claim to a more scientific culture than the national police, even recruiting from France's top-flight engineering schools, has sent a select group of gendarmes, possessing specific knowledge sets, to Troyes Technology University for training. These "N'Tech" graduate investigators then return to each region of the gendarmerie, to provide the institution with an adequate network of scientific resources.

The gendarmerie estimates that, having selected agents with the necessary potential, it takes about three years to endow them with expertise that can be put to use in a branch where it is needed. The new specialists' potential must, of course, be maintained through appropriate training and career management.

Training up *gendarmes* who are already in service can be complex: it takes time and, moreover, the right type of profile remains hard to find, especially in the IT field, where skills rapidly become obsolete. Consequently, the service therefore has to hire already (highly) qualified personnel, who have state-of-the-art skills when recruited.

Integrating scientific profiles into the security forces

When it comes to recruitment–and indeed more generally–the police and *gendarmerie* look to generalists, rather than specialists, to meet their needs. Both forces, after all, are organized so as to able to intervene anywhere and at any time; the use of scientific or specialized profiles remains an exception.

Progressively, the number of new technology specialists–digital investigators, technical first responders, cyberinvestigators, security or economic intelligence staff, etc.–has grown significantly. Whether in specialist units, in relay groups, or integrated into mixed teams, they are where they are because they meet a need. And yet, the barriers to employability are real.

It takes time to acquire expertise. This pre-supposes a forward-looking approach to the management of human resources, dependent on the use of appropriate tools and on a proactive policy in these areas. These profiles, some of which are highly technically qualified, are also much sought after by private companies, offering better pay packages than the administration.

It seems, then, that the police and *gendarmerie* face an uphill task.

In recent years, the DGSI has embarked upon a strategic recruitment plan, not hesitating to do some active talent-scouting, including at the graduate fairs of the *Grandes Ecoles*. In this context, the authorities know how to be competitive in terms of remuneration.

Despite a number of positive experiences, the ability of the police and gendarmerie to implement the HR changes required to give them the means to meet their ends remains a moot point. There are still many structural barriers which, when combined with a failure of ambition in the forward planning of employment and skills, mean that neither the gendarmerie nor the police are well-placed to offer real career opportunities to talented young people.

Integrating resources from outside

Faced with the difficulty of finding specific skill sets in its own ranks, the *gendarmerie* has taken steps to adapt to emerging issues and to offset the lack of particular profiles. Decree n°2008-959 allows the service to recruit officers or NCOs under contract in order to meet immediate needs. The Order of 21 January 2011 lists the occupations concerned; this fairly heterogeneous panel of skills is designed to evolve, and to cover every field of activity.

In 2005 there were 15 of these "commissioned" staff, as they are known; by the beginning of 2016 that figure had risen to 98, reflecting greater use of this recruitment lever. However, 75% of these are psychologists, and the C3N has incorporated only three computer-science PhDs.

Meanwhile, the administrative framework for this type of "commissioning" remains rigid. While the maximum cumulative duration of contracts is relatively long (17 years), these recruits do not have the option of joining the *gendarmerie* definitively at the end of this period. Commissioning can also prove problematic in terms of overall human resources management: commissioned staff are

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

integrated into pay grades that correspond to a certain level of remuneration, and every position thus occupied is one less potential promotion path for gendarmes working their way up through the ranks.

Although fewer in number than the commissioned staff, the gendarmerie also uses contract staff for more "one-off" needs and specific missions. No long-term career opportunities are offered, but the emoluments proposed are said to be line with the private sector. This type of recruitment is, however, becoming more scarce.

In either case, work goes into analyzing and anticipating future needs, and each branch or region is invited to express its recruitment or training objectives.

The police force has no equivalent to the "commissioned staff" principle. Most of the requirement for scientific profiles is met through examination-based recruitment or through specialist training for servicing police officers. The Technical and Scientific Police (PTS) subdirectorate is, however, able to integrate some contract staff, even if examination-based recruitment remains the rule.

The DGSI also has the possibility of using contract-based recruitment, a trend that has gathered pace since the directorate became autonomous. But the share of contract staff is capped at 15% in order to "*safeguard the service's identity as a national police force*". By way of comparison, the corresponding proportion at the DGSE has already reached 23%. [21]

Ultimately, the use of contract staff in the security forces looks more like a very local exception than a real option available to all of the directorates.

(21) "*Les moyens consacrés au renseignement intérieur*" (Resources allocated to domestic intelligence) information report by the French Senate Finance Committee, October 2015.

And yet the new operational situation is driving police forces to adapt their HR strategies, particularly with regard to scientific posts. The institutions need to further improve their attractiveness and learn to anticipate their needs. To do so, the management rules must evolve toward greater flexibility and fluidity. There are early but promising signs of movement in the right direction; these must be encouraged and facilitated.

Ad-hoc collaboration with experts

While we have been looking at the administrative and contractual options for bringing in cutting-edge skills into internal security on a lasting basis, it is clear that other routes could also usefully be explored to give investigators access to the expertise of some our academics, journalists or other qualified personalities. Their role as observers or experts could both enrich and contextualize the knowledge base of the investigators and analysts who work for the police, *gendarmerie* or intelligence services. Their detailed (historical, sociological, international, etc.) knowledge of certain forms of crime (narcotics, mafia, terrorism, etc.) or simply of certain circles (religious radicalism, the *banlieue*, protest movements, etc.) should not be a "separate field of knowledge"; it should be a source of support during investigations, just as much as in initial or ongoing training.

This mixing of expertise has yet to be properly implemented. Once can only call, as did Interior Minister Bernard Cazeneuve in his speech to the DGGN on April 20, 2016, for "the years ahead to be years in which the Ministry of the Interior opens up to its environment, and in particular to that of its universities and research centers".

A digital strategy, yes—but why?

What it means for the security forces to have a digital ambition

The digital revolution currently spreading through every organization, public or private, is traditionally presented as a dual opportunity. On the one hand, we are told, it makes it possible to offer customers or users a new, integrated, higher value added "experience". On the other, it will help organizations to optimize their ways of working: an aspiration of particular relevance to the public sector, which, around the world, is subject to the implacable maxim "doing more with less".

For police officers and gendarmes, the promise of the digital revolution is one of more enriching, more pertinent work, closer to users, and ultimately more effective.

The digital transformation experts, however, underline just how complex this process "which could easily take ten years" can be if the transformation is to be complete. It is impossible to know what technologies we will have in ten years' time. But knowing where we want to be by then, knowing what we want to do, and what we want to be recognized for... these things are essential for inspiring and leading the men and women of the security forces towards a common goal and a collective ambition. It is this strategic vision that defines the framework; within this framework, we can argue about the tools, resources and technologies that need to be implemented to achieve this goal.

A proposed digital vision for the security forces

Defining a digital ambition for the next ten years is a difficult and perilous exercise, especially as a Minister of the Interior—the emblematic figure whose role it is to embody this strategy, alongside the DGGN, the DGPN and the DGSI—only stays in office for an average of two years. [22] With their significantly longer terms of office (usually three to five years), the directors-general find it easier to follow their work through for the duration.

One can only hope that the dark days that France went through in 2015 will enable the standard-bearers of this digital strategy for the security forces to give it impetus and take it to a point of no return. We can then be ambitious and put forward the following vision:

To become—through the use of digital technologies—one of the world's three leading security forces in terms of efficiency and the quality of service provided to all

(22) Under France's current constitutional setup (the 5th Republic founded in 1958), one has to go back to Raymond Marcellin to find a long-serving minister (May 30, 1968, to February 27, 1974).

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

The scale of progress (moving from "good" to "excellent") is ambitious, the goal is noble, and the aspiration carries within it a win-win relationship for all of the parties.

Turning it into an operational digital strategy

The security forces' digital strategy could center on four pillars:

- Physical contact points (police stations, brigades, but also patrols and mobile stands, etc.): the objective here being to offer citizens a new experience;
- Services provided: what package of digital services should we offer and develop?
- Data: the use of data in greater depth, and more systematic sharing, will ensure better informed decisions;
- Internal processes: digitizing these processes will help reduce costs (real or hidden), free up administrative time in favor of value-added time, and enable greater efficiency in task handling (the digitization of police custody,[23] for example, promises significant productivity gains).

(23) Police custody is currently still a paper-based procedure, using multiple registers.

However, the costs and complexity of a transformation are such that one cannot activate all of these levers at the same time. The starting point for digital transformation must be adapted to the maturity of the organization, and to its strategic objectives.

The figure below illustrates what an initial series of actions might look like (some have already been initiated).

Exhibit 5 : The digital transformation of the security forces requires priority levers and opportunities to be defined

Digital transformation goes through three stages:

1. Define a digital strategy
2. Activate levers on one link in the value chain (prevention, surveillance, etc.) or on a specific issue
3. Put the fundamentals in place

	1 Digital strategy *(vision and plan)*			
	2 Contact points	Services	Data	Processes
Prevention	Scoring-based advice to users	Integration of connected objects into alert systems	Predictive analysis	Organization of patrols
Surveillance	-	Cyber patrols	Big Data (analysis of crime phenomena, etc.)	▪ ALPR ▪ Smart cameras
Recording of crimes	▪ Appointment system ▪ Pre-completion of forms on tablet at station	▪ Online complaints ▪ Online dialogue with police officers/agents	▪ Statistical monitoring ▪ Local alerts about similar crimes	Predictive resource allocation
Investigation	-	Appeals for witnesses	Big Data (search for clues, lines of inquiry)	Information sharing
Intervention	Warnings and alerts	-	Enrichment of target files	Mobile access
Case-building	-	Appeals for witnesses	Big data (search for evidence, etc.)	Digital exchange with the justice systems
	3 **Enablers** *(organizational structure, digital talents, IT enablers and culture change)*			

Source : McKinsey: authors' analysis

Good practices for rolling out a digital strategy

To organize and successfully execute an in-depth digital transformation along the lines that we propose requires four actions to be carried out:

- Explain the reasons for the change and convince people, so that individuals understand what is expected of them, find it meaningful, and buy in to the idea (by developing and sharing a "change story" that covers every topic and every level of the organization);
- Develop skills and know-how, so that individuals adopt the desired behaviors (training, career management);
- Set the example, so that individuals understand the importance and inevitability of change from the behaviors they see in line managers, in peers or in the organization's opinion leaders and influencers;
- Reinforce the whole project with formal mechanisms, so that individuals are motivated for change by structures, processes, information systems and practices of reward and recognition.

Once the digital strategy has been defined (what, why, and with what targets), careful thought must be given–still well upstream–as to which quantified performance indicators should be monitored over time in order to measure and encourage progress, or even to trigger the transition to the next phase. That may sound elementary, but it is a key condition for the success of a digital transformation. As one expert told us: "One of the main reasons for failure in the digital systems whose implementation we monitored was the absence of quantified indicators. What works best is to define a 3- to 5-year strategy, and manage it with 3- to 6-month indicators."

A good performance indicator should measure three things: user satisfaction, the process itself (e.g. degree of generalization to other units, etc.) and the resulting gain (financial, time, etc.). To ensure that the change approach is both ambitious and proactive, the task of defining quantified targets must lie with the change leaders ("top-down" mode); targets cannot be copied across from field observations.

By way of illustration, three indicators could be defined for the digitization of police custody:

- User (police officer and *gendarme*) satisfaction, aiming for an average rating of at least 4/5;
- 50% of custody detentions digitized within 12 months;
- 0% of staff time freed up.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

RECOMMENDATIONS FOR POLICING 3.0

Transform structures by building on a long-term vision

Prepare a new "programming law" on justice and internal security

In a fast-changing world, where the constant threat of terrorism results in immediate and significant decisions being taken, the need for a mid- to long-term framework and vision seems more necessary than ever. This might, for example, enable services to have a multi-year budget visibility and to plan their actions and investments more calmly and therefore more efficiently.

Such a framework could be provided by a new LOPPSI (law of orientation and programming for internal security performance). The proposed new law, the third piece of legislation of its kind, may have its acronym enriched with a new letter,[24] "LOPPSIJ", adding a J for justice, to better integrate investigative approaches and the criminal justice system. Careful to respect the separation of powers, this law would in practice involve two distinct but concomitant statutes, and would analyze in detail the implications for the Interior and Justice Ministries over the next ten years.

(24) LOPPSI 2 (2011) already incoporated an extra letter: a second P, for performance.

It would particularly look at the ambitions, the resources required to attain them, and questions such as video surveillance, Big Data, internet, the role and use of reservists (operational and civilian reserves), R&D investment (demonstrators, initiatives to follow up, etc.), and the renewal of old or obsolescent equipment, etc.

This is, of course, a method exercise, to be initiated and overseen at the highest level of government, going beyond the useful but sporadic initiatives and contributions that emerge from the proposals of the Ministerial Delegation to the Security Industries or of certain inspectors-general of armaments, the ideas put forward by CHEMI and INHESJ, or input from think tanks.

Provide meaningful support for change

Managing change requires not only clearly-stated political will, but also very broad acceptance (in the sense of understanding and adherence) of transformation in the security forces. The degree of maturity of each structure is therefore an important factor. The top of the management chain must take ownership of these elements, and the impetus must come from the Prime Minister and the Minister of the Interior.

Change governance can then be designed without having to create new structures, notably by implementing the six following actions.

- Define a multi-year vision and a coherent overall strategy, by means of a new programming law (see above);
- Bring the DGAFP into the management dialogue with the budget department (some timid steps were made towards this in 2016–it is up to the Prime Minister's office to make this initiative a permanent feature);
- Set up leadership in the field of Big Data, coordinated by a ministerial data manager and a team of facilitators (see below);
- Institute new working methods (recruitment by profile, systematic feedback, career-long training, eliciting ideas from front-line teams via performance workshops);
- Create a select panel of independent experts to analyze results and initiate useful orientations. This body–situated outside of any ministerial hierarchy–would be designed to act as the "sand in the oyster" for the system. It would consist of reference persons from the world of research, from the private sector, and of former senior ranking officers from the police and *gendarmerie*. At regular intervals (every six or even three months) the panel would examine the crime figures or the results of action programs, with the aim not of "validating" the figures, but of delivering an independent view from outside the system, based mainly on experience feedback, surveys, and computer data analyses that the panel would be empowered to commission. Its objectivity would enable options to be explored that the services might not naturally tend to consider;
- Generalize the practice of front-line operatives flagging up concrete improvement ideas. The "Performance Workshops" put in place to good effect by the *gendarmerie* could, for example, usefully be applied to all of the departments in the Ministry of the Interior. Front-line teams (of all grades and functions) formulate good practices in the form of suggestion sheets, which are submitted to a panel of designers, and then to a monitoring committee (after taking opinions from the relevant departments). The committee validates the most relevant actions for rollout throughout the country and adoption by all of the services, which are free to adopt the measures most suited to their own needs. An initial synthetic assessment of the action conducted by the national *gendarmerie* could serve as a stepping-stone for its development in the national police.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Take decompartmentalization further

Contemporary threats have precipitated the security forces–and the intelligence services in particular–into a world characterized by "short time" and by the need for exchange: the diametrical opposite of what has, for so long, been their institutional culture; namely, "long time" and secrecy. Collaboration and information sharing have become absolute priorities.

A number of initiatives have demonstrated that collaboration between departments or between multidisciplinary teams (regional intervention groups, specialized inter-regional jurisdictions, the DGSI and the Central Territorial Intelligence Service (SCRT), combining forces to combat radicalization, etc.) can achieve better results.

Any action or reorganization that will help to construct a less compartmentalized police force must therefore be encouraged:

- The pooling and convergence of equipment and IT tools (between police and *gendarmerie*, but also between departments in each service);
- The pooling of training;
- Jointly-led exercises or foresight initiatives;
- Cross-mobility between services or institutions, and shared management of support teams: exchanges of top managers, as has been successfully done between the DGSI and the DGSE;
- The appointment of contract staff in each service;
- Regular exchange meetings (activity tracking, exchanges of best practices, etc.);
- A system of performance monitoring and management dialogue which, from top level through to local level, analyzes and encourages collaboration and information sharing;
- The integration of the "collaboration" dimension into appraisal, promotion and remuneration policies;
- Organizational mergers (e.g. should the DGSI and the SCRT be joined? If so, what about the gendarmerie's Operational Foresight Subdirectorate (SDAO)? Should the police and *gendarmerie* cybercrime departments be grouped together? etc.);
- And so on.

Above all, decompartmentalize access to information

Strict application of the principle of file specialization has led to a plethora of government files (police, judicial, social, financial, tax, etc.). This proliferation of files, and their division into silos, make them difficult–if not impossible–to access. As for crossing-referencing the information they contain with the information held in private files (by telecom operators, access providers, etc.), that is almost out of the question.

Simplifying consultation, traceability and *a posteriori* checking procedures would optimize their use, while guaranteeing better protection for people's fundamental rights and privacy.

This could be done by implementing the three following procedures:

- A procedure for non-recurrent access to, and simplified consultation of, the various government files by all operational forces, on condition of traceability. This procedure could be realized by putting in place a unique identifier specific to each investigator, and security mechanisms (passwords, certificates, professional ID, etc.) for secure prior identification;
- A unified information request form for data held in the various government files. Using such a form could avoid having to enter details many times in succession on forms designed for each type of file—an extremely time-consuming task for investigators. This could be achieved by using harmonized data collection fields that apply to all files, and by uniformizing the services' information systems. Such a form would facilitate checking of the information obtained, the databases consulted, and the intended use of the data. As a consequence, people's right of access and rectification would also be improved;
- A strict control procedure, performed *a posteriori* by a legal authority (a magistrate such as "a liberty and custody judge" (*juge des libertés et de la détention*) to guarantee the respect of individuals' rights and the conditions under which data is consulted and extracted, without slowing down the investigation process

The legislative requirements would be met, on the one hand, by the absence of any global file, or of interconnections between files, or free and constant access by investigators and, on the other, by perfect traceability of access, consultation and extraction operations, and their a posteriori control by a separate independent authority. Such an approach would be in line with the fundamental rights and values defended by France's personal data protection agency, the *Commission nationale de l'informatique et des libertés* (CNIL).

The requirements for any future data management system should stipulate that it must be interoperable with the pre-existing information systems, in order to facilitate overall consistency and the continued viability of the procedures mentioned above.

Consider setting up a dedicated digital information analysis service

Creating a single service to centralize and handle data from different sources (police, gendarmerie, justice system, public or private), run by experts on the meaning and use of such data, may sound like an attractive idea. However, it raises a number of organizational and legal questions with implications that extend beyond the scope of our work.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Given the key role that data, in tomorrow's world, will play in the fight against crime in all its forms, the Ministry would be well advised to begin exploring the options in this direction.

A service of this kind would be better able to capitalize on good data mining practices (consistency of stored data, centralization of backup responsibilities, salient processes, rapid sharing of feedback between operators, etc.), control access to data, and ensure its traceability.

Implement proper information system project management

From our interviews, it emerges that the root causes for the failure of many technological or IT projects lie in their duration–simply too long–and their excessive (sometimes even grandiose) ambitions in terms of functionalities.

To take account of the increasing pace of change in technology and in functional requirements, future projects should endeavor to comply with the following rules:

- Limit their duration to a maximum of three years (as a guarantee against the risk of obsolescence);
- Put in place a strong project oversight entity, common to the police and gendarmerie, to handle the master plan;
- Aim for a goal of standardization between the police and *gendarmerie*, but without making it a question of principle;
- Add, to this goal of standardization, a goal of interoperability, for greater overall efficiency.

.

Develop talent already present in the institutions

Introduce proper forward planning of employment and skills

To pave the way for policing as it will be in five to ten years' time, the police and *gendarmerie* must look at their needs per position, per mission and per territory over that time scale, looking not only at future jobs, but also at new career paths.

This approach–the methodical forward planning of employment, staffing and skills–will need to be coordinated, if not unified, between the police and the *gendarmerie*. Above all, it will need to be ring-fenced to protect it from the vicissitudes of events or short-term political decisions.

The General Directorate of Administration and Civil Service (DGAFP) can play a critical role here, both to ensure the homogeneity of the human resources policy within the administration, and to make sure that the skills and career paths put in place conform to the choices made and periodically updated.

Create and promote dedicated digital investigation branches

High-quality training courses already exist that enable the police and *gendarmerie* to have hundreds of investigators specializing in digital analysis and cybercrime. But little seems to be done to maintain, organize and promote these skills, which will be essential in tomorrow's hyperconnected digital world.

An initial approach, as part of a long-term vision, might be to pool the training efforts of the police and *gendarmerie*. Better still: since we know that digital jobs will be hard to fill in the coming years, for lack of trained individuals, [25] the police and *gendarmerie* could set up a joint structure dedicated to continuous training in digital skills. A real center of excellence of this type could dispense specific training modules in cybercrime and digital investigation. Taught by outside experts (ANSSI, university faculty, private players, etc.) and in-house instructors (investigators, etc.), these courses would be at the cutting edge while remaining in phase with current operational needs. They would be accessible both *via* continuing training (accepting enrollment applications from individuals with a basic grounding in office applications or digital) and through external entrance examinations (consisting of specific and relevant tests), without affecting the possibility of recruiting contract staff when the needs (skills or urgency) so require.

Until that time, the programs developed by one institution must be open to, and recognized by, the others. It is regrettable, for example, that the ICC accreditation can be attributed to gendarmes, but that there is no reciprocity when it comes to N'Tech certification.

Once trained, the ICCs and the N'Tech *gendarmes* must be shown that their skills are needed, [26] and therefore actively maintained and applied; this may mean that these profiles will have to be managed nationally and centrally (see also our recommendations on predictive analysis and the management of the related analytics skills). The expectations of these agents in terms of employment conditions, career plan, remuneration–and, perhaps, qualifications in recognition of acquired experience–could then legitimately be fulfilled.

(25) See the joint report by IGAS, the two National Education General Inspectorates and the High Council for the Economy, Industry, Energy and Technology: "*Les besoins et l'offre de formation aux métiers du numérique*" (Training needs and provision in digital specializations), February 2016.

(26) A recent survey by the anti-cybercrime sub-directorate (SDLC) showed that 10% of ICCs had not been given a cybercrime case to deal with during the previous twelve months. Others had been given only one.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Find the right match between needs, allocations and uses

The decision to send police officers for ICC training is determined by the central employment directorates on the basis of their annual quotas; it is easy to see, therefore, how the organization might seem to be lacking in planning or overall vision. Analysis of needs per department or per geography before assigning training courses could inject more efficiency into the system.

Likewise, prior validation of the profiles to be trained, both in terms of motivation and in terms of basic skills, would seem to be a necessity. The completion of a number of self-training modules would be an excellent prerequisite in this case. For an ultimate guarantee, candidates could then be selected *via* an interview process.

Finally, the allocation of standardized ICC equipment at the end of the course should also be adapted to future needs and uses. In our view, priority should be given to effective technology and a recent computer rather than a full set of equipment that runs the risk of being made obsolescent before it has even "paid for itself".

Attract new talent

Adapt and open up entrance examinations

In today's world, it is hard to justify the primacy of legal training in the upper echelons of the police and *gendarmerie*, where many other competences are required than knowledge of the law. It seems clear that the *gendarmerie*'s greater openness to scientific profiles gives it greater agility in dealing with the digital challenge.

The examination system must therefore be rethought, particularly the police entrance examinations, to enable non-legal specialists to compete for places on an even footing.

In other words, the security forces must endeavor to include scientific and digital profiles among their new recruits, including at commissioner or officer rank. For that, the police and *gendarmerie* will need to reinforce their attractiveness as employers relative to the private sector and develop sufficient strengths (pay, career prospects, training, mobility, etc.) to identify, attract and integrate the best elements.

Finally, timing recruitment processes (*i.e.* the examination calendar) to coincide with the end of the school year or the arrival on the labor market of young graduates would avoid the police and *gendarmerie* being treated as fallback career options (although this seems to have changed following the 2015 attacks). Suitable communication campaigns rolled out at carefully targeted establishments, or the development of apprenticeship contracts, could also be effective levers for selecting the right candidates.

Broaden the field of commissioned officers

While the principle of recruiting commissioned officers is useful for the access to cutting-edge skills and the diversification of profiles that it provides, the volumes involved are still too small to have a significant impact.

The scheme could gain from additional flexibility, both in terms of the career prospects on offer (promotion, definitive integration into the service, etc.) and in terms of the range of eligible skills and profiles. The list of specializations covered could, for example, include the forward planning of skills.

This being the case, and given the positive contributions made by this scheme, consideration should be given to extending it to the national police and the DGSI.

Favor interactions with the outside world

In Sections 1.2.5 and 1.2.6 we sketched out what an effective partnership between the police, the *gendarmerie* and the private sector might look like (R&D collaborations, investigations, access to specialist expertise, assistance for exports, etc.).

Because it is also a way of involving citizens and cultivating the security forces' image of professionalism and proximity, eliciting outside contributions or competences from the academic or private sphere is a practice that should be encouraged. These exchanges could be built upon to maintain the level of knowledge and excellence of our forces over time. To stimulate such exchanges, a "library" of expert partner profiles could be compiled and made widely accessible, contributing to the sharing of contacts between services and to the expansion in the scope of intervention of this external community.

The "software programming marathon" initiative organized in April 2016 by the national *gendarmerie* is a move in that direction. Under ST(SI)² supervision, 26 engineering school students were thereby able to help improve the functioning of the application "GendLoc".

Finally, this "complicity" could, of course, be extended to private security firms. In the county of Stockholm, for example, there has been strong collaboration since 2009 between Securitas patrols and local or national police: transmitting targeted information to the authorities, signaling badly parked vehicles for ticketing, preventing groups of people gathering to disturb the peace, and so on. The radio equipment of the private agents is even compatible with that of the fire brigade, to facilitate assistance in critical situations, while their dashboard cameras are connected to the municipal surveillance network to capture any details that might be useful to the security forces.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Implement the digital strategy

In Section *A digital strategy, yes–but why? (p.32)* we discussed what a "digital ambition" might look like for the French security forces, as well as good practices to follow in rolling it out. To write and orchestrate this digital strategy, we believe that it must be embodied at the highest level, and must focus primarily on freeing up personnel from time-consuming non-value-added tasks by leveraging the productivity gains made possible by new technologies..

Create a post of Digital Director within the Ministry of the Interior

To signal the importance of what is at stake here, and to ensure the success of the digital transformation as outlined in these pages ("To become–through the use of digital technologies–one of the world's three leading security forces in terms of efficiency and the quality of service provided to all"), the Ministry of the Interior could appoint a Digital Director.

Reporting directly to the Minister, the Digital Director would oversee the Ministry's entire digital transformation agenda (definition and implementation of strategy, training, etc.) and would take a cross-departmental approach, working with all of the general directorates to ensure the seamless digitization of the organization as a whole.

As a specialist in digital, primarily, and with the support of expert advisors [27], the Digital Director would oversee the digitization of several processes (e.g. police custody, police officer authentication by electronic signature, archiving and access to archives, etc.), while making sure the entire administrative chain (Justice, Treasury, etc.) is integrated into the police processes.

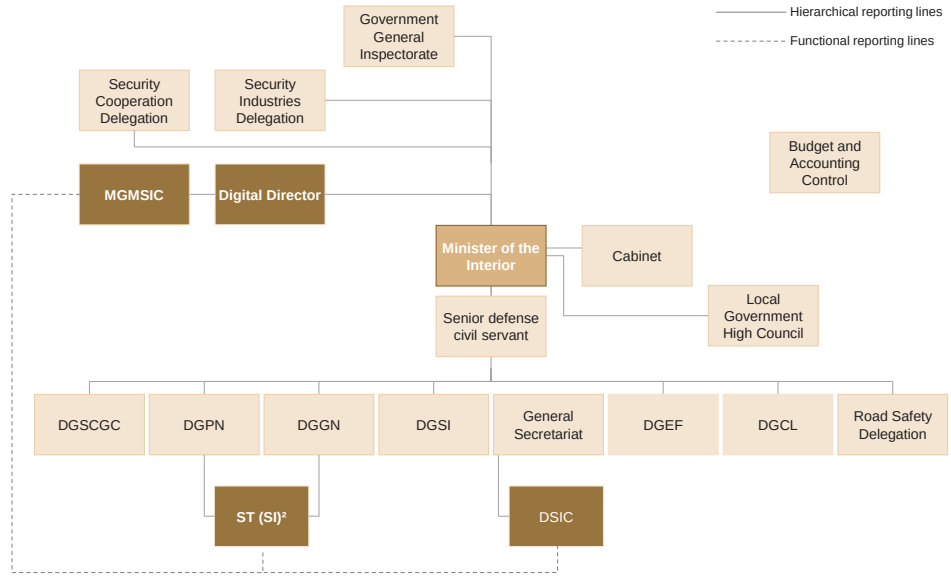
The Digital Director would be responsible for developing online contact points and internet services (e.g. online dialogue, appointments, pre-completion of forms using tablets made available to the public on arrival at the police station or *gendarmerie*, cyber patrol policy, internet communication policy, etc.).

The Digital Director would also exercise leadership in the field of Big Data, to accelerate the dissemination of Big Data techniques throughout the Ministry (in reactive mode to help solve cases, and in proactive mode to guide and target surveillance) and encourage initiatives in advanced analytics (predictive analysis, web surveillance and social networks, etc.). He or she would also work to facilitate the consistency and coverage of files, and to define the open data policy, in keeping with the approach developed by the senior data administrator.

To facilitate coordination between the different departments in charge of the information systems (ST(SI)² and the DSIC in particular) and to ensure independent trade-off decisions on these topics, we recommend that the MGMSIC (Ministerial Information and Communication Systems Governance Mission)–

(27) As reported by *Les Echos* (March 04, 2016), the CEO of Alphabet (Google), Eric Schmidt, will, for example, head a consultative committee on technological innovation at the Pentagon (complex data analysis, organization of information sharing, etc).

Exhibit 6: The position of the Digital Director within the Ministry of the Interior



Source : authors' analysis

currently attached, like the DSIC, to the General Secretariat of the Ministry of the Interior–should in future be placed under the authority of the Digital Director. This organizational configuration should provide overall coherence, continuity, and greater efficiency in the development and management of information systems.

More generally, the Digital Director would work to develop digital and analytical skills (data scientists, etc.) within the directorates, while at the same time developing a digital culture in the top management of the Ministry and its general directorates. He or she would play a pivotal role in decompartmentalizing access to information.

Given the scope of the Digital Director's role, he or she would participate in the Ministry's key investment decisions, contributing directly to discussions about priorities, mid- to long-term goals, or short-term trade-offs.

What we are calling for, ultimately, is the creation of a highly strategic position: that of a "Director of Digital, Strategy and Programs".

Dematerialize core processes, including with the Justice department

In an environment still heavily dominated by paperwork (registers, monitoring logs, circulars, departmental memos, telexes, etc.), the digitization of police processes could achieve very substantial gains in productivity and efficiency. As we pointed out earlier, the work hours saved could represent the equivalent of over 20,000 police and *gendarme* posts.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

One evident priority is to replace all of the existing registers (custody, detention, weapons, non-lethal weapons, weapons for security auxiliaries, etc.) with software applications using an intranet model. This digitization process could be based on suitable management of user profiles and systematic use of the currently under-utilized professional ID card as a means of authentication and electronic signature. This is the route that the national *gendarmerie* decided to take some years ago. The DGPN, in turn, is now embarking on the complete dematerialization of its custody management processes. It only remains to persuade the judicial authority to do away with the corresponding printed version of the register and to digitize the transmission of information to prosecutors or examining magistrates.

Likewise, lines of command should be able to benefit from the new functionalities offered by the "Mobility" project currently being rolled out. It is surely time to rethink the rigid format of the telexes transmitted via RESCOM, which do little to enhance efficiency. In this area, the national gendarmerie has opted for a much less cumbersome tactical messaging system, similar to mail clients like Outlook, to transmit commands.

Dematerialize digital evidence, and the way it is managed

Even as digital is generating and multiplying new types of evidence gathered from smartphones, from video surveillance, or from connected objects or vehicles, the procedural rules continue to require that digital evidence be materialized on a physical medium in order to be counted as evidence.

This process could be optimized by adopting a common standard for the collection and analysis of digital evidence, to apply to all investigators. This would facilitate sharing and archiving.

The police and justice departments could benefit from looking into technical solutions for handling digital evidence in its native environment, even if it means revising the criminal procedure.

Given the sheer abundance of such material, one could begin by implementing a solution dedicated to processing video files (collection, identification, management, sharing, advanced analysis, etc.). Designed, from the outset, as an open platform, this solution could then be extended to other forms of digital evidence. This would mitigate the risks associated with taking a more global approach from day one.

Here again, the professional ID card could support this digitization process by enabling judicial police officers to sign evidence digitally, much as when affixing seals to physical evidence.

Ultimately, an evidence management system of this type would be a source of time-savings for investigators, allowing them to focus better on their core role and on higher value-added tasks.

Unify identification and authentication systems

Access to the information systems of the police and *gendarmerie* is not managed in a joined-up manner. It is not currently possible to log in to all of the applications with a single identification and authentication step.

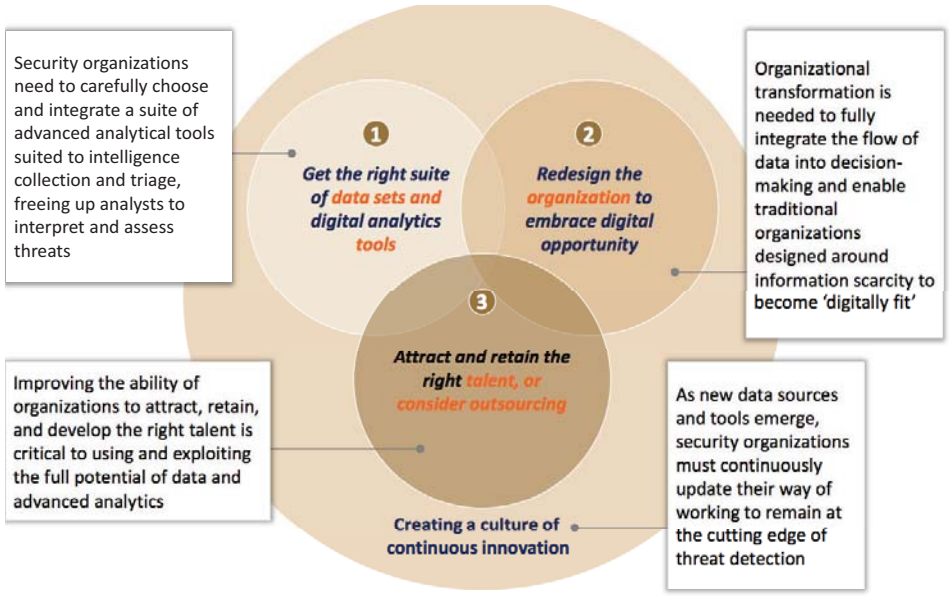
To encourage convergence, an effort is required to unify the identification and authentication systems of the two institutions.

Such a project would also be an ideal opportunity to simplify the management of user privileges by introducing standard roles and profiles common to both entities.

Beef up digital investigation methods

For security forces the world over, implementing digital investigation methods presents the same three challenges: namely, technical, organizational, and talent management challenges.

Exhibit 7: Intelligence and security organizations currently face three distinct challenges to harnessing the power of data for good



Source: McKinsey (Police service line, 2016)

To deliver an effective response to these imperatives, our security forces need to have a horizon-scanning mechanism to look out for new developments in digital investigation; they must be equipped and structured to monitor the internet and social networks; and they must view cyberspace as a new territory that needs to be defended.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Keep a watch on the digital investigation market

There is no shortage of software and technological solutions for monitoring the internet and social networks. The supply of such solutions is global, is constantly changing, and is often driven by innovative startups (American, Israeli, etc.) whose products are complementary but never interchangeable.

Even if it is not their core activity, police officers and gendarmes must keep close tabs on developments in these markets, identifying potential high-impact innovations and looking at ways to integrate them. This should not be left to the manufacturers or software houses themselves; to do so would be to relinquish a degree of independence. Outsourcing this task to a technology intelligence agency would represent a cost, and would raise the issue of the agency's security credentials.

The police and *gendarmerie* could pool forces to perform this active monitoring task without the need for major investment. A group of three to six people, made up of IT enthusiasts and experienced investigators, would form a community to collect, assess and disseminate information, drawing on visits to international trade fairs, press and interest searches, exchanges with other security forces around the world, and so on. Their findings would be shared with designated reference persons in each central directorate and at different geographical scales. This community of experts would, of course, be brought in on each new project or each call for tenders relating to digital investigation.

Equip and structure to monitor the internet £and social networks

To detect low-level threat signals, the security forces need to acquire cutting-edge tools for the surveillance of the internet (to probe the "Dark Web") and social networks (to analyze links between people, the redistribution of content, etc.). There are numerous operational uses: monitoring terrorist propaganda and exchanges between individuals suspected of radicalization, fighting arms trafficking or child pornography, tracking protest movements and anticipating their actions, and so on. The market offers many tools, which need not be listed here.

Missions and requirements may differ, but some level of pooling should be sought when deploying these resources: shared access to tools; transparency about lines of enquiry in order to avoid duplication; cross-fertilization through the exchange of information and analyses; and, of course, economies of scale.

The services that should a priori be equipped with these capacities are the SCRC, C3N, OCLCTIC, SDAO, SCRT and DGSI (for abbreviations, see §4.1)–as well as, of course, the DGSE. Further downstream, it might be worth considering setting up a single entity with responsibility for cyberspace surveillance, working for all of the security forces.

Until that time, the work should be performed by web-wise analysts, specifically trained in the new tools and working in pairs with investigators (such as the ICCs from the OCLCTIC) in order to ensure that their analyses are relevant and actionable at the operational level.

Finally, it is essential that this internet and social network surveillance work be carried out in a spirit of information sharing. Analyses must therefore be communicated regularly and proactively to the central directorates and to all services, central or regional, in charge of intelligence, counter-terrorism, border controls, or the maintenance of law and order.

View cyberspace as a new beat to patrol

With digital space becoming an area of sovereignty in its own right, the police and gendarmerie must see it–as do the armed forces–as a new space to be occupied, to avoid it becoming a breeding-ground for lawlessness.

In addition to this type of "plain clothes" surveillance, the security forces must, in the coming decade, build a credible presence for themselves on the internet and on the social networks. The outlines of this presence remain to be defined: "treading the beat" on discussion forums or at internet service providers; the ability for users to click on a "police emergency" button when browsing the web; the dissemination of targeted prevention messages, or a visible police presence, on certain websites, etc.

This cyber-police force has a particular role to play in countering propaganda or monitoring the spread of rumors (jihadism, protests in "protection zones", etc.). Experience shows that they can have a real impact. During the August 2011 riots in Birmingham, the British police–by acting both overtly and covertly on the internet–were able to calm some of the tensions developing around demonstrations.

Accelerate and sustain predictive approaches

Extend experiments, especially in high-crime areas, with a view to wider roll-out

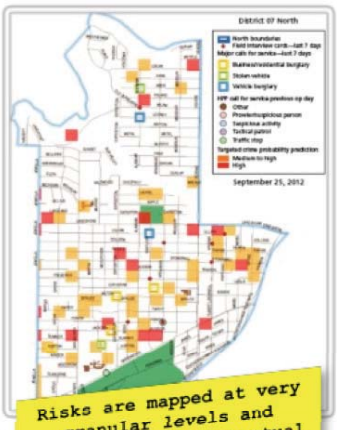
Experiments in predictive policing have multiplied in recent years, mainly in the US. After New York, with its almost elementary statistical approach, Los Angeles, Atlanta and some medium-sized cities claim to have cut crime significantly by routing patrols on the basis of "predictions" established using sometimes extremely simple algorithms. Several European cities (in Germany, Italy and the UK, among others) are now surfing the "predictivist" wave.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Exhibit 8: Several illustrations support the idea that prediction-led policing works

PredPol services

- Californian start-up PredPol[1] uses only 3 data series (type, place and time of crime) to map crime predictions in 500' x 500' areas
- They claim a decrease in crime of 8% to 32% in the cities they serve
- Subscription fees: USD 30k per year for continuously updated predictions



Risks are mapped at very granular levels and presented with contextual details

Evaluation in Milan

- An academic assessment of Milan's predictive policing experience (2007, robberies) concluded that:
  - *"Predictive policing improves police patrolling by a large degree"*
  - *"Benefits appear to outweigh the cost by a factor of 5"*

Source : PredPol website, press search (Le Monde 04/24/2015) University of Essex, *"Information Technology and Police* Productivity", G. Mastrobuoni, 2015 ; Rand Corporation, *"Predictive policing"*, 2013

1 Created in 2012; turnover:USD 0.62m; staff: 25 FTEs. Clients are cities incl. Atlanta, LA, London, Montevideo, Munich...

There is a cultural preference in France for preserving the spirit of initiative of front-line police officers and for "man-made" decision-making, avoiding shortsighted actions that might merely displace crime geographically. But in a context of limited, even over-stretched, resources the security forces have no choice but to increase operational efficacy by using the tools, data and resources available to them.

It is surely important, then, for the experiments currently conducted by the national *gendarmerie*'s Central Criminal Intelligence Service (SCRC) to be extended rapidly to other geographical areas.[28] This presents the Ministry of the Interior with a valuable opportunity for pooling, by transferring the statistical developments and the know-how of the gendarmes to the geographic and operational territory of the police.

(28) The SCRC is currently trialing a predictive analysis program in *Aquitaine* (general crime in *gendarmerie* territory) and in the Oise (auto theft in police and *gendarmerie* areas).

One might also envisage setting up predictive analysis trials straight away in the most sensitive of France's 80 high-crime *zones de securité prioritaires* (ZSP), establishing and analyzing predictions–without fear or favor–on a half-daily basis, in order to organize patrols.

Develop a long-term strategy to manage analytical talent

The implementation and operational use of predictive analysis calls for new competences: statistical analysis, data processing, and the ability to understand the roles and needs of patrols or investigators and translate them into a mathematical research methodology.

A targeted recruitment drive will be needed to bring in these new competences, but it will also be necessary to define ways of retaining these "data scientists", who are already much sought after in the private sector: salary, job content, career path, and so on. Collaboration with universities or research centers (such as the National Observatory of Crime and Criminal Justice Responses, ONDRP) could foster fruitful emulation, as could the creation of two-person data scientist and investigator teams.

Support the spread of predictive analysis throughout the organization

Our interviews detected a degree of resistance that might hamper the rollout of predictive analysis. Like the installation of geolocation systems in vehicles, it could be perceived as a loss of autonomy by front-line operatives for whom it is experience and judgment that will always make the difference.

To reduce this risk, and instead favor rapid and whole-hearted adoption, requires tailored communication and a specific implementation method: persuasion by example, the appointment of reference persons in brigades and police stations, transparency on results, a visual performance management system around patrols and predictions (e.g. crime mapping, etc.), daily briefings, experience feedback and sharing within patrols, and the involvement of data scientists at ground level.

Modernize the command centers (CIC and CORG)

Modernizing the command centers (CIC for the police and CORG for the gendarmerie) is a major undertaking and is one of the five "challenges" in the Interior Ministry's security modernization plan. A significant contribution was made by the *gendarmerie* in 2011-2012 with the introduction of the Public Security Database (BDSP).[29] The DGPN, meanwhile, saw sufficient potential in this objective to appoint, in February 2016, a *commissaire divisionnaire* tasked exclusively with supervising this project and acting as its prime contractor.

Without going into the details of this vast project–to be completed in 2019–some of its key orientations should be borne in mind, to serve as guidelines for the planned renovation.

(29) Developed by Thales, the BDSP enables gendarmes–from command-center level through to patrol level–to access a summary of all available information relating to a mission or intervention.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Integrate digital functionalities into emergency calls

The emergency number *17 "police-secours"*—which came in with the wholesale adoption of the fixed-line telephone in French households in the early 1970s—developed around the principle of the telephone call. For forty years, there have been no significant changes in this system, but it can now benefit from the potentialities offered by digital.

For example, as emergency calls are now made mainly from mobile telephones, the smartphone used could be automatically geolocated, enabling call handlers—tasked with sending in teams—to immediately establish the exact position of the caller, who—often under stress—may have difficulty explaining precisely where he or she is.

Likewise, "17" call platforms should be able to receive documents (photographs, videos, SMSs, MMSs, etc.) from callers to provide pointers for first responders and, where applicable, to be used immediately by the investigation services. This option is already in place for the emergency number of the French rail operator, SNCF (31 17 by telephone or 31 177 by SMS).

Finally, callers could be sent an SMS automatically once an emergency vehicle has been allocated to respond to the request.

Decompartmentalize the command centers

The various command centers in the Ministry of the Interior (and beyond) need to be decompartmentalized both horizontally and vertically.

The first goal is to improve the interoperability of the centers, both between the different emergency services (police, *gendarmes*, fire brigade, ambulance) and between centers in the same directorate, particularly within the national police. In the latter case, one generally finds an "organ pipe" model, which, while it enables services to work normally in the usual configurations, poses serious difficulties in crisis situations. As soon as the privileges have been assigned, neighboring CICs liable to be affected by the repercussions of a local situation must be given complete visibility on the incident in question. Likewise, the map available to any one CIC must include the map for adjacent départements (for interventions in "border" sectors, hot pursuit outside the *département*, etc.).

Tools do currently exist that enable a degree of interoperability between services, but they tend to be insufficient, especially when it comes to managing complex or large-scale situations. Once again, by adopting common core technologies or dedicated interfaces, police officers, *gendarmes* and firefighters should be able to share their information, and the details of their interventions. These new possibilities could even include the shared geolocation of all responders and the reciprocal communication of available forces, including the military forces deployed under the *Sentinelle* anti-terrorism operation (data that are not currently exchanged on IT applications).

Decompartmentalization must also be performed vertically within directorates. A command center must, as a minimum, have visibility on the activity of smaller adjacent centers, in order to support them if needed, or even step in to take control of crisis situations. Likewise, this visibility must apply continuously up to the general staff of the central directorates of the police and DGPN (incident files, maps, geolocation, etc.) to whom information is currently passed only via email or in telephone reports.

The same possibilities must be made available to the crisis centers at the prefectures (*cf.* the departmental operations centers (CODs)).

Leverage digital to manage incidents more effectively

In addition to the handling of incoming emergency calls, as mentioned above, the use of digital tools is likely to bring significant added value when it comes to managing incidents and directing teams at the front line.

To derive maximum advantage from future mobility options (the use of smartphones and tablets by police officers and *gendarmes*), command centers must be given the possibility to send digitized documents (emergency response guides, intelligence reports, wanted person notices, various instructions, photographs, video surveillance images, etc.) directly to patrols, to back up commands transmitted by radio. Experiments under way, in France and abroad, clearly show that, in the near future, operational information will no longer be transmitted by voice alone. Technical decisions need to be made rapidly in order to anticipate new multimedia uses in exchanges between operational centers and field units, made possible by recourse to off-the-shelf multi-application terminals. In parallel, this movement must be accompanied by an operational command doctrine, to prevent the anarchic development of unregulated systems.

These changes presuppose that the process of replacing the current, ageing, INPT network with a secure broadband radio network is finalized. Only on this condition can the police and *gendarmerie* services respond to the new modes of information transmission used every day by the population, and profit from the essential information conveyed by images, sound, text or geolocation data.

Finally, even if the human operators must have the last word, preserving a degree of initiative, some thought should be given to what Big Data—leveraged by sophisticated algorithms and tested predictive policing solutions—can offer in terms of decision support: assigning interventions according to the geolocation of vehicles, organizing pursuit or dragnet operations, monitoring a specific area at a specific moment, adapting the rotation cycle of video surveillance cameras, etc. Prior testing, however complex it may be to organize, is probably going to be the best way to assess the relevance and effectiveness of such approaches.

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Integrate drones into command center capabilities

Whether tracking convoys, road traffic or crowd movements, or participating in search operations, helicopters already provide valuable support to ground units and command centers.

Increasingly, drones will assist in this role, both for monitoring demonstrations and for stealth operations (in crisis situations, etc.) in outdoor, but also indoor, environments.

We should already be thinking about how to integrate the full range of airborne resources into the operational capabilities of the CICs and CORGs: fleet deployment, piloting, access to images, etc.

Make optimal use of image walls

Unlike the prefecture of police, which was quick to see the possibilities offered by image walls at its command center (DOPC), centralizing images from some 20,000 cameras deployed in public areas, the DGPN and the DGGN for a long time restricted video surveillance to a crime prevention role, leaving the management of these images to municipal police forces or urban surveillance centers (CSUs).

The rapid improvement in the quality of real-time video transmission and the growing importance of images to convey information have made it essential to integrate video surveillance into the CICs and CORGs as a decision support tool. The developments observed recently in this field must be pursued further and generalized.

The command centers must therefore be equipped with the main functionalities for controlling the cameras (direction, zoom, etc.). When managing an incident or an intervention, the mapping module must be capable of indicating the presence of any video surveillance cameras in the vicinity, and of screening the corresponding images. It must be possible to record short video sequences and attach them to the corresponding incident file. Finally, the command centers must have the necessary interfaces to accommodate and display large number of videos from institutional and private partners (haulage contractors, car parks, and the like).

Bring the social networks into the command centers

Because they are a tool of instant mobilization, with the power to reach large numbers of people in real time, the social networks can be a source of valuable information for the security forces: detecting incidents, tackling developments in demonstrations, anticipating crowd movements by analyzing the forwarding of messages, monitoring crisis situations (natural disasters, major accidents, terrorist

attacks, etc.) and, in return, broadcasting alerts or anti-rumor messages, etc. The Paris fire brigade had has such a system up and running at its command center for several years already.

Once re-processed or reformatted, this information could also be sent out to the teams on the ground to enable them to adapt their intervention accordingly. It could also be used to enrich reports submitted to higher ranks.

Integrating such a capability, of course, raises the question of the technological equipment and solutions that will enable adequate surveillance and response in terms of communications. There are also questions about ergonomic layout and work organization in the command room: to fully harness the potential of this new capability requires fluid and responsive exchange between operators. It also requires equipment that will enable specially-trained personnel (trained in the tools and in crisis communication) to be operationally present and to communicate in real time.

Initiate a new relationship with the population

Leverage new digital services to get closer to the public

To create a new, deep and lasting bond with citizens, the institutional communication effort must be supplemented by a genuine palette of online services, to create an element of proximity, familiarity and "service".

A number of options can already be put forward:

- Expand the scope of online pre-reporting by the public;
- Propose personalized alerts (by email or SMS) based on place of residence, property owned, and demographic or even geolocation criteria;
- Enable online information exchange (by instant messaging or webcam);
- Create a channel for the direct and immediate reporting of information or witness statements, open to the public at large during crisis situations (hostage-takings, major traffic accidents, natural disasters, etc.), along the lines of *"Alerte enlèvement"*, France's Amber alert system;
- Offer assistance to victims and witnesses (online action guidelines and a dedicated communication channel);
- Develop appeals for witnesses;
- Put public crime data online (for the sake of transparency, but also to be consistent with the government's open data policy);
- Propose an online option for making personal appointments at local police stations (*e.g.* name and contact details of the lead officer, names and contact details of desk staff).

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Encourage and consolidate citizen involvement

Above and beyond anything that digital technologies can contribute, the reinforcement of the bond of proximity with the citizens also depends on their involvement and their contribution–through appropriate channels–to the work of the police and the *gendarmerie*.

Reserves, whether civilian or operational, provide an excellent opportunity to breathe life into this bond, so long as processes are put in place to manage and mobilize these networks.

A number of initiatives build on cell phone geolocation to develop voluntary action during crisis situations. Previously registered citizens, with attested skills, who happen to be present at the site of a serious incident would provide assistance by aiding victims, supplying intelligence or witness statements to the operational teams, or helping to secure or cordon off an area. This geolocation principle could also be applied to members o the reserves.

Similar initiatives are also being developed in the private sphere, such as the mobile application Qwidam, which aims to reinforce the security of citizens by encouraging day-to-day solidarity and mutual assistance, based on SOS messages or alerts sent by users of the application and shared with other users within a radius of 500 meters. The police and *gendarmerie* might reflect on the role–if any–they want to play in the spread of these increasingly popular solutions.

Citizen involvement can also be fostered by making more frequent, more visible, and therefore more proactive use of appeals for witnesses. Such procedures should not be restricted to (rather timid) appeals on the internet, and could involve any type of crime and any geography. French culture admittedly tends to be reticent about anything seen as encouraging people to inform on each other, but initiatives by Spain's *Policía Nacional* confirm that appeals for witnesses have a real impact and have sometimes even played a key role in solving certain cases. [30]

Finally, proximity could also be developed by reaching out to citizens and canvassing their expectations (*via* regular public meetings at local level, qualitative research, surveys, etc.), and allowing front-line police officers and *gendarmes* to express themselves within the safe space of quality circles. In the early 2010s, the police of Pittsburgh (USA) reviewed its crime-fighting strategy after conducting surveys of civil society and of its own personnel. This generated a better understanding of expectations, which in turn led to improved communication and cooperation within the police, closer collaboration with the public and, more broadly, greater trust in the institution. Ultimately, the fight against crime emerged stronger and more effective.

(30) An anti-drug-trafficking campaign on Spanish social networks in January 2012 elicited 25,000 emails and led to 850 arrests. Other campaigns–anti-domestic violence, wanted persons–have met with similar success.

***

As our work draws to a close, we are firmly convinced that the digital transformations for which the French security forces must now prepare are not the reflection of a headlong race for technology. On the contrary: they underline the absolute need to put the human factor–whether the members of the security forces or the citizens they serve–back at the heart of the system, and the center of public action.

As Charles de Gaulle declared at a press conference on March 25, 1959, *"In truth, in our time, the only thing worth arguing about is Man. It is Man that we must save, nurture and develop"*.

***

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

APPENDICES

Appendice 1

Acronyms and abbreviations

French		*English gloss*
ANSSI	agence nationale de la sécurité des systèmes d'information	National agency for information system security
APJ	agent de police judiciaire	Judicial police agent
BDSP	base de données de sécurité publique (gendarmerie nationale)	Public security database (national gendarmerie)
BEFTI	brigade d'enquêtes sur les fraudes aux technologies de l'information (Préfecture de Police)	IT fraud investigation brigade (Prefecture of Police)
C3N	centre de lutte contre les criminalités numériques (gendarmerie nationale)	Digital crime-fighting center (national gendarmerie)
CIC	centre d'information et de commandement	Information and command center
CORG	centre opérationnel de renseignement de la gendarmerie (niveau départemental)	Operational intelligence center of the gendarmerie (department level)
CROGEND	centre de renseignement opérationnel de la gendarmerie (niveau national)	Operational intelligence center of the gendarmerie (national level)
CSU	centre de surveillance urbain	Urban surveillance center
DCPJ	direction centrale de la police judiciaire	Central directorate of the judicial police
DGAFP	direction générale de l'administration de la fonction publique	General directorate of civil service administration
DGGN	direction générale de la gendarmerie nationale	General directorate of the national gendarmerie
DGPN	direction générale de la police nationale	General directorate of the national police

DGSE	direction générale de la sécurité extérieure	General directorate of external security
DGS	direction générale de la sécurité intérieure	General directorate of internal security
DGSCGC	direction générale de la sécurité civile et de la gestion des crises	General directorate of civil security and crisis management
DINSIC	direction interministériel du numérique et des systèmes d'information et de communication	Interministerial department for digital and for information & communication systems
DMIS	délégation ministérielle aux industries de la sécurité	Ministerial delegation to the security industries
DOPC	direction de l'ordre public et de la circulation (préfecture de police de Paris)	Directorate of public order and traffic (Paris Prefecture of Police)
DSIC	direction des systèmes d'information et de communication (ministère de l'Intérieur)	Directorate of information & communication systems (Interior Ministry)
EC3	European cybercrime center (Europol)	European cybercrime center (Europol)
GIR	groupe d'intervention régional	Regional intervention group
ICC	investigateur en cybercriminalité (police nationale)	Cybercrime investigator (national police)
INPT	infrastructure nationale partagée des transmissions	National shared transmission infrastructure
JIRS	juridiction inter-régionale spécialisée	Specialized inter-regional jurisdiction
LAPI	lecteur automatisé des plaques d'immatriculation	Automatic license-plate recognition (ALPR)
LOPPSI	loi d'orientation et de programmation pour la performance de la sécurité intérieure	Orientation and programming law for internal security performance
LRP-GN	logiciel de rédaction des procédures de la gendarmerie nationale	Report editing software (national gendarmerie)
LRP-PN	logiciel de rédaction des procédures de la police nationale	Report editing software (national police)
MGMSIC	mission de gouvernance ministérielle des systèmes d'information et de communication	Ministerial governance mission on information & communication systems
OCLCTIC	office central de lutte contre la criminalité aux technologies de l'information et de la communication ; police nationale)	Central office for the fight against ICT-related crime (national police)
OPJ	officier de police judiciaire	Judicial police officer

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

PHAROS	plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (police nationale)	Platform for harmonizing, analyzing, cross-checking and referring reported infringements (national police)
PTS	police technique et scientifique	Forensic police
RESCOM	messagerie d'autorité de la police nationale	National police command transmission channel
SCRC	service central de renseignement criminel (gendarmerie nationale)	Central criminal intelligence service (national gendarmerie)
SCRT	service central de renseignement territorial	Central territorial intelligence service
SDAO	sous-direction de l'anticipation opérationnelle (gendarmerie nationale)	Operational foresight subdirectorate (national gendarmerie)
SDIS	service départemental d'incendie et de secours	Departmental fire and rescue service
SDLC	sous-direction de la lutte contre la cybercriminalité (police nationale)	Subdirectorate for the fight against cybercrime (national police)
SGMAP	secrétariat général à la modernisation de l'action publique	General secretariat for public service modernization
STAD	système de traitement automatisé de données	Automatic data processing (ADP) system
ST(SI)²	Service des technologies et des systèmes d'information de la sécurité intérieure	Internal security information systems and technologies service

Appendice 2

Experts interviewed

Ms. Vic BAINES, Trust and Safety Manager Europe, Middle-East and Africa, Facebook

Général de division **Simon-Pierre BARADEL,** Judicial Police Coordinator, DGGN

Mr. Alain BAUER, criminologist, CNAM

Mr. Willy BRUGGEMAN, Chairman of the Federal Police Council of Belgium

Mr. Elie BURSZTEIN, Head of Anti-Fraud and Anti-Abuse, Google

Mr. Patrick CALVAR, Director General Internal Security, DGSI

Mr. Matthieu CLOUZEAU, Director of Prevention and Protection, City of Paris

Vice-Amiral **Arnaud COUSTILLIÈRE,** Head of Cyber Security, French Defense Ministry

Mr. Thierry DELVILLE, Delegate to the Security Industries, French Interior Ministry

Colonel **Jean-Marc DETRÉ,** chargé de mission, Directorate of Operations and Employment, DGGN

Colonel **Christophe DUBUIS,** Training Bureau, DGGN

Mr. Christophe DURAND, Head of Cyber Strategy, Interpol, and his team

Mr. Christophe FICHOT, Comptroller General, Deputy Head of STSI²

Mr. Eric FILIOL, Head of the Operational Cryptography and Computer Virology Lab, ESIEA

Mr. Emile GABRIÉ, Head of State and Local Government Affairs, CNIL

Mr. Alejandro MARTINEZ GARCIA, Director, and **José Maria Rodriguez,** Development Director, Center 112, Madrid

Mr. Benoit GODARD, Liaison Officer for the European Cybercrime Center (EC3), Interpol, Europol

Ms. Carolina GONZÁLEZ and **Mr. Enrique SACRISTAN,** Section Heads, Press and Information Office, Spanish National Police

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

Mr. Cyril GOUT, Commissioner, Central Computer and Technology Tracking Service, Forensic Police Subdirectorate, France

Mr. Olivier GRUMELARD, Deputy Director, Information Systems Security Operating Center, and **Mr. Vincent STRUBEL,** Deputy Director for Expertise, ANSSI

Mr. Joachim KÄLLSHOLM, President, Securitas Sverige AB

Ms. Caroline KRYKWINSKI, Deputy Director, Interministerial HR Policy Management, DGAFP, and her team

Mr. Lionel LE CLEI, VP Communication & Security, Global Security Activities Advisor to the President, Thaless

Mr. Blaise LECHEVALLIER, Commissioner, Technology Advisor, Board of the DGPN

Colonel **Dominique LUCHEZ** and Lieutenant-Colonel **Bruno MAKARY,** Military Personnel Department, DGGN

Mr. Philippe LUTZ, Comptroller General, Deputy Director for Resources and Skills, National Police

Mr. Matteo PACCA, Senior Partner, McKinsey & Company

Lieutenant-Colonel **Pierre PASSÉ,** Recruitment, Testing and Examinations Bureau, DGGN

Mr. Dominique RENARD and **Cédric MURGIER,** Captains, OCLCTIC

Mr. Steve RICHARD, Chairman, National Observatory of Municipal Police Forces, France

Ms. Sylvie SANCHIS, Commissioner, Head of BEFTI

Mr. Yaron SAVORAY, Director for Europe and the Middle East at the McKinsey Center for Government and Leader of the Policing Service Line, McKinsey & Company

Colonel **Jérôme SERVETTAZ,** Commander, Criminal Intelligence Central Service, Colonel **Patrick PERROT,** Head of the Criminal Investigation and Analysis Division and Colonel **Franck MARESCAL,** Head of the Central Observatory on Smart Transport Systems, National Gendarmerie

Mr. Bernard STIEGLER, philosopher

Mr. Henri VERDIER, Interministerial Director for Digital and for Information and Communication systems, SGMAP and **Ms. Laure LUCCHESI,** Deputy Director, Etalab

Appendice 3
Bibliography

- *"Les défis technologiques des forces de sécurité intérieure"*, Delville report, Ministry of the Interior, June 2014
- *"Une police en réseau : une vision pour la police en 2025"*, Willy Bruggeman report, Belgian Federal Police Council, June 2014
- *"La gestion des carrières dans la police et la gendarmerie nationales"*, Cour des Comptes, February 3, 2015
- *"La fonction de police judiciaire dans la police et la gendarmerie nationales"*, Cour des Comptes, December 22, 2014
- *"Disruptive technologies: Advances that will transform life, business, and the global economy"*, McKinsey Global Institute, May 2013
- *"L'implication des citoyens dans la sécurité intérieure : jusqu'où ?"*, INHESJ, auditors' report, 2016 (forthcoming)
- *"La participation des militaires à la sécurité intérieure"*, INHESJ, auditors' report, 2016 (forthcoming)
- *"Enjeux et difficultés de la lutte contre la cybercriminalité"*, INHESJ, auditors' report, July 2015
- *"Les politiques publiques de vidéoprotection : l'heure des bilans"*, INHESJ, auditors' report, February 2015
- *"Fichiers de police et libertés : des enjeux nationaux, une nouvelle donne internationale"*, INHESJ, auditors' report, January 2015
- *"Predictive policing: the role of crime forecasting in law enforcement operations"*, Rand Corporation, 2013

© INHESJ – June 2016 – Strategic Diagnostic Group No 3 Report

ÉCOLE MILITAIRE
1 place Joffre
Case 39
75700 PARIS 07 SP
Tél.: 33 (0)1 76 64 89 00
Télécopie : 33(0)1 76 64 89 31