CRSI

CENTRE DE RÉFLEXION
SUR LA SÉCURITÉ INTÉRIEURE

La Lettre de la Sécurité Intérieure



Numéro 5 - Printemps 2022

Ils soutiennent l'action du CRSI :

Sommaire

- L'édito du Président 3
- Le mot du Secrétaire général 4
- Brèves de sécurité 5
- L'actualité de la sécurité… vue du compte Twitter du CRSI 6

Les dossiers :

- Pour un usage augmenté de la biométrie au service d'une meilleure sécurité publique, par Benoît FAYET 7
- Zoom : Ailleurs en Europe, « Perspectives critiques sur le salafisme aux Pays-Bas », Par Guillaume LEFÈVRE 13
- La modernisation militaire de la Chine : « changement militaire majeur » ? par Tewfik HAMEL, Docteur en histoire militaire et études de défense (Université Paul-Valery – Montpellier 3) *Republication avec l'aimable autorisation de la Revue Défense Nationale, partenaire du CRSI* 18

Les exclusivités du CRSI :

- Dossier - Les services de renseignement militaires français 26
- Interview exclusive de Richard LIZUREY, ancien directeur général de la gendarmerie nationale, prédécesseur du général Christian RODRIGUEZ 35
- Focus sur les unités de Police Secours, Par Christelle GÉRARD 43
- Quel cadre légal international en matière de cybercriminalité ? : enjeux et défis. Par Marc-Olivier Boisset et Jean Langlois-Berthelot 46
- Cybersécurité : Focus sur le rapport annuel de l'UE sur les cybermenaces, Par Guillaume LEFÈVRE 56

Lu pour vous :

- « Surmonter les crises. Idées reçues et vraies pistes pour les entreprises », Par Raphaël de VITTORIS. 59

Nos activités récentes 62



L'édito du Président

Chers amis,

Après avoir fait le choix de ne pas interférer dans les campagnes électorales présidentielle puis législatives, le CRSI a le plaisir de vous adresser une nouvelle édition de sa Lettre de la Sécurité Intérieure.

Ce début d'année 2022 a été marqué par le retour de la guerre au cœur de l'Europe, 77 ans après la fin de la Seconde Guerre mondiale. Sans même parler du risque (réel) de voir la France se retrouver directement impliquée en fonction des différents scénarios possibles, l'impact de ce conflit sur la sécurité intérieure de notre pays est d'ores et déjà certain : la hausse des prix de l'énergie et de certaines matières premières, ainsi que les crises migratoires en cas de famine en Afrique ou au Maghreb, sont en effet susceptibles de produire des conséquences directes sur la stabilité de notre pays.

Ces conséquences de la guerre s'ajouteront aux sujets classiques inhérents à la sécurité intérieure. À cet égard, l'augmentation continuelle de la violence au sein de la société française (+ 32 % de violences volontaires enregistrées entre 2017 et 2021) est un facteur de préoccupation majeur. Violences autour du Stade de France le 28 mai dernier, multiples refus d'obtempérer et violences urbaines quasiment toutes les nuits : l'actualité récente regorge hélas d'exemples illustrant cette tendance lourde.

Aucun programme politique, qu'il soit économique, social ou culturel ne prospérera de façon pérenne sur un socle social aussi profondément fracturé. Il faut le dire et le répéter : la sécurité de nos concitoyens n'est pas un enjeu de droite ou de gauche, mais un prérequis primordial à la réussite de toute politique publique.

Le CRSI est au travail, poursuit sa mission et ses activités en lien avec la sécurité intérieure et espère que cette nouvelle Lettre de la Sécurité Intérieure répondra à vos attentes. Je remercie chaleureusement les différents auteurs et contributeurs qui ont participé à son élaboration.

N'hésitez pas à la partager largement avec votre entourage

Bonne lecture !

Thibault de MONTBRIAL
Président du CRSI



Le mot du Secrétaire général

Chers lecteurs, chers amis,

Pour bon nombre d'entre nous, la fin de la seconde Guerre Mondiale, puis de la Guerre Froide, nous avaient projeté dans une Europe en paix.

Une paix, du moins sur le territoire de l'Europe continentale que nous pensions durable et assurée.

Aujourd'hui, force est de reconnaître que la guerre est malheureusement peut-être à nos portes, et dans tous les cas, bien réelle en Ukraine, avec l'ensemble des conséquences et changements qu'elle entraîne, pour le monde entier, pour l'Europe bien sûr, et les Ukrainiens d'abord, pour la France aussi c'est certain.

C'est un changement profond auquel nous assistons et devons faire face dorénavant et l'équilibre devient fragile et l'avenir incertain.

La menace est sérieuse, y sommes-nous préparés réellement ? Sans doute jamais assez.

Au-delà de cette guerre qui détruit d'ores et déjà un pays, l'Ukraine, et des menaces pour notre sécurité européenne comme nationale, l'année 2021 s'est achevée comme l'année 2022 a débuté : hausse des atteintes aux biens et aux personnes, hausse des violences à l'encontre des policiers et gendarmes, hausse de la cybercriminalité, menace terroriste (davantage endogène) toujours très élevée, islamisme croissant…

Le contexte économique et social jumelé au contexte sanitaire (crise COVID 19), les récentes tensions (d'une rare intensité) en Corse, renforcent encore les difficultés et menaces auxquelles nous sommes confrontés et pour lesquelles une réponse adaptée en matière de sécurité intérieure est toujours nécessaire. À cette nécessité d'ordre et de réponse autant opérationnelle et pragmatique, que politique et institutionnelle, viennent donc se greffer les questions de Défense avec la guerre en Ukraine qui pourrait s'étendre et constituer un conflit d'ordre mondial aux conséquences désastreuses.

Cette nouvelle Lettre de la Sécurité Intérieure vous apportera de nouveaux éclairages, sur la sécurité intérieure bien sûr, avec notamment à partir de ce numéro et les prochains, un dossier spécial consacré aux différents services de renseignements français (civils et militaires), dont il est important en cette période si particulière de rappeler le rôle essentiel.

Par ailleurs, j'ai souhaité vous proposer, très prochainement, et je m'y attache personnellement, un numéro spécial de notre LSI consacré à la guerre en Ukraine.

En ces temps troubles et plus que jamais, restons conscients et les yeux ouverts sur le monde qui nous entoure, et sachons ensemble relayer les valeurs républicaines et françaises qui nous animent, tout comme veiller à la sécurité de nos concitoyens et de nos institutions.

Bien à vous,



Guillaume LEFÈVRE
Secrétaire général du CRSI

Les chiffres du moment

Insécurité et délinquance, en 2021 :

- Homicides (y compris coups et blessures volontaires suivis de mort) : **+4 %**.
- Le nombre de victimes de coups et blessures volontaires (sur personnes de 15 ans ou plus) enregistrées augmente très fortement en 2021 : **+12 %** (après +1 % en 2020 et +8 % en 2019)
  - **+14 %** pour les victimes de violences intrafamiliales.
  - **+9 %** pour les victimes d'autres coups et blessures volontaires.
- La hausse est également très nette pour les escroqueries : **+15 %**.
- La hausse est encore plus forte pour les violences sexuelles enregistrées : **+33 %**.
- Les vols sans violence contre des personnes augmentent : **+5 %** (après -24 % en 2020).
- Les vols d'accessoires sur véhicules : **+4 %**.
- Les cambriolages de logements et les vols de véhicules sont stables (après respectivement -20 % et -13 % en 2020) et les vols violents diminuent encore en 2021 : **-2 %** pour les vols avec armes.
- Les vols violents sans arme : **-6 %**.
- Le nombre de mis en cause augmente fortement en 2021 en matière de lutte contre les stupéfiants :
  - **+38 %** pour usage dans un contexte de mise en place des amendes forfaitaires délictuelles.
  - **+13 %** pour trafic.

Source : *Rapport Insécurité et délinquance en 2021 : une première photographie - Interstats Analyse N°41* (ministère de l'Intérieur).

Autres données :

- La part des français qui jugent le bilan négatif en matière de sécurité sur le quinquennat en cours : **59 %.** (Source : *Le Journal du Dimanche, 23 janvier 2022*).
- La part des français qui jugent le bilan positif en matière de délinquance et de criminalité sur le quiquennant en cours : **28 %.** (Source : *Le Journal du Dimanche, 23 janvier 2022*).
- La part des français qui ont très confiance ou plutôt confiance dans la police : **72 %.** (Source : *sondage CEVIPOF, janvier 2022*).

L'actualité de la sécurité… vue du compte Twitter du CRSI

CRSI a retweeté

Thibault deMontbrial
@MontbrialAvocat

Le #BCRA (services secrets de la France Libre) est né il y a 80 ans. Bon anniversaire à l'ancêtre de nos Services et en particulier de la #DGSE, et hommage à ceux qui œuvrent dans l'ombre et dans le monde entier à la #sécurité de notre pays #renseignement

Ordre de la Libération - Invalides @O2LaLiberation · 17 janv.
Il y a 80 ans naissait le Bureau central de renseignements et d'action (BCRA), les services secrets de la France libre dont la DGSE est en grande partie l'héritière. Le chef du BCRA, le colonel Passy, qui est Compagnon, est l'inventeur d'un nouveau modèle de renseignement !
Afficher cette discussion



CRSI a retweeté

G. Lefèvre
@lefevreg

#Sécurité #Violences #Gendarmerie On a frôlé le drame : au moins un #tir à balles réelles visant des #gendarmes mobiles lors d'une manifestation en #Corse le 3 avril dernier @CRSI_Paris



pandore-gendarmerie.org
Des gendarmes mobiles visés par au moins un tir à balles réelles en Corse - Le …
Manifs sous très haute tension en Corse. La police judiciaire est à la recherche d'un homme qui a tiré à l'arme de poing en direction de gendarmes mobiles. La …

CRSI
@CRSI_Paris

Explosion de la #violence en France: focus sur la forte augmentation des homicides et tentatives d'homicide @Le_Figaro

Christophe Cornevin @ccornevin · 30 janv.
L'inquiétante explosion des tentatives d'#homicide. Climat de tension exacerbée, passages à l'acte plus fréquent : voici le cocktail détonnant que décrypte l'ami @leclercjm @Le_Figaro #Violence
lefigaro.fr/actualite-fran…

CRSI a retweeté

G. Lefèvre
@lefevreg

#Justice #Terrorisme Le parquet national antiterroriste #Pnat a annoncé ce 19 janvier, avoir ouvert une #enquête pour #assassinat en relation avec une entreprise terroriste après le meurtre samedi d'une touriste française à #Tiznit au #Maroc @CRSI_Paris



nouvelobs.com
Une touriste française de 79 ans tuée sur un marché au Maroc, enquête ouvert…
L'attaque a eu lieu samedi à Tiznit, dans le sud du Maroc.

CRSI a retweeté

G. Lefèvre
@lefevreg

#Sécurité #Justice #Cybercriminalité Le groupe de #ransomware Lockbit 2.0 annonce avoir piraté le Ministère de la Justice français et menace de publier des documents d'ici 2 semaines (pas de précision sur leur nature ni l'ampleur du #piratage) @CRSI_Paris



capital.fr
Des hackers piratent le ministère de la Justice et réclament une rançon
Un groupe de hackers menace de publier des fichiers volés au ministère de la Justice si une rançon n'est pas payée avant le 10 février prochain., Le cœur de l…

https://twitter.comCRSI_Paris

Note de réflexion : Pour un usage augmenté de la biométrie au service d'une meilleure sécurité publique

par Benoît FAYET (Membre du Comité stratégique du CRSI)

Les événements sportifs mondiaux à venir en France en 2023 (Coupe du monde de rugby) et 2024 (Jeux Olympiques et Paralympiques) **sont une formidable perspective pour notre pays mais représentent également une menace majeure en terme de sécurité publique.** L'amélioration des capacités de contrôle et de vérification des identités à grande échelle, la mise à disposition de base de données plus fiables et l'usage de technologies adaptées pour les forces de sécurité intérieure sont, entre autres, des enjeux clés pour être en mesure de répondre aux attentes liées à l'organisation future de ces évènements mondiaux. Au-delà de ces évènements, la situation sécuritaire fortement dégradée en France aujourd'hui (terrorisme, violences et insécurité au quotidien, crise migratoire, ...) appelle à identifier des solutions capables d'apporter sur le long terme des réponses pour assurer la sécurité des citoyens.

Parmi ces solutions, l'usage des biométries au service de la sécurité publique doit être débattu. Le début de quinquennat et la perspective d'une nouvelle loi d'orientation et de programmation du ministère de l'intérieur (LOPMI) doivent permettre ce débat pour améliorer la sécurité des français de manière durable tout en ne transigeant pas sur la protection des données et leur bon usage qui sont autant de principes fondamentaux de notre société.

Biométrie, biométries ? Quel cadre juridique ?

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques ou biologiques. La biométrie évolue aujourd'hui au-delà des techniques « historiques » (biométrie faciale, digitale ou génétique) avec d'autres techniques émergentes (biométrie comportementale, olfactive, vocale,...) présentant des maturités techniques et technologiques différentes, faisant que l'on parle désormais des biométries ou de la multi-biométrie. **La reconnaissance biométrique de l'individu se fait par identification ou par authentification**. L'identification consiste à repérer un individu dans un espace et une population donnée à partir de ce qui est déjà connu de lui d'un point de vue biométrique et l'authentification consiste à confronter des données biométriques déjà enregistrées à celles présentées par un individu lors d'un contrôle.

Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (empreintes digitales, ADN, ...). À ce titre, les données biométriques ont légitimement un cadre juridique strict et sont classées dans la catégorie des données sensibles au sens de la loi « informatique et libertés » et du RGPD (1).

(1) Règlement européen relatif à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Le RGPD interdit le traitement des données biométriques aux fins d'identifier une personne physique de manière unique mais des exemptions sont prévues quand la personne concernée a consenti au traitement de ses données, lorsque le traitement porte sur des données rendues publiques par cette personne ou pour des motifs d'intérêt public. Ce cadre juridique a été complétée dernièrement par la Directive « police-justice » qui autorise le traitement des données biométriques aux fins d'identifier une personne physique de manière unique seulement en cas de nécessité absolue et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.

Quels usages aujourd'hui de la biométrie par les forces de sécurité intérieure ?

La biométrie est depuis longtemps utilisée par les policiers nationaux ou les gendarmes au quotidien et constitue un outil indispensable et essentiel d'un point de vue opérationnel dans leurs missions d'enquête, de recherche d'auteurs d'infractions et de matérialisation de la preuve, de surveillance et de contrôle du territoire qui, par nature même de ces missions, nécessitent de reconnaître l'identité de personnes.

La biométrie est devenue indispensable notamment pour les activités de lutte contre la fraude et l'usurpation d'identité par rapport aux moyens existants liés à de la donnée alphanumérique.

Des fichiers informatiques (2) ont été créés permettant, dans l'exercice de ces missions de sécurité intérieure, de collecter des données biométriques digitales ou génétiques et de procéder à une signalisation biométrique de personnes ayant commis des infractions.

D'autres fichiers informatiques disposent également de données biométriques, comme le TAJ (3) par exemple ou figurent des images faciales de certaines personnes qui y sont inscrites. En outre, de récents règlements européens visant à renforcer le contrôle aux frontières extérieures de l'UE et la coopération policière entre les pays membres de l'accord de Schengen prévoit que des données biométriques (photographies, empreintes digitales) figurent à terme dans les fichiers nationaux de ces pays, qui pourraient alors être interrogés sur ces données en cas de signalement. Une mise en conformité de la France à ces règlements est en cours.

Quels usages demain de la biométrie par les forces de sécurité intérieure ?

Au-delà de ces usages existants, les nouvelles potentialités technologiques actuelles autour de la biométrie doivent être étudiées pour permettre aux forces de sécurité intérieure d'être plus performantes dans leurs missions de sécurité publique, de police judiciaire, de renseignement ou de contrôle aux frontières.

Il apparaît que la Coupe du monde de rugby en 2023 et les Jeux Olympiques de 2024 sont une opportunité de tester en situation réelle ces nouveaux usages dans un cadre expérimental juridiquement strict (loi d'expérimentation, ...) avant d'éventuellement les généraliser ensuite au-delà de ces évènements, si ces usages sont concluants et respectent la protection des données personnelles. Il semble notamment que la Coupe du monde de rugby, évènement de moindre ampleur, pourrait être le cadre d'expérimentations réunissant l'ensemble des acteurs concernés, juridique, opérationnel (policiers nationaux et gendarmes) et politique.

(2) Fichier automatisé des empreintes digitales (FAED) et Fichier national automatisé des empreintes génétiques (FNAEG).
(3) Traitement des Antécédents Judiciaires.

Il convient en effet de dépasser les débats actuels via des expérimentations concrètes, pour s'assurer que les technologies répondent aux besoins opérationnels des forces de sécurité intérieure, définir précisément avec les acteurs juridiques concernés les cas d'usage, l'analyse d'impact relative à la protection des données personnelles, construire le cadre de contrôle et d'évaluation nécessaire et enfin tester et démontrer la maturité technique de technologies qui seront alors meilleures et mieux maitrisées une fois ces expérimentations réalisées. Seuls des tests en situation réelle menés en France permettront en outre de développer des technologies de confiance en lien avec l'écosystème industriel national.

La distinction entre authentification et identification biométrique évoquée plus haut est structurante pour maintenir un niveau acceptable juridiquement de l'usage de la biométrie au service de la sécurité publique. L'identification biométrique n'apporte pas de garantie à date, à ce titre, en terme de fiabilité technologique et donc d'un point de vue juridique. Il apparaît donc que le recours à l'authentification biométrique est donc plus acceptable juridiquement et plus fiable technologiquement à ce jour et que cela peut être, lors des événements sportifs de 2023 et 2024, une solution à expérimenter. L'authentification biométrique pourrait ainsi être testée pour accéder à des sites lors de la Coupe du monde de rugby et les Jeux Olympiques (stades, fans zones, village olympique, centres d'entrainement). Une fois l'analyse d'impact relative à la protection des données personnelles réalisée, si le cadre technologique et les gains opérationnels sont réels, une extension à des cas d'usage ultérieurs pourrait alors être envisagée, comme l'authentification biométrique pour des accès à des sites sensibles (sites touristiques ou culturels par exemple) qui nécessitent un ticket ou les personnes se sont déjà authentifiées pour accéder à ces sites. **En terme d'authentification, la biométrie digitale ou faciale peut ainsi renforcer les dispositifs d'authentification aux points d'accès à des sites sensibles.** Elle fiabilise le processus de contrôle qui repose aujourd'hui essentiellement sur des cartes ou des titres d'identité dont l'utilisation peut être facilement usurpée. Le but recherché est la lutte contre les risques d'intrusions par usurpation d'identité ou de badges dans des sites réunissant du public. Ces authentifications pourraient se faire sur le modèle du dispositif de contrôle aux frontières PARAFE, sans stockage centralisé de données à caractère personnel et sans recours à une base de données biométriques pour comparer des données.

L'authentification biométrique est aussi un levier intéressant pour servir ensuite dans d'autres cadres, comme les transports en commun, gares ou stations de métro pour repérer des individus recherchés sur la base de listes de personnes préalablement définies (watchlists) encadrées juridiquement et issues de fichiers informatiques du type FPR (4), ce qui permet de limiter l'impact en terme de protection des données et de ne pas opérer une surveillance indifférenciée de l'ensemble des personnes présentes dans une station ou une gare. Dans ce cas d'usage (temps réel dans l'espace public), l'un des principaux termes du débat porte sur les données d'entrée à insérer dans le dispositif, l'expérimentation reposant en effet sur des listes de personnes recherchées suivant des critères définis en amont.

(4) Fichier des personnes recherchées (FPR).

L'utilisation de watchlists issues de fichiers informatiques supposerait un travail en amont d'analyse d'impact en terme de protection des données personnelles du fait de l'utilisation d'une partie des données de ces fichiers informatiques au regard du principe de proportionnalité défendue par la CNIL et devrait naturellement faire l'objet d'une autorisation par la loi ou un décret.

L'authentification biométrique peut aussi permettre de rechercher dans un espace donné une personne prédéfinie via de la reconnaissance faciale. Il est techniquement possible de localiser dans un espace défini ou parmi une foule définie des personnes recherchées pour une infraction via un scan avec les concordances possibles avec des fichiers préalablement autorisés à être consultés juridiquement. **Il n'est donc pas nécessaire d'identifier l'ensemble des personnes présentes dans l'espace et qui n'offrent pas de correspondance avec la base de recherche.** Cette technologie peut également se limiter à des cas d'usage spécifiques que ce soit la recherche d'une personne jugée dangereuse dans une zone où elle aurait été repérée, à des fins de prévention ou de poursuite ou la recherche d'une personne disparue en danger ou identifiée comme victime.

L'analyse pourrait se faire à terme sans reconnaissance faciale via d'autres biométries, comme la biométrie comportementale.

Expérimenter en situation réelle la biométrie comportementale lors de la Coupe du monde de rugby et les Jeux Olympiques est une piste intéressante pour faciliter l'identification des situations de danger et détecter automatiquement des anomalies dans un espace donné et bien délimité, via le déploiement de scanners corporels par exemple.

Il s'agit de solutions qui pourraient être testées puis être étendues à terme, au-delà de ces évènements qui sont une occasion unique de tester en situation réelle une approche multi-biométrique et tenir compte de l'émergence des biométries dites « à distance » (visage, voix, odeur). Les biométries à distance sont capables de repérer des situations anormales et de donner l'alerte notamment d'intrusions, de franchissements massifs, de colis suspects ou encore de bagarres ou agressions.

Les résultats des expérimentations réalisées jusqu'alors ne semblent pas concluants, aussi, la Coupe du monde de rugby et les Jeux Olympiques à venir doivent être l'opportunité de tester à nouveau ces dispositifs pour, s'ils sont concluants juridiquement (après analyse d'impact relative à la protection des données personnelles), technologiquement et opérationnellement, les étendre à des cas d'usage ultérieurs. **Les biométries à distance peuvent en outre optimiser le visionnage des caméras de vidéoprotection ou des caméras embarquées (véhicules) ou piétons. L'analyse automatisée a posteriori rend possible un traitement d'images en grande quantité qui aurait été difficile ou impossible pour des opérateurs humains.**

Enfin, une autre opportunité liée à la biométrie concerne la modernisation des équipements mobiles des forces de sécurité intérieure.

En lien avec l'authentification biométrique, l'idée serait de développer des solutions de captation biométrique adaptées aux smartphones utilisés au quotidien par les policiers nationaux et les gendarmes dans le cadre de leurs missions de sécurité publique ou de police judiciaire (5),

(5) Terminaux NEO.

pour authentifier un individu en temps réel aux abords d'un site sensible ou en amont d'un évènement via des capteurs d'empreintes digitales sans contact ou de la biométrie du visage via la caméra d'un smartphone.

Ces solutions sans contact répondant en outre aux enjeux sanitaires actuels. Les technologies de captation biométrique déportées sur smartphone existent et sont disponibles. Il peut être opportun de les tester à grande échelle lors de la Coupe du monde de rugby et les Jeux Olympiques à venir pour, si elles sont concluantes juridiquement (après analyse d'impact relative à la protection des données personnelles), technologiquement et opérationnellement, les étendre à des cas d'usage ultérieurs.

Le développement de modules techniques d'interrogation des fichiers informatiques (TAJ, …) depuis un smartphone à partir de la captation numérique d'une empreinte digitale peut aussi être une piste de réflexion et une solution à tester, spécifiquement pour les opérations de vérification d'identité ou d'investigation judiciaires qui le justifient. Naturellement, une analyse d'impact juridique devrait être effectuée au préalable pour cela, sachant que le recueil d'empreinte digitale dans le cadre d'une vérification d'identité est une possibilité désormais offerte par des récents règlements européens (6).

En conclusion, au regard de la situation sécuritaire très dégradée aujourd'hui en France, il semble indispensable d'envisager des moyens nécessaires à un renforcement de la protection des français.

Les prochains évènements sportifs mondiaux à venir en France doivent être ainsi l'opportunité de tester en situation réelle de nouveaux usages des biométries au service d'une meilleure sécurité publique. Cet usage de technologies ne doit pas être une fin en soi mais un levier supplémentaire pour renforcer à long terme la sécurité des français au-delà de ces évènements, tout en garantissant la protection des données personnelles et leur bon usage qui sont autant de principes fondamentaux de notre société, ce que peuvent permettre des expérimentations en amont et en situation réelle.

(6) Règlement (UE) n° 2018/1862 relatif au Système d'information Schengen.

À propos de l'auteur de ce dossier :



Le CRSI remercie **Benoit FAYET** (ci-contre) pour sa contribution.

Diplômé de Sciences-Po Paris, Benoit Fayet a exercé dans le conseil en stratégie et management puis dans le secteur de la sécurité des particuliers.

Il est aujourd'hui consultant dans un cabinet de conseil en transformation digitale. Il effectue des missions de conseil au profit de ministères régaliens sur des enjeux et des problématiques de sécurité intérieure et de transformation numérique.

Benoit FAYET est membre du Comité stratégique du CRSI.

Contact :

Courriel : benoit.fayet@soprasterianext.com
LinkedIn : https://fr.linkedin.com/in/benoit-fayet

Zoom : Ailleurs en Europe, « Perspectives critiques sur le salafisme aux Pays-Bas »

Par Guillaume LEFÈVRE

Une étude publiée en 2021 par le Centre International de Lutte contre le Terrorisme (ICCT International Centre for Counter Terrorism, situé à La Haye) examine les effets du salafisme sur certaines communautés musulmanes aux Pays-Bas.

Dans l'étude, 15 entretiens ont été menés avec des membres de la communauté musulmane néerlandaise. Certains des principaux enseignements et conclusions du rapport mettent en évidence les échecs des politiques interventionnistes de l'État pour freiner la propagation du salafisme dans le pays. L'étude détaille également certains des aspects les plus méconnus concernant la popularité soudaine du mouvement islamiste radical.

En général, les généralisations sur la communauté musulmane néerlandaise faites par des personnalités politiques publiques ont découragé les musulmans néerlandais ordinaires et modérés de coopérer avec la sécurité de l'État. Au lieu d'aliéner le mouvement radical marginal, les politiques gouvernementales ont réussi à aliéner l'ensemble du segment musulman, ce qui a découragé les efforts pour arrêter la propagation du salafisme et, en fait, a conduit à l'impulsion opposée.

L'étude fait d'abord une distinction importante en soulignant que le salafisme se présente sous de nombreuses formes. Alors que les universitaires décrivent le mouvement comme un sunnite réformiste qui interprète la religion de l'islam dans sa forme la plus traditionnelle et la plus littérale selon les trois premières générations de l'islam, il est beaucoup plus complexe. Alors que cette définition convenait il y a des décennies, le mouvement a depuis évolué et maintenant les chercheurs préfèrent diviser davantage les salafistes en trois catégories : les puristes et les salafistes apolitiques, les salafistes politiques et les salafistes djihadistes. L'étude souligne que pour comprendre le problème actuel auquel est confrontée la société néerlandaise, il est important de comprendre que le salafisme n'est pas monolithique.

Origines du schisme

L'étude pointe vers l'année 2004 où un schisme s'est produit dans la société néerlandaise, marqué par l'assassinat de Theo Van Gogh, un réalisateur qui a réalisé un court métrage illustrant comment l'islam maltraite les femmes. Il a été tué par un djihadiste-salafiste nommé Mohammed Bouyeri et l'événement a été un catalyseur pour la rhétorique et les attitudes anti-islamiques dans la société. Cet événement a marqué le début d'une sécurisation de l'Islam radical qui a imprégné la société dans les décennies qui ont suivi l'attaque terroriste.

Avance rapide jusqu'en 2019, et un rapport de l'Institut Verwey-Jonker a été publié, qui a fourni des preuves convaincantes de l'incompréhension et du manque de recherches sur le phénomène du salafisme. Après avoir analysé 15 ans de littérature néerlandaise sur la question, sa conclusion était que la catégorisation des groupes salafistes non violents comme une menace pour la sécurité était une méthode contre-productive qui aliénait une grande partie des musulmans néerlandais non violents. En conséquence, plus de 50% des musulmans néerlandais pensaient que l'Occident souhaitait éradiquer complètement leur religion. L'étude de 2019 a suggéré que le recours à des sources secondaires plutôt qu'à des sources primaires compromettait la capacité de comprendre correctement le problème et de générer des solutions plus efficaces pour le combattre.

Les politiques de « titrisation » ont encore renforcé une mentalité « nous contre eux », souligne le rapport. Cela s'est traduit par des interactions musulmanes ordinaires avec les services de sécurité, caractérisées par une atmosphère d'anxiété et de paranoïa. Les musulmans ont le sentiment d'être pointés du doigt, ciblés et marginalisés par une société qui les méprise simplement à cause de leur foi.

Au cours des entretiens menés aux fins de l'étude, il a été conclu que les répondants sont devenus hyper conscients et sensibles à leurs niveaux de religiosité projetés. Les personnes interrogées dans le cadre de l'étude craignaient que la généralisation du salafisme par le gouvernement et sa définition incorrecte de ce que signifie pratiquer l'islam « strict » n'incitent de nombreux musulmans traditionnels à croire qu'ils seraient également considérés comme des salafistes. Cela a produit un sentiment « d 'hypervigilance » parmi les musulmans néerlandais, où beaucoup se sont sentis obligés de modérer leur comportement par crainte d'être perçus ou considérés comme des extrémistes. Ils ont vraiment senti que l'islam ne serait jamais pleinement accepté par la société néerlandaise en raison de la rhétorique stéréotypée constante contre l'islam invoquée par les médias, le gouvernement et les écoles. En conséquence, cela a produit des pratiques d'autocensure dans les communautés musulmanes.

Décideurs politiques mal informés

Une personne interrogée nommée Sara a décrit le terme « salafisme » comme un « terme fourre-tout » où les différenciations entre les différents types de salafisme n'étaient pas reconnues ou comprises par la société. Ce malentendu a bien sûr accru l'islamophobie dans la société néerlandaise. Une majorité écrasante de répondants considéraient les décideurs politiques comme mal informés, n'ayant pas correctement analysé et étudié la question de manière objective. En raison de ces lacunes politiques, l'étude a montré que les obstacles bureaucratiques empêchaient la société de surmonter les attitudes islamophobes et de dissiper les idées fausses sur le salafisme et l'islam dans son ensemble.

Les répondants ont mis en évidence un exemple de la manière dont les décideurs politiques étaient mal informés, soulignant l'idée de l'État selon laquelle les salafistes radicaux étaient largement concentrés dans les grandes zones métropolitaines.

Les répondants ont contesté cette notion et ont déclaré qu'en fait, il y avait une présence plus importante dans les petites villes en raison du fait que ces zones étaient moins surveillées et policières. Des endroits tels que Geleen, Oss, Delft, Leidschendam, Roermond, Maastricht, Ede, Den Bosch, Zeeland et Nimègue ont été cités par les personnes interrogées comme d'autres endroits où les salafistes radicaux se sont installés.

Capital social

Le sentiment d'identité nationale a également été cité par les personnes interrogées comme une force dissuasive pour rejoindre le salafisme radical. Les répondants de nationalité turque ont pointé le faible nombre d'individus extrémistes dans leur communauté qu'ils attribuent au fait d'un sentiment d'appartenance à une communauté turque. En raison des ressources culturelles élevées de cette communauté, cela a diminué le besoin des jeunes Turcs de chercher du capital social ailleurs. Ils étaient moins vulnérables et susceptibles d'être la proie de la propagande radicale et des tactiques de recrutement.

À l'inverse, les musulmans néerlandais d'origine marocaine ou algérienne ont été cités comme plus vulnérables en raison de leur manque de cohésion en tant que société ethnique et capital social. Les recruteurs salafistes ont pu saisir ces communautés vulnérables à la recherche d'un sentiment d'appartenance et exploiter les perceptions de discrimination et d'islamophobie au profit de leur programme de recrutement.

La puissance d'Internet

L'étude aborde ensuite les défis associés à la surveillance de la propagande djihadiste en ligne. La présence sur Internet a obtenu le troisième score le plus élevé dans la catégorie de l'enquête « influence radicale du salafisme ». Cela est dû en grande partie à l'émergence de la génération Z, qui maîtrise la technologie et est immergée dans la culture en ligne. Parce que ces jeunes individus ne connaissent qu'un monde où l'information est facilement disponible sur leurs appareils électroniques, cela les rend plus sensibles au recrutement en ligne, et moins au recrutement en face à face. La capacité d'atteindre ces jeunes esprits, qui ne sont pas encore pleinement développés et, par conséquent, très malléables, est une force extraordinaire qu'il est difficile de combattre correctement.

La raison pour laquelle les méthodes en ligne sont privilégiées et largement utilisées tient également au fait qu'elles comportent un faible risque de détection, contrairement au recrutement en face à face. Sa discrétion va également de pair avec la vitesse et le volume avec lesquels les informations peuvent être consommées et repartagées. Un orateur radical n'a pas besoin de travailler pour constituer un public physique auquel s'adresser, il a simplement besoin d'un appareil photo et son sermon peut être partagé de manière exponentielle en ligne et atteindre des milliers de personnes. Associé à un accès médiocre à l'éducation, en particulier aux connaissances islamiques appropriées, cela ne fait qu'augmenter la propension d'un individu à adhérer à une idéologie radicale, n'ayant aucune base solide pour exercer sa pensée et son jugement critiques.

Mauvaise connaissance de l'Islam

Cela est inhérent au fait que le besoin d'identité a obtenu un score plus élevé que la religion dans la catégorie recrutement, ce qui signifie que les individus sont largement attirés vers la radicalisation en raison de l'isolement social plutôt que de la conviction religieuse. En fait, les répondants ont caractérisé les salafistes djihadistes comme des individus principalement de faible foi qui ont été recrutés dans leur jeunesse, plutôt que d'être très religieux avant leur recrutement. En fait, un répondant a déclaré : « 99,9 % des jeunes [radicalisés] n'ont aucune connaissance et ne peuvent pas lire le Coran, et ne connaissent pas bien les traditions ».

Les mesures antiterroristes actuellement mises en œuvre par le gouvernement comprennent : la tenue de listes publiques des organisations salafistes actives, l'interdiction des centres d'asile salafistes, l'interdiction des relations gouvernementales avec des institutions salafistes connues, l'interdiction aux prédicateurs salafistes d'entrer aux Pays-Bas et l'interdiction du financement par l'Arabie saoudite, le Koweït et le Qatar, entre autres mesures. Cependant, l'étude conclut qu'une composante essentielle manquante de la stratégie consiste à impliquer les communautés musulmanes dans la prévention du salafisme politique ou djihadiste. Cela applique la mauvaise approche où les actes de terrorisme sont punis mais pas empêchés, ne faisant que mettre un pansement sur le problème et ne le corrigeant pas en son cœur. Ce n'est pas inhérent aux Pays-Bas, mais c'est un faux pas général en ce qui concerne les efforts de lutte contre le terrorisme dans le monde entier. Alors,

Quelle conclusion dans ce rapport ?

En conclusion, il y a un problème fondamental avec l'approche de l'État dans la lutte contre la radicalisation, comme le souligne clairement l'étude. Les raisons de la prolifération des radicaux salafistes sont liées à une combinaison de facteurs, notamment la facilité et le secret associés aux méthodes de recrutement en ligne, l'intolérance sociétale croissante et l'incompréhension du salafisme et de l'islam en général, le sentiment de marginalisation et de manque d'appartenance que les Néerlandais Les musulmans portent avec eux, et l'intense sécurisation qui a créé un sentiment de paranoïa et de peur au sein des communautés musulmanes d'apparaître « trop strictes » dans leur foi musulmane.

Une approche antiterroriste plus efficace serait celle d'une inclusion visant à prévenir les principales sources de radicalisation, plutôt que de simplement traiter les radicaux après qu'ils ont déjà commis des crimes ou imposé une menace à la société. Une méthode clé pour y parvenir serait de travailler aux côtés des communautés musulmanes et de les aider à identifier et à combattre les sources de radicalisation avant qu'elles ne se concrétisent.

Lire le rapport complet ici : fichier PDF



La modernisation militaire de la Chine : *« changement militaire majeur »* ?

Par Tewfik HAMEL, Docteur en histoire militaire et études de défense (Université Paul-Valery – Montpellier 3)

Lors du XIXe Congrès national du Parti communiste chinois (PCC) en octobre 2017, le président chinois et secrétaire général du PCC Xi Jinping a fait avancer le calendrier de la modernisation militaire de la Chine de près de 15 ans. Tout en exhortant les militaires à « être à la hauteur des missions et des tâches de la nouvelle ère », il a accéléré les objectifs de modernisation militaire, exigeant de l'Armée populaire de libération (APL) d'achever la mécanisation et de faire des progrès majeurs dans l'informatisation d'ici 2020, de devenir une armée entièrement « moderne » à l'horizon 2035 et d'être transformée en une armée de « classe mondiale » pour 2049, afin de soutenir le « rêve chinois du grand rajeunissement de la nation chinoise ».

L'objectif actuel de remodeler l'APL grâce à la technologie pour gagner la prochaine guerre dans des « conditions de haute technologie » est l'une des répliques d'un examen stratégique global qui a débuté dans les années 1990 (1). En 1995, le haut commandement a lancé des réformes pour faire passer l'APL d'une armée à forte intensité de main-d'œuvre à une armée à forte intensité techno- logique. En mars 2003, Jiang Zemin, alors président de la Commission militaire centrale (CMC) du PCC, a insisté sur l'impératif d'« avancer énergiquement une révolution des affaires militaires (RMA) aux caractéristiques chinoises, afin de garantir que nos forces armées suivent le développement rapide actuel de la science, la technologie et la RMA » (2). L'« innovation militaire » aux « caractéristiques chinoises » ne se limite pas à l'amélioration de l'équipement pour mieux refléter les exigences changeantes de la défense nationale.

Le principal objectif du plan directeur pour le développement de l'APL a été de réorganiser les systèmes et structures à tous les niveaux, et l'une des raisons pour lesquelles il y a autant de confusion sur le processus de réforme de l'APL est que la littérature existante ne différencie pas suffisamment deux types de changementmilitaire : 1) le « changement mineur » décrit un « changement dans les moyens et méthodes opérationnels (technologies et tactiques) qui n'ont aucune incidence sur la stratégie ou la structure organisationnelle » ; 2) alors que le « changement majeur » est un « changement dans les objectifs, les stratégies réelles et/ou la structure d'une organisation militaire » (3). Il se produit lorsque la technologie (nouvelle ou existante) converge avec l'adaptation des structures organisationnelles, des doctrines, des concepts de guerre et de la vision d'un conflit futur. Qu'en est-il alors de la modernisation de l'APL ?

(1) HAMEL Tewfik, « The Evolution of China's Military Strategy », Outre-Terre, n° 58-59, 2020, p. 199-146.
(2) LI Xiaobing, A History of the Modern Chinese Army, University Press of Kentucky, 2009, 432 pages, p. 2
(3) FARRELL Theo, TERRIFF Terry (dir.), The Source of Military Change, Lynne Rienner Publisher, 2002, 301 pages, p. 5-6.

La problématique du contrôle civil dans un système non démocratique

L'accent mis sur la professionnalisation de l'institution militaire présente certaines limites dans les relations civilo-militaires chinoises. Les niveaux tactique et politique, la relation entre les choix organisationnels, les compétences militaires et la stabilité politique interne ont des effets militaires sur l'issue de la guerre. Les militaires ont de meilleures chances de réussir au combat, lorsqu'ils adoptent les bonnes pratiques organisationnelles (promotion au mérite, commandement décentralisé, communication ouverte, entraînement réel et régulier). Bien que le « système moderne » d'efficacité tactique soit optimal pour réussir dans la guerre, de nombreux pays ne l'adoptent pas, car l'équilibre entre menaces internes et externes détermine si le régime permet à son armée d'adopter ces caractéristiques organisationnelles. Souvent par peur d'un coup d'État, les dirigeants autoritaires compromettent la compétence du leadership des officiers, en promouvant la fidélité au régime et en limitant la capacité des officiers à faire preuve d'initiatives ou à optimiser l'entraînement de leurs forces au combat (4).

La question du contrôle civil sur l'armée est fondamentale dans le contexte de la politique étrangère chinoise et mérite une attention particulière, étant donné l'importance de l'armée pour la survie du système de parti léniniste. Apparemment, dans les États socialistes, avec des armées de partis et non nationales, les relations civilo-militaires ne constituent pas le sujet d'étude le plus approprié, à l'inverse des relations partis-armées.

L'APL est toujours la branche armée du PCC, plutôt qu'une armée nationale. En supposant toutefois qu'un parti communiste engagé dans la révolution socialiste ne pouvait pas tolérer l'autonomie limitée requise d'une armée professionnalisée, les analystes ont du mal à expliquer l'anomalie apparente de l'APL post-Mao Tsé Toung. Le PCC s'est abstenu de se comporter comme un régime léniniste classique. Sa rupture sous Deng Xiaoping avec la poli- tique révolutionnaire a abouti à l'adoption d'un nouveau paradigme selon lequel l'APL a évolué vers une « armée de parti avec des caractéristiques professionnelles ».

Depuis le milieu des années 1990, les analystes constatent une autonomie militaire croissante par rapport au parti, ainsi que des signes d'un contrôle accru du gouvernement sur les forces armées – une évolution linéaire de la symbiose au contrôle à une autonomie limitée. La « nouvelle base » de l'interaction civilo- militaire est celle dans laquelle les civils « accordent aux généraux l'autonomie administrative et opérationnelle qui leur est due dans la gestion de leurs affaires de guerre, en échange de leur non-intervention dans les affaires civiles ». On parle d'un « contrôle objectif conditionnel » selon lequel le PCC tente de trouver un équilibre subtil entre deux impératifs concurrents et de « concilier deux exigences contradictoires » pour l'armée.

Celle-ci doit être « suffisamment politiques » pour soutenir la direction centrale mais « pas ouvertement politique », c'est-à-dire qu'elle ne doit pas intervenir dans la politique intérieure. Simultanément, les dirigeants centraux encouragent le professionnalisme militaire comme « un outil efficace pour détourner les généraux de poursuites politiques indésirables » (5).

(4) TALMADGE Caitlin, The Dictator's Army, Cornell University Press, 2015, 320 pages.
(5) JI You, China's Military Transformation, Polity Press, Cambridge, 2015, 256 pages, p. 4, 8 et 39.

L'APL jouit d'une autonomie professionnelle dans certains domaines, mais est soumise à des mécanismes de contrôle profonds et étendus. Le contrôle poli- tique direct et l'autonomie professionnelle varient, à la fois entre les niveaux hiérarchiques et les domaines d'intervention. Le parti peut accorder une autonomie substantielle dans la gestion des affaires militaires aux officiers supérieurs, qui auront la tâche d'ajuster ou d'initier un changement dans la stratégie militaire en réponse à l'environnement de sécurité changeant. Puisque les officiers supé- rieurs sont membres du PCC, celui-ci peut déléguer la responsabilité des affaires militaires sans craindre un coup d'État, ni que l'armée poursuive une stratégie incompatible avec les objectifs politiques du Parti. Une telle délégation n'est possible que lorsque la direction politique est unie sur les politiques fondamentales du parti et la structure de l'autorité au sein du parti (6).

La « longue marche » : le mythe fondateur

Chaque nation a son mythe fondateur, et pour la Chine moderne, c'est la longue marche, qui a établi Mao Tsé Toung comme le chef absolu du PCC et inspiré d'autres à suivre le chemin de la révolution. Bien que la longue marche soit un désastre sur le plan militaire pour les communistes chinois, de ses cendres est né un triomphe politique qui a finalement conduit à la fondation de la Chine moderne. Mao pensait que la violence et le soutien des masses étaient nécessaires à la réalisation d'un ordre communiste, et l'un des défis les plus critiques auxquels il était confronté fut l'impératif d'établir un soutien militaire à la révolution tout en empêchant simultanément l'armée de devenir trop puissante.

La Chine repose sur l'idée d'un lien étroit, voire symbiotique, entre la direction politique et une armée politisée. Tout en soutenant que le pouvoir politique ne peut pas être atteint sans le recours à la force – « le pouvoir politique naît du canon d'une arme à feu » – Mao croyait aussi que le parti devait garder le contrôle politique ultime pour que la paix et la prospérité soient atteintes – « le parti doit commander aux fusils ».

L'imbrication des structures partisanes et militaires et la politisation de la bureaucratie rendent les approches institutionnelles inadaptées. L'APL trouve ses racines dans le soulèvement de Nanchang en 1927 des communistes contre les nationalistes. Initialement appelée l'Armée rouge, seule une fraction a survécu à la longue marche. L'APL est restée une « armée du parti » et le « leadership absolu » du PCC sur l'APL a été officialisé en décembre 1929, lors de la « Conférence Gutian », durant laquelle Mao a clarifié le rôle de l'armée : « servir principalement les fins politiques ».

Pour Lénine et Mao, l'armée n'a pas de missions en dehors de celles du Parti. C'est durant cette réunion qu'a été formalisé le principe du « Parti commande aux fusils » et proclamé que le PCC est le chef absolu de l'Armée rouge, car celle-ci n'est pas n'importe quelle institution de guerre, mais une institution qui a pour mission politique d'apporter la révolution communiste à l'ensemble de la Chine. Gardant cet objectif à l'esprit, la résolution de Gutian a appelé à un endoc- trinement intensifié des troupes afin de garantir de fortes convictions politiques. Ce contexte a de profondes implications pour la compréhension des relations civilo-militaires depuis l'arrivée du PCC au pouvoir.

(6) FRAVEL Taylor, Active Defense, Princeton University Press, 2019, 396 pages, p. 19.

Fait intéressant, 85 ans plus tard, le 30 octobre 2014, Xi Jinping a réitéré le même message dans son discours à la Conférence sur le travail politique au sein de l'armée à Gutian. Pour lui, le renforcement du contrôle du Parti sur l'APL est aussi important que l'amélioration de la capacité de combat de l'APL. Le rapport au XVIIIe Congrès du Parti a souligné l'importance de renforcer le travail du Parti au sein de l'APL. Il a chargé celle-ci de mettre en œuvre un programme d'éducation politique axé sur la transmission du
« gène rouge ». En juin 2018, la CMC a publié la « Guideline on Implementing the Program of Passing on Red Gene » affirmant que le programme d'éducation devrait se concentrer sur « la construction de la loyauté absolue en ce qui concerne la sauvegarde du noyau du parti et l'obéissance aux ordres du parti » (7).

De l'armée du parti à l'autonomie limitée

Quoique lentement, l'APL a régulièrement progressé depuis sa création. Au fil du temps, trois écoles ont émergé dans les études stratégiques : symbiose, professionnalisme et contrôle du parti. Ces catégories d'analyses, complémentaires, ne s'excluent pas mutuellement. Le professionnalisme est un processus continu et l'APL a continué à se moderniser dans plusieurs dimensions. S'il y a eu des tensions, c'est entre le contrôle du parti et une autonomie militaire limitée. Alors que la norme d'une relation symbiotique s'est maintenue au fil des ans, à différentes périodes au cours des 70 dernières années (notamment 1959-1962, 1971- 1982 et 1989-1992), le PCC a déployé des efforts supplémentaires pour exercer un contrôle sur les forces armées, tandis qu'à d'autres moments, l'armée a cherché à accroître son autonomie par rapport au PCC. À plusieurs reprises, l'armée a tenté d'exercer son rôle dans les affaires de haut niveau du parti (notamment en 1967, en 1976, en 1989 et dans une certaine mesure en 1996), mais souvent en raison d'une partie des élites « tirant » les militaires en politique durant les périodes de troubles sociaux et de faiblesse du parti (8).

Dans d'autres périodes (1954-1959, 1974-1975, 1982-1989), l'APL a voulu accroître son autonomie par rapport au parti, mais il s'agissait d'une autonomie limitée. Comme une « armée de parti avec des caractéristiques professionnelles », l'APL n'a jamais cherché à se séparer pleinement du PCC (ou vice-versa). Elle a simplement désiré une plus grande autonomie dans les affaires qu'elle considère comme relevant de son domaine institutionnel – formation, doctrine, structure des forces, nominations du personnel, éducation militaire et protection de la sécurité nationale. Pendant ce temps, les tendances professionnelles ont plus ou moins été persistantes au fil du temps. Ainsi, les relations de l'armée avec l'État-parti ont évolué et ont été fluctuantes. Ce phénomène était corrélé en fonction de la force ou de la faiblesse du parti-État. En d'autres termes, pendant les périodes où le parti-État était fort et la société stable, l'armée avait tendance à agir comme un acteur bureaucratique. Lorsque l'État-parti était affaibli, l'armée avait tendance à agir, soit comme arbitre politique entre factions concurrentes, soit à soutenir une faction contre une autre, ou encore à intervenir plus largement pour stabiliser la société (9).

(7) JIAN Zhang, « Toward A "World Class" Military », in GOLLEY Jane et al. (dir.), China Story Yearbook 2019, ANU Press, 2019, p. 228.
(8) SHAMBAUGH David, *Modernizing China's Military*, University of California Press, 2002, 402 pages, p. 17-18.
9) SHAMBAUGH David, LILLEY James (dir.), China's Military Faces the Future, Routledge, 1999, 384 pages, p. 32.

Le 24 novembre 2015, lors d'une conférence sur la réforme militaire de la CMC, Xi Jinping a annoncé le programme de réforme le plus radical et le plus complet de l'APL depuis 1949. Dire que l'APL a subi une profonde transformation est un euphémisme et son ascension en 2012 au poste de secrétaire général du PCC est un point critique pour l'« intégration civilo-militaire » en Chine. En proposant, en octobre 2013, le « striving for achievement » comme nouveau principe de base de la diplomatie chinoise, la politique étrangère chinoise a pris une nouvelle direction qui éclipse la posture de « garder profil bas ». Sous sa direction, l'APL a accéléré la marche vers la modernisation qui a commencé en 1978 sous Deng Xiaoping. La réforme qu'il a initiée, vaste et profonde, affecte la politique intérieure et les bases du système politique chinois. Son ampleur ne peut être comparée qu'à l'échelle des mesures anticorruption prises dans toute la Chine.

En janvier 2016, la CMC a publié la « Ligne directrice sur l'approfondis- sement de la réforme de la défense nationale et de l'armée » visant à éliminer les « obstacles institutionnels, les contradictions structurelles et les problèmes politiques » qui avaient entravé le développement de la défense nationale et de la puissance militaire de la Chine. Au cœur de la réforme se trouve la modernisation de la structure organisationnelle de l'APL pour « libérer davantage son efficacité au combat » (10). Xi Jinping a demandé à l'APL de mener davantage d'exercices de combat et de donner la priorité à la construction de capacités militaires d'un « nouveau type ». Selon lui, les « unités de l'APL doivent se préparer au combat et étudier les guerres. Elles devraient se concentrer sur l'amélioration de leurs capacités d'opérations interarmées et de leur niveau de technologie » (11).

Lors du XIXe Congrès du PCC, Xi Jinping a réussi à utiliser le pouvoir de sa campagne anti-corruption pour faire adopter de grands changements dans la composition et la structure du CMC, qui ont brisé un obstacle bureaucratique clé à la rationalisation du commandement et du contrôle, et ont contribué à assurer la loyauté des hauts responsables militaires envers le Président.

En modifiant la composition et en réduisant la taille du CMC, Xi Jinping a pu consolider le contrôle politique sur la plus haute instance militaire. Le nombre de membres du CMC fut réduit de 11 à 7 sièges, et les chefs des services de l'APL ont été retirés du plus haut organe décisionnel militaire. Xi a procédé au recalibrage des rôles, missions et structures de l'APL ainsi qu'au rééquilibrage du trio : Parti-État-Armée.

La modernisation militaire sous Xi Jinping

Les réponses de Pékin aux défis de sécurité ont entraîné une série de réformes qui ont produit un nouveau paradigme de défense. Depuis 1949, elle a eu neuf stratégies militaires. Celles adoptées en 1956, 1980 et 1993 ont constitué des changements majeurs En modifiant la composition et en réduisant la taille du CMC, Xi Jinping a pu consolider le contrôle politique sur la plus haute instance militaire.

(10) JIAN Zhang, op. cit., p. 222.
(11) LEI Zhao, « Xi Orders New PLA Units to be Combat Ready », China Daily, 19 avril 2017 (www.chinadailyasia.com/).

Le nombre de membres du CMC fut réduit de 11 à 7 sièges, et les chefs des services de l'APL ont été retirés du plus haut organe décisionnel militaire. Xi a procédé au recalibrage des rôles, missions et structures de l'APL ainsi qu'au rééquilibrage du trio : Parti-État-Armée.

. Les lignes directrices décrivaient une nouvelle vision de la guerre qui nécessitait de transformer l'approche de l'APL en matière de doctrine opérationnelle, de structure de force, de technologie et d'entraînement. Les six autres stratégies (1960, 1964, 1977, 1988, 2004 et 2014) reflétaient des ajustements et des améliorations des orientations existantes (12). Parmi les développements clés dans les efforts de restructuration de 2018 figurent la refonte majeure de la structure de commandement conjoint de l'APL et la publication de nouvelles lignes direc- trices de la formation militaire se focalisant sur les opérations conjointes.

Ces développements font suite aux changements structurels à partir de 2016 dans les organes de direction de l'APL, les services de combat et les théâtres d'opérations. Les efforts de réforme de la deuxième phase se sont concentrés sur la formation des soldats pour opérer au sein de la nouvelle structure de commandement interarmées de l'APL. La « ligne directrice sur l'approfondissement de la réforme de la défense nationale et de l'armée » de janvier 2016 couvrait presque tous les aspects de l'APL : l'échelle, la structure et la composition des forces, le système de commandement militaire, la structure de commandement des opérations inter- armées, les formation, éducation et recrutement, l'intégration de la recherche et de développement (R&D) et de l'industrie de défense civile/militaire, la restruc- turation de la police armée du peuple, et le système juridique militaire (13).

Ces efforts peuvent être intégrées dans trois cercles : commandement des opérations inter- armées, les formation, éducation et recrutement, l'intégration de la recherche et de développement (R&D) et de l'industrie de défense civile/militaire, la restruc- turation de la police armée du peuple, et le système juridique militaire (13). Ces efforts peuvent être intégrées dans trois cercles :

- Développement, acquisition et mise en service de nouveaux systèmes d'armes, de technologies et de capacités de combat.

- Un éventail de réformes institutionnelles et systémiques, y compris des changements organisationnels et dans la culture bureaucratique de l'APL, visant à optimiser la force.

- Le développement de nouvelles doctrines de combat pour l'utilisation de ces nouvelles capacités.

Cette réorganisation souligne l'engagement du PCC à établir un système militaire moderne aux « caractéristiques chinoises » en vertu duquel l'État peut augmenter ses mécanismes de contrôle et ses lignes d'autorité sur l'APL, tandis que le PCC se retire dans une position plus élevée. En 2018, l'APL disposait d'un nouveau système de commandement et de contrôle parmi lequel la CMC en charge des affaires militaires globales, les commandements de théâtre en charge des opérations interarmées en temps de guerre et les services en charge du développement des forces. En termes de relations Parti-État-Armée, le PCC énonce la direction politique plus large, tandis que l'armée formule concrètement la ligne stratégique et met en œuvre des politiques spécifiques.

(12) FRAVEL Taylor, « Shifts in Warfare and Party Unity », International Security, 42, n° 3, 2018, p. 37-83.
(13) JIAN Zhang, *op.cit.*, p. 222-223.

CRSI CENTRE DE RÉFLEXION SUR LA SÉCURITÉ INTÉRIEURE
Fondée en 1939

Le CMC est désormais responsable de la formulation de la politique, du contrôle de tous les moyens militaires et de la direction supérieure de la guerre. Dans la nouvelle structure de commandement, le Président exerce un contrôle opérationnel direct sur l'APL.

Changement militaire et unité du parti

Le retrait des commandants des services des membres du CMC affaiblit les services par rapport à la CMC, bien que la domination des forces terrestres et la culture organisationnelle axée sur les services au sein de l'APL compliquent la tâche de créer une force conjointe. En raison de l'énorme masse continentale de la Chine et malgré une diminution importante de ses effectifs, l'armée de terre reste le plus grand service de l'APL au moment où Pékin cherche à développer une force inté- grée dotée de capacités navales et aériennes de premier ordre. Ces changements éloignent l'APL de la mentalité de la « grande armée » héritée de l'ère maoïste. En 2018, pour la première fois, la part de l'armée dans l'APL est tombée en dessous de 50 %, tandis que celles de la marine, l'armée de l'air et la force de fusée ont augmenté. Cela reflète l'évolution de la perception chinoise de l'environnement de sécurité ; l'importance croissante des domaines maritime, spatial et cyber ; et la nécessité de défendre les intérêts croissants à l'étranger.

Le changement nécessite souvent une longue période de gestation avant de se concrétiser. Un exemple classique de ce paradoxe est la lente mécanisation du champ de bataille puisqu'il a fallu deux décennies à l'armée britannique pour mécaniser sa cavalerie. En effet, ce n'est qu'en 1941 que les chefs d'état-major successifs ont commencé à appliquer les leçons de 1916. « Au lieu de reconnaître le potentiel du char, ils ont tiré la conclusion que l'innovation et le progrès sont intrinsèquement dangereux et donc à éviter. (14) » Sans l'émergence d'une acceptation bureaucratique par les hauts responsables politiques et militaires, y compris un financement adéquat, il est difficile que les nouvelles façons de lutte se répandent et s'enracinent dans les institutions militaires. Dans le cas de la Chine, le pays a poursuivi des changements majeurs dans sa stratégie militaire lorsqu'un changement important dans la conduite de la guerre s'est produit dans le système international, mais seulement lorsque la direction du parti est unie.

Dans les changements majeurs de 1956, 1980 et 1993, la Chine a considé- rablement changé la façon dont elle employait son armée pour atteindre des objectifs militaires qui font progresser ses objectifs politiques. Les changements dans la conduite de la guerre et l'unité du parti étaient des facteurs déterminants dans ces trois changements de la stratégie militaire. La stratégie de 1956 a été adoptée durant une période d'unité au sein du PCC. Les officiers supérieurs, en particulier Su Yu et Peng Dehuai, ont commencé le changement de stratégie alors que l'APL absorbait les leçons de la Seconde Guerre mondiale, de la guerre de Corée et de la révolution nucléaire (15). La compréhension de l'APL de la guerre du milieu du XXe siècle – façonnée par ses observations du théâtre européen et ses expériences aux derniers stades de la guerre civile – signifiait que le modèle de guerre dominant pouvait être caractérisé comme une guerre basée sur l'attrition de grandes unités militaires, pour la plupart mécanisées.

(14) DIXON Norman F., On the Psychology of Military Incompetence, Basic Books, 1979, 528 pages, p. 111.
(15) FRAVEL Taylor, Active Defense, op. cit., p. 32.

La stratégie de 1980 a été adoptée après que Deng Xiaoping a consolidé sa position de chef suprême de la Chine et rétabli l'unité du parti à la suite des divisions de direction et du bouleversement général de la révolution culturelle. Les officiers supérieurs, en particulier Su Yu, Song Shi-Lun, Yang Dezhi et Zhang Zhen, ont initié et dirigé le changement de stratégie en réponse à leur évaluation de la menace soviétique, basée sur les opérations aériennes et blindées dans la guerre israélo-arabe de 1973. La stratégie de 1993 a été adoptée après que Deng a rétabli l'unité du parti à la suite de la division de la direction, pendant et après la violente répression des manifestations de 1989 sur la place Tian'anmen. Les officiers supérieurs, Liu Huaqing, Chi Haotian, Zhang Zhen et Zhang Wannian, notamment, ont initié le changement de stratégie après la démonstration de nouveaux types d'opérations militaires durant la guerre du Golfe (16).

Les dirigeants civils du PCC ont dominé le processus, et les changements ultérieurs de la doctrine militaire étaient basés sur les orientations stratégiques qui en résultaient. Seul le changement de 1964 ne peut pas être expliqué par ce schéma – le cas où Mao est intervenu dans les affaires militaires pour changer la stratégie militaire. Sinon, ce sont les officiers supérieurs qui ont initié tous les autres changements dans la stratégie militaire chinoise (17). Cela explique pourquoi la stra- tégie nucléaire de la Chine est restée constante au cours de la même période. Les dirigeants du PCC n'ont jamais délégué à des officiers supérieurs la responsabilité de la stratégie nucléaire. Parce que celle-ci est subordonnée à la politique nucléaire, c'est une question qui ne peut être tranchée que par les plus hauts niveaux du parti. ◆

Cet article est une republication et le CRSI remercie vivement M. Tewfik HAMEL, son auteur, et la Revue Défense Nationale, partenaire du CRSI, pour leurs autorisations.

(16) Ibidem., p. 270-271.
(17) Ibid., p. 107.

DOSSIER - Les services de renseignement militaires français : **la Direction du Renseignement et de la Sécurité de la Défense**

Lundi 17 janvier 2022. La liste, lue à haute voix, ne comprenait que des prénoms ou des pseudonymes. Les services secrets extérieurs français ont rendu hommage ce jour là, sous l'arc de Triomphe, à leurs agents morts en opération en présence du Premier ministre.

Entre secret et discrétion, les « services secrets ou spéciaux » ont toujours attiré, intrigué, et suscité de nombreuses interrogations, plus généralement les services de renseignements (dont certains, il est vrai, sont parfois plus discrets ou secrets que d'autres), mais au moment où les cybermenaces et surtout les cyberattaques explosent, au moment où l'ordre mondial, et particulièrement en Europe est bouleversé avec l'entrée en guerre de la Russie contre l'Ukraine, et l'avenir encore plus incertain, la France ne peut se prémunir, anticiper, comprendre et opérer sans ses services de renseignements.

Moins médiatiques et surtout moins connues du grand public, c'est une évidence, que leurs homologues du civil, les services de renseignement militaires n'en sont pas moins indispensables à notre sécurité et notre défense et leurs rôles et missions ne risquent pas de s'affaiblir, bien au contraire…

Le CRSI vous propose un tour d'horizon détaillé des trois directions principales des services de renseignement militaires (DRM, DGSE, DRSD), dans vos trois prochaines Lettre de la Sécurité Intérieure, dont celle-ci, par laquelle nous commençons, avec la Direction du Renseignement et de la Sécurité de la Défense (DRSD).



Fondement juridique et introduction

Le Code de la Défense (articles D.3126-5 à D.3126-9) indique que la Direction de la Protection et de la Sécurité de la Défense (DPSD), devenue par décret du 7 octobre 2016 Direction du Renseignement et de la Sécurité de la défense (DRSD) est le service de renseignement « dont dispose le ministre de la défense pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles ». Son organisation est fixée par arrêté du 30 mars 2016.

La DRSD, dont la devise est de « renseigner pour protéger », exerce une mission de contre-ingérence au profit du ministère de la défense et des entreprises de défense. En première ligne avec les autres services dans la lutte contre le terrorisme et les subversions violentes, la DRSD contribue à préserver les intérêts français, notamment en protégeant les sites sensibles de la défense et les forces françaises. À ce titre, sur les théâtres extérieurs où les armées sont engagées, elle a acquis une compétence reconnue en contribuant à la protection des soldats français.

Elle intervient aussi dans le domaine de la sécurité économique par des actions de sensibilisation et d'audit de sécurité au profit des entreprises de défense, intéressées par ses conseils pour préserver un secteur riche en emplois.

Pour faire face aux nouvelles menaces en matière de cyberdéfense, elle développe actuellement une capacité de lutte informatique défensive.

Toujours prompte à s'adapter aux menaces émergentes, la DRSD poursuit sa modernisation.
La DRSD est organisée autour d'une direction centrale implantée à Malakoff (92) et d'un maillage de 56 emprises réparties sur tout le territoire national (métropole et outre-mer) en corrélation avec les implantations militaires et les industries de défense. Elle est présente à l'étranger à titre permanent auprès des forces françaises stationnées en Afrique et au Moyen-Orient.

Active à la fois en milieu militaire et en milieu industriel, la DRSD offre toute la palette des métiers du renseignement, de la recherche à l'exploitation.Elle est dotée d'un corps spécifique d'inspecteurs de sécurité de défense et s'appuie par ailleurs sur un personnel très qualifié d'ingénieurs et de techniciens pour faire face aux menaces informatiques.

Le Service de renseignement du ministre des Armées

La DRSD est « le service dont dispose le ministre des Armées pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles », selon les termes de l'article D3126-5 du code de la Défense. Autrement dit, la DRSD a pour cœur de métier la contre-ingérence de la sphère de défense.
La devise de la DRSD est : renseigner pour protéger.

La DRSD est l'un des six services du premier cercle de la communauté du renseignement. Celui-ci est composé de la DGSE, de la DGSI, de la DRM, de la DNRED et de TRACFIN.

À ce titre, la DRSD est autorisée à mettre en œuvre toutes les techniques de renseignement régies par la loi renseignement de juillet 2015. La DRSD concourt directement à éclairer la prise de décision des grands donneurs d'ordres militaires et civils, ainsi que des autorités politiques.

Un périmètre d'action large et précis

La sphère de défense est la zone d'exclusivité de l'action du Service. La sphère défense comprend le personnel, les informations, le matériel et les installations sensibles sous l'autorité du ministre des Armées, ainsi que les entités en lien avec ceux-ci ou présentant un intérêt pour le ministère. Les unités militaires, les acteurs du secteur économique (entreprises, start-ups,…), les instituts de recherche, les associations et organisations présentant un intérêt pour la Défense, ou liés à elle, font partie de la zone d'exclusivité de la DRSD. La protection de ces éléments est vitale pour le pays.

La DRSD a pour mission de mettre en œuvre des mesures de contre-ingérence et des mesures de protection pour assurer la sécurité de cette sphère défense, qui concourt directement à la sécurité de la défense nationale (y compris la protection du patrimoine et du potentiel scientifique et technique national).

La DRSD est le service de renseignement du 1er cercle compétent sur la sphère de défense.

Un positionnement clé

Au sein de la communauté du renseignement
La DRSD siège avec les autres services de renseignement à la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT), autour du Président de la République.

Au niveau ministériel et interministériel
La DRSD est directement subordonnée au ministre des Armées. Elle entretient des relations avec les armées, les autres organismes du ministère des armées et des autres ministères.
Elle participe notamment aux groupes de travail interministériels du Secrétariat général de la défense et de la sécurité nationale (SGDSN). La DRSD est un acteur incontournable du renseignement et de la sécurité économique au sein de la sphère industrielle de Défense. Elle travaille en relation avec des services spécialisés tels que le service de l'information stratégique et de la sécurité économiques (SISSE). Dans le domaine cyber, la DRSD travaille en partenariat avec des acteurs institutionnels tels que l'ANSSI, le CALID, le COM CYBER,…

À l'international
La DRSD recueille, analyse et diffuse du renseignement de contre-ingérence permettant l'information des autorités du ministère sur les menaces potentielles susceptibles d'affecter les intérêts de la défense en France. Pour ce faire, elle dispose, sur tout le territoire national y compris l'outre-mer, d'un maillage dense, au plus près des forces et des entreprises liées à la défense. A l'étranger, des postes permanents ou des détachements de contre-ingérence en OPEX permettent de remplir la mission de protection des forces. Enfin, la DRSD entretient des relations de coopération étroites avec nombre de ses homologues étrangers.

Renseigner pour protéger : la contre-ingérence défense

La DRSD fait partie des six services de renseignement français du premier cercle. A ce titre, elle dispose de toutes les techniques de renseignement et fait face, en se modernisant, à une évolution permanente de la menace. La DRSD agit dans un cadre particulier : la contre-ingérence. Une ingérence est un acte hostile visant à porter atteinte, autrement que par la confrontation militaire directe, aux intérêts fondamentaux de la Nation ainsi qu'à la défense nationale et au secret de la défense.

La contre-ingérence vise à déceler les intentions adverses en identifiant et en neutralisant toute menace pouvant conduire à des actes hostiles de la part d'organisations, de groupes ou d'individus isolés. Dans ce cadre, la DRSD a pour mission de renseigner sur les vulnérabilités et les menaces internes et externes pesant sur la sphère défense (personnel, matériel, informations et emprises) et de contribuer aux mesures de protection et d'entrave.

Cette mission se décline en deux domaines :

- la contre-ingérence des forces ;
- la contre-ingérence économique ;

La cyber défense est intégrée de manière transverse aux deux domaines.

Les menaces pesant sur la Défense sont analysées sous l'angle du TESSCo : terrorisme, espionnage, sabotage, subversion, crime organisé. Les menaces cyber sont également prises en compte. Dans le périmètre de « la sphère Défense », la DRSD agit donc sur un spectre de missions comparable à celui des autres services de renseignement.

La contre-ingérence des forces

Au sein du périmètre Défense, sur le territoire national comme à l'étranger, la contre-ingérence des forces est chargée d'identifier les menaces liées au terrorisme, à l'espionnage, à la subversion et à la criminalité organisée à l'encontre du ministère.
En amont, le Service évalue les vulnérabilités des dispositifs déployés et des unités considérées, et conseille le commandement sur les mesures de prévention à mettre en œuvre pour les réduire.
La contre-ingérence des forces s'intéresse en premier lieu aux ressortissants de la Défense (militaires et civils), à leur environnement et aux menaces susceptibles de peser à leur encontre. Elle contribue à leur sécurité et aux mesures d'entrave nécessaires à leur protection, par l'orientation des capteurs (humains et/ou techniques), l'exploitation et l'analyse des éléments recueillis, et l'information du commandement et de la communauté du renseignement. Elle cherche également à déceler et à entraver toute menace externe susceptible de porter atteinte à l'Institution.

Elle contribue ainsi, au titre de son périmètre fonctionnel, à l'appréciation de situation autonome des autorités politiques et militaires, et travaille au quotidien avec les services partenaires français et étrangers.

La contre-ingérence économique

En matière de contre-ingérence économique, la DRSD s'emploie au quotidien à lutter contre de multiples menaces. La guerre économique est une réalité : prises de contrôle par des actifs étrangers, captations de savoir-faire, vols d'informations et de supports classifiés, cyber-attaques, intrusions consenties ou non, sabotages de matériels, d'installations, ingénierie sociale, atteintes à la réputation des entreprises, détournements de biens à double usage civil/militaire par des acteurs de la prolifération, escroqueries, conflits d'intérêts, infractions à la réglementation et activités illicites liées au commerce des armements sont autant d'exemples de menaces pouvant peser sur l'industrie de Défense.

S'inscrivant dans un cadre interministériel et interservices, le périmètre d'action de la DRSD s'applique aux industries et aux établissements de recherche en lien avec la Défense. La DRSD accompagne plus de 4 000 entités.

La mission du Service consiste à déceler et à neutraliser toute menace contre les intérêts nationaux, la souveraineté nationale et le potentiel scientifique et technique de la Nation. Ces menaces résultent de l'activité, légale ou non, d'acteurs divers au profit d'intérêts extérieurs. Elles peuvent affecter le secret de la Défense nationale, le potentiel scientifique et technique de la Nation, les intérêts ou le patrimoine matériel et immatériel des entreprises ou les organismes en lien avec la Défense. Il s'agit donc de défendre la technologie des entreprises françaises et de préserver leur compétitivité dans un univers économique de plus en plus concurrentiel. In fine, par son action, la DRSD participe à la préservation de nos capacités opérationnelles.

La contre-ingérence cyber

Domaine transverse, le cyberespace constitue un milieu stratégique dans lequel la DRSD mène des actions de contre-ingérence. Dans ce secteur, la DRSD identifie les vulnérabilités et menaces susceptibles de porter atteinte aux personnes, matériels et informations sensibles du ministère.

Elle privilégie l'anticipation et s'appuie sur ses moyens propres. Elle travaille en partenariat avec des acteurs institutionnels tels que l'ANSSI, le CALID, le COM CYBER. Par ailleurs, elle contribue à la lutte informatique en participant à la protection des systèmes d'information du ministère et de l'industrie de défense.

Ces missions peuvent avoir un caractère :

- Préventif : sensibilisations, inspections, alertes ;

- Curatif : analyse des cyber-attaques, soutien à la remédiation et encadrement de la reprise d'activité.

Protéger pour renseigner : la protection du secret

Conformément au Code de la Défense, « *la Direction du Renseignement et de la Sécurité de la Défense est le service de renseignement dont dispose le ministre des armées pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles* ». De facto, la DRSD a pour mission de veiller à l'intégrité du secret de la défense nationale. Celui-ci se présente sous la forme d'informations ou de supports classifiées (ISC). Ces ISC sont détenus tant par des entités militaires que civiles. L'instruction générale interministérielle n° 1300 (IGI n° 1300) sur la protection du secret de la défense nationale définit les règles de gestion et d'utilisation des informations et supports classifiés.

Dans le cadre de cette mission essentielle pour garantir la souveraineté de la France, la DRSD conseille, guide et contrôle les entités et les personnes qui sont susceptibles de détenir ou d'accéder à une information ou à un support classifié.

Elle regarde particulièrement : la conformité réglementaire des dispositions permettant d'assurer la protection physique et la cyberprotection des ISC, le risque lié à la menace interne.

Et l'avenir ?

C'est d'abord, de nouveaux locaux permettant de répondre aux évolutions de notre environnement de sécurité et de défense avec le lancement de la construction d'un nouveau bâtiment pour la DRSD au Fort de Vanves, à Malakoff (92).

82 millions d'euros. C'est le coût du nouveau bâtiment qui accueillera le siège de la DRSD. La première pierre a été posée jeudi 6 janvier 2022 par la ministre des Armées, Florence PARLY, au Fort de Vanves, à Malakoff.

La construction du nouvel édifice au sein du Fort de Vanves s'inscrit dans une volonté de transformation, face à des menaces grandissantes qui « pèsent sur la sécurité nationale » a déclaré Florence PARLY, ministre des Armées, venue déposer la première pierre.
Selon la DRSD, il permettra aux équipes de travailler dans des conditions optimales et sera doté de fonctionnalités pour le moment manquantes, à savoir un amphithéâtre, des ateliers et des laboratoires modernes.

Le bâtiment de 646 places a également été pensé pour pouvoir accueillir de nouveaux agents, comme le prévoit la loi de programmation militaire.

Avec plus de 350 000 enquêtes administratives réalisées en 2021 (soit un millier par jour), la Direction du Renseignement et de la Sécurité de la Défense, dont les missions portent sur le contre-espionnage et la contre-ingérence, est sans conteste le premier service enquêteur de France.

Pour faire face à cette activité qui ne risque pas de s'amoindrir dans les années à venir au regard du contexte international et de l'extension des champs de conflictualité, la DRSD a engagé une transformation de son organisation, avec pas moins d'une trentaine de chantiers « innovants » en cours. L'objectif est de gagner en cohérence, de simplifier ses processus « métiers », d'améliorer ses capacités de recueil et d'analyse du renseignement et de mettre l'accent sur la cybersécurité et les nouvelles technologies.

Parmi ces chantiers, en collaboration avec Airbus Defence & Space, la DRSD développe une « nouvelle base de souveraineté » qui, appelée SIRCID, vise à lui permettre de stocker et d'exploiter les renseignements à partir d'une solution logicielle 100% française. Devant entrer en service en 2022, son coût est de 18,69 millions d'euros. Selon son directeur, le général Éric BUCQUET, il s'agit de la « première solution souveraine en matière de système d'information de contre-ingérence d'un service de renseignement ».

Par ailleurs, en juillet 2021, son logiciel SOPHIA (Synergie pour l'Optimisation des Procédures d'Habilitation des Industries et de l'Administration) a été mis à jour (sous forme électronique) pour prendre en compte les nouvelles dispositions de l'Instruction générale interministérielle (IGI) 1300 sur les niveaux de classification, traiter les obsolescences et ajouter de nouvelles fonctionnalités. D'autres outils pour renforcer la fiabilité des avis de sécurité, notamment en automatisant les recherches d'informations sur les candidats, sont en cours de développement.

Cette transformation s'accompagnant d'une nouvelle hausse de son effectif (plus de 200 agents sur la période 2019-2025), il est apparu nécessaire de doter la direction centrale de la DRSD d'un nouveau siège. D'où la hausse significative (+92%) de ses crédits de paiement, ceux-ci passant de 18,4 à 35,4 millions d'euros en 2022, une première pour la DRSD. Au total, 82 millions d'euros seront investis dans ce nouveau bâtiment, dont la première pierre a été posée par Florence PARLY, la ministre des Armées, ce 6 janvier 2022.

« *Dès 2024, il concentrera les services experts et opérationnels dans un même lieu. Tout a été pensé pour que l'information circule de la manière la plus fluide possible entre les services. Il s'agit donc d'un véritable bâtiment opérationnel, doté de toutes les fonctionnalités qu'est en droit d'exiger une direction centrale d'un service de renseignement de premier rang* », a rappelé la ministre lors de son allocution prononcée devant le personnel de la DRSD, au Fort de Vanves.

Dans un avis budgétaire publiée par l'Assemblée nationale, l'automne dernier, il est précisé que ce nouveau siège permettra de « regrouper les activités « cœur de métiers » de la DRSD au sein d'un bâtiment unique accueillant 646 places en anticipant les évolutions d'effectifs de chacune des divisions », de « proposer des espaces flexibles s'adaptant à l'évolution des organisations, des modes de travail et des métiers, tout en répondant aux besoins de proximités fonctionnelles des divisions les unes par rapport aux autres et au sein des divisions », de « tenir compte des exigences techniques et réglementaires pour tous les espaces, et en particulier pour les ateliers », et d'installer de « nouvelles capacités » et « d'appliquer les réglementations liées à la sûreté à l'échelle du bâtiment et aux locaux ».

Quoi qu'il en soit, Mme PARLY a insisté sur la « croissance importante des menaces d'ingérences étrangères » pour mieux souligner la mission de la la DRSD. « Nous voyons une résurgence des actions décomplexées de nos compétiteurs. Face à ces tentatives d'espionnage, d'entrave et de discrédit de notre action, vous agissez : vous détectez, vous investiguez, vous identifiez et si cela s'avère nécessaire, vous vous assurez de contrecarrer ces actions malveillantes », a-t-elle dit.

Aussi, a poursuivi la ministre, « je compte sur vous pour être particulièrement vigilants en matière de contre-ingérence économique » car « c'est un champ qui est de plus en plus investi, nous en avons encore eu la preuve assez récemment ». Était-ce une allusion au contrat des sous-marins australiens, ravi au nez et à la barbe de la France par les États-Unis et le Royaume-Uni ?

En tout cas, a fait valoir Mme PARLY, la « guerre économique, à la croisée des rapports de force géopolitiques et des négociations commerciales, est un champ de conflictualité que nous ne devons pas sous-estimer : il a la particularité de nier les alliances au profit des intérêts ». Et de conclure : « Dans le champ de la compétition économique, il n'y a qu'une seule règle, celle du « chacun pour soi »'. Et le « chacun pour soi », cela signifie pouvoir compter sur vous, sur votre excellence, la pertinence de vos capteurs et votre capacité de discernement ».

Pour aller plus loin :

⇨Présentation de la DRSD en vidéo :



Si vous n'arrivez pas à visualiser correctement la vidéo, cliquez ici

⇨ Secret de la défense nationale : une formation en ligne (MOOC) pour accompagner la nouvelle réglementation

⇨ Déclaration de Mme Florence PARLY, ministre des armées, sur le renseignement militaire, à Malakoff le 6 janvier 2022 (texte intégral)



⇨ Le site Internet de la DRSD

La communauté française du RENSEIGNEMENT

Interview exclusive de Richard LIZUREY, Ancien directeur général de la gendarmerie nationale Prédécesseur du général Christian RODRIGUEZ

En exclusivité, le CRSI vous propose l'interview du général d'armée, Richard LIZUREY, ancien directeur général de la gendarmerie nationale (DGGN) de 2016 à 2019. Il nous livre sa vision personnelle de l'institution, et notamment de ses évolutions, de ses forces, mais encore de sa culture. Enfin, il nous donne son avis sur les évolutions récentes (guerre en Ukraine) et les menaces qui nous entourent.

Propos recueillis par Guillaume LEFEVRE, Secrétaire général du CRSI

CRSI : *Mon général, vous avez dirigé la gendarmerie nationale pendant un peu plus de 3 ans, du 1er septembre 2016 au 31 octobre 2019. Cela parait peu à l'échelle d'une vie, mais du fait des évolutions rapides de la société française, spécifiquement sur les questions de sécurité intérieure, c'est énorme. Que retenez-vous de ces années à la tête de la gendarmerie nationale et de cette période ainsi traversée ?*

Général d'armée Richard LIZUREY :

Lorsqu'on est au service d'une institution comme la Gendarmerie Nationale, on est d'abord au service de tous nos concitoyens, à qui nous devons un service public de sécurité de qualité. On est également au service des personnels de l'institution, car ce sont ces personnels qui en font l'efficacité et l'âme. Le directeur général n'est donc qu'un serviteur et ce qui m'a toujours inspiré c'est l'humilité et le respect devant l'engagement exceptionnel de tous les personnels de la gendarmerie.

J'ai eu une immense chance de pouvoir vivre les 10 dernières années de service dans des postes à responsabilités : en qualité de conseiller gendarmerie de deux ministres de l'intérieur, à partir de 2009 après l'intégration de la GN au ministère de l'intérieur, puis comme major général pendant plus de 4 ans et enfin 3 ans comme directeur général. Pendant toutes ces années, j'ai pu apprécier l'exceptionnelle capacité d'adaptation des personnels de la maison, leur dévouement au service des autres, ainsi que l'image positive qu'inspire la gendarmerie dans la société.

Les dernières années ont été marquées par des événements majeurs qui ont mis les institutions à l'épreuve, mais je suis, comme ancien DG, comme élu local aujourd'hui et comme citoyen, reconnaissant de l'engagement de celles et ceux qui ne comptent pas leur peine, qui vont jusqu'au bout de leur engagement au service de notre sécurité.

Cet engagement est d'autant plus important que notre société a évolué vers une confrontation des individualismes, une montée des violences et une remise en cause de plus en plus systématique de l'autorité. Ceci résulte d'une dégradation du contrat social et d'une politisation excessive des sujets de sécurité. Lorsque l'on voit des responsables politiques qui encouragent à la désobéissance – fût-elle civile –, en tête de manifestations à caractère séparatistes ou excuser les troubles à l'ordre public, il n'est pas besoin de chercher trop loin les responsabilités dans le délitement du contrat social.

Face à cette situation, force est de reconnaître que les forces de sécurité intérieure, police nationale, polices municipales et gendarmerie nationale sont au rendez-vous, faisant face avec courage, constance et abnégation aux défis sécuritaires. La gendarmerie nationale prend toute sa part dans ce combat pour la sécurité.

Au cours de plus de 42 années de service, j'ai toujours apprécié la qualité des personnels de la Gendarmerie, de tous statuts, qu'ils soient civils, militaires d'active ou de réserve. Je suis fier d'avoir pu contribuer, avec et grâce à tous ces personnels, à l'évolution du service public de sécurité.

Je suis reconnaissant envers tous les personnels de cette institution pour ce qu'ils ont apporté à nos concitoyens, pour ce qu'ils m'ont apporté aussi, car cette Force humaine faite de soldats de la loi est une maison remarquable et originale.

J'ai une totale confiance en la capacité de cette maison à faire face, en témoigne l'engagement exceptionnel dans la séquence des GJ, dans tous les événements d'ampleur mais également dans les actions quotidiennes au contact de la population.

CRSI : *Pendant vos 3 années à la tête de la gendarmerie, comme depuis la prise de fonction (fin 2019) de votre successeur le général d'armée Christian Rodriguez [NDLR : qui fut auparavant major général de la gendarmerie nationale], soit pour maintenant 6 ans, la gendarmerie a également beaucoup évolué. Quelles sont selon vous les forces dont dispose la gendarmerie nationale pour évoluer et correspondre au mieux aux réalités à laquelle elle est confrontée ou engagée au quotidien aujourd'hui ?*

Général d'armée Richard LIZUREY :

Le première force de la GN ce sont ses personnels, exceptionnellement engagés et dévoués aux autres. Leur engagement quotidien et leur formation à la rusticité en font un atout important pour tenir le territoire, en métropole, outre-mer ou à l'étranger. Pendant toute ma carrière j'ai eu la chance de rencontrer des personnels de tous statuts qui n'étaient animés que par le sens de l'intérêt général et du service public.

Et je ne parle pas que des personnels de la gendarmerie départementale ou de la gendarmerie mobile, deux subdivisions d'arme qui sont en première ligne sur le terrain, je pense également à toutes les unités spécialisées, à tous les réservistes et tous les personnels administratifs civils et militaires. C'est la diversité des personnels et la force de leur engagement qui fait la force de la famille gendarmerie.

La très grande diversité des métiers et l'organisation de la GN qui repose sur l'action des cellules de base que sont les brigades territoriales permette une grande capacité d'adaptation. La déconcentration de l'action au plus près des besoins de nos concitoyens permet une agilité opérationnelle reposant sur l'esprit d'initiative. Car l'intelligence locale est une force exceptionnelle pour répondre à la diversité des situations. Imaginer tout pouvoir diriger du centre est une erreur, pire, une faute.

D'ailleurs, le maillage territorial et la présence dans la profondeur est un autre atout de la maison. Même le désert a besoin de gendarmes, car les zones reculées peuvent servir de zone de repli de délinquants et il est également indispensable de garantir à tous un même niveau de service public de sécurité.

Ce maillage territorial et le logement des gendarmes sur leur lieu de travail est le gage d'une proximité avec la population, socle de l'efficacité opérationnelle. Le gendarme vit avec et au plus près d'une population qu'il est chargé de protéger.

Un autre atout est la capacité collective à l'innovation. La modernisation de la GN repose certes sur des esprits brillants servant à la DGGN, mais elle s'appuie sur un socle exceptionnel de personnels qui, imprégnés de l'esprit de leur mission, cherchent à faire toujours mieux et participent à la démarche d'innovation. La GN est ainsi une institution qui exprime une polyvalence heureuse entre opérationnel et technologie : la captation sélective du progrès scientifique appuie la modernisation technologique qui se nourrit d'une démarche bottom up.

Ceci étant, nous ne sommes pas dans le meilleur des mondes et la GN court également un risque de découplage de la société par endroits lorsque le gendarme oublie son ADN de contact. Force est de reconnaître que la proximité et le contact, notions indispensables pour la qualité du service public, n'est pas une réalité universelle et qu'ici ou là des marges de progrès existent.

C'est également une force de la maison de disposer d'un contrôle social facilité par le logement en caserne. L'organisation et la discipline militaire permet également de recadrer les comportements inappropriés ou déviants.

CRSI : *La gendarmerie nationale est une vieille maison, une institution appréciée des Français, au-delà de son ancrage territorial et de son statut militaire, comment résumeriez-vous simplement la « culture » de la gendarmerie et l'image qu'elle en véhicule depuis maintenant des siècles (1791 : naissance officielle de la gendarmerie nationale) ?*

Général d'armée Richard LIZUREY :

Le modèle original de la GN en fait un ovni administratif qui est souvent interrogé par les responsables politiques, notamment ceux formés au management budgétaire plutôt qu'à celui de l'efficacité.

Souvent, le premier mot qui vient à l'esprit lorsque l'on parle de la culture de la GN est la « militarité ». Mais de quoi s'agit-il ? Pour certains, ce terme renvoie aux années d'avant 2009, lorsque la GN dépendait du ministre de le défense et ils peuvent encore exprimer une certaine nostalgie d'un « âge d'or » de la militarité qui ne correspond toutefois plus à la vision actuelle des personnels.

Pour d'autres, la militarité doit être vue comme un état d'esprit, un engagement et un dévouement total à la mission. En fait, je pense que la culture de la gendarmerie est celle du service et de la disponibilité, même si sur ce dernier point les aspirations individuelles tendent à remettre en cause un certain nombre de règles.

En effet, la gendarmerie n'échappe pas à l'évolution de la société et le risque est que les dispositions du texte relatif au temps de travail ne soient peut-être que le début d'une évolution de long terme conduisant à la banalisation du statut militaire.

La Gendarmerie Nationale est qualifiée de « Force humaine », de « maison », de « grande Famille ». ce ne sont pas que des concepts et cette culture du collectif fait partie de l'ADN de tous les personnels de la gendarmerie.

Ce qui caractérise cette institution est donc son collectif, qui fait sa force : lorsqu'un gendarme est touché, c'est toute la maison qui souffre, lorsqu'un de ses membres « dérape », c'est toute la maison qui est touchée.

La proximité a pu être perdue sur le chemin de la rationalisation, de la course aux indicateurs et aux chiffres. Il faut reconnaître que les années de RGPP ont notoirement éloigné les forces de sécurité de la population et ont dégradé la qualité de service. Mais le sens du contact reste dans le socle culturel des personnels.

Enfin, ce qui symbolise l'action de la GN est son humanité, l'application des lois devant être faite avec discernement. Les termes de « Force humaine » symbolisent cette culture faite d'engagement, de proximité, d'empathie et d'intelligence locale.

CRSI : *Création de la Brigade numérique, du Comcybergend, du Centre National des Opérations (CNO), renforcement du GIGN (notamment en régions), développement et montée en puissance de la réserve opérationnelle,… la gendarmerie nationale semble à la pointe de l'innovation, de la recherche et de sa propre transformation permanente : comment avez-vous piloté ces changements majeurs et quelles sont vos inspirations pour poursuivre un tel engagement ?*

Général d'armée Richard LIZUREY :

Tout d'abord il me paraît essentiel d'indiquer que la gendarmerie a, de tout temps, eu le souci de la modernisation : en témoigne notamment le développement de l'informatique au sein de l'institution à la fin du siècle précédent, qui a conduit à la mise en place d'un intranet national et le choix des logiciels libres, pour lesquels la gendarmerie a été précurseur.

La création, depuis maintenant plus de 15 ans, des ateliers de la performance (désormais « Ateliers de l'innovation ») et celle de la communauté e-care (précurseur d'autres communautés comme Solaris) ont permis de donner la parole aux personnels de terrain. Ces démarches bottom-up se sont poursuivies avec la « feuille de route » mise en place par Denis Favier et par la mise en place de Néogend dont l'évolution applicative se nourrit des propositions du terrain.
La conception et la mise en œuvre d'un plan stratégique de recherche et d'innovation en sécurité intérieure a permis, depuis 2017, de coordonner l'ensemble des acteurs de la gendarmerie sous la houlette d'un directeur et l'éclairage d'un conseil scientifique. Cette dynamique de modernisation se poursuit, appuyé par le recrutement de personnels scientifiques qui, grâce à leur double culture scientifique et opérationnelle, savent proposer et développer avec bonheur des outils opérationnels adaptés à la réalité du terrain.

Ceci étant, comme toute grande maison, le changement et la transformation n'est pas un long fleuve tranquille. Au même titre que l'équipe de France de football peut s'appuyer sur 67 millions de sélectionneurs, que le Président de la République peut s'appuyer sur 67 millions de médecins pour faire face à la crise COVID, le DGGN peut s'appuyer sur 130.000 DG d'active et de réserve, qui ont tous un avis sur la situation et sur les mesures à prendre…

Toute transformation doit donc s'appuyer sur une concertation préalable, une explication transparente et un accompagnement bienveillant pour une mise en œuvre agile et différenciée. Rester à l'écoute des évolutions dans tous les domaines technologiques, mais toujours les apprécier à l'aune des besoins qu'expriment nos concitoyens, tel est le socle de la transformation et de l'efficacité opérationnelle.

CRSI : *Parlons « opérationnel » si vous le voulez bien ? Lutte anti-terroriste et menace terroriste endogène, islamisme croissant, montée spectaculaire de la cybermenace, accroissement du séparatisme et des groupuscules « ultras », augmentation globale de la délinquance et des trafics, des violences conjugales (notamment faîtes aux femmes), accroissement sans commune mesure des agressions envers les élus comme des policiers et gendarmes,… la liste est évidemment non exhaustive, et l'approche des prochaines élections présidentielles risque d'accroitre encore les problématiques de sécurité publique : comment la gendarmerie réagit-elle face à ses nouveaux engagements opérationnels nécessaires ? Cela nécessite il un changement de doctrine d'emploi des forces ? Comment la gendarmerie arrive à répondre présent sur autant de théâtres d'opérations ? Quelles sont ses atouts d'un point de vue opérationnel ?*

Général d'armée Richard LIZUREY :

La Gendarmerie, tout comme la Police Nationale et les polices municipales, est en première ligne face aux menaces de toute nature. Et les menaces ne vont pas en diminuant.

Elle s'adapte aux menaces sécuritaires grâce à la modularité de son dispositif qui permet une montée en puissance sans solution de continuité de la première patrouille à toutes les structures nationales .

Ce n'est pas la doctrine d'engagement qu'il faut changer, mais les moyens qu'il faut continuer à moderniser et l'initiative qu'il faut développer. La sécurité publique est d'abord une exigence et une réalité locale, avant d'être une politique nationale.

La sécurité n'est pas une science exacte et ne doit pas être un objet de politique politicienne : une campagne électorale présente le risque de caricaturer ce sujet, chaque candidat expliquant qu'il ou elle a des solutions idéales, alors même qu'il est patent que les réponses sécuritaires supposent une approche globale, incluant le champ de la prévention et celui de la justice, indissociable de toute solution sécuritaire.

La très grande qualité d'engagement des personnels, leur capacité de rusticité et leur dévouement au service des autres sont les ingrédients indispensables à la qualité du service public de sécurité. Pour conserver l'âme de la maison, il faut que les personnels de tous statuts soient reconnus et valorisés.

Pour conserver une dynamique positive, il est nécessaire que le commandement soit agile, éclairé et bienveillant, ce qui ne va pas toujours de soi dans une institution à statut militaire :

- l'agilité est la capacité de faire prévaloir l'intelligence locale sur la vision normalisatrice nationale,
- le commandement éclairé prend en compte tous les paramètres de contextualisation et notamment les évolutions technologiques et sociétales,

- la bienveillance, qui n'est pas de la démagogie et n'exclut pas de la fermeté, est indispensable pour susciter et encourager les initiatives. Le droit à l'erreur est un élément essentiel dans ce domaine : il faut reconnaître à celles et ceux qui agissent le droit de se tromper et faire la chasse à celles et ceux qui se contentent d'observer sans rien faire, comme des blaireaux au fond de leur terrier…

Il me semble que la GN dispose donc de tous les ingrédients pour faire face aux défis sécuritaires, pour peu que l'on fasse confiance aux acteurs de terrain.

Parmi ces acteurs, je souhaiterais citer et témoigner ma reconnaissance aux réservistes de la Gendarmerie, qu'il s'agisse de la réserve citoyenne ou de la réserve opérationnelle. La réserve est un atout indispensable à l'efficacité opérationnelle et sans nos réservistes, il est certain que la qualité de service ne serait pas au même niveau. Il convient de poursuivre leur recrutement, leur formation et leur engagement par une politique volontariste et un budget adapté, ce qui n'a malheureusement pas toujours été le cas, notamment pendant les années de RGPP.

CRSI : *Projetons-nous ? La gendarmerie nationale, dans 10 ans, dans 50 ans, à titre personnel pour l'un et l'autre, comment la voyez-vous, comment l'envisageriez-vous, et même comment la souhaiteriez-vous ?*

Général d'armée Richard LIZUREY :

Au-delà de la vision des politiques, la gendarmerie évoluera en fonction de ce que voudront en faire ses personnels. En effet, le gendarme est le meilleur ami ou le meilleur adversaire de la gendarmerie.

A la lumière des dernières années, deux grandes évolutions peuvent être imaginées, chacune comportant naturellement des sous-scenarii :

1 - Un statu quo du dispositif actuel : probabilité faible, tant les événements et les changements politiques vont influencer les institutions. La porosité sociale dans les structures communes, la pression technocratique sur toutes les structures poursuivra une dynamique de rapprochement des forces de sécurité intérieures.

Dans cette perspective globale, il est possible d'imaginer des spécialisations de plus en plus marquées, qui ont d'ailleurs déjà commencées : le principe du « menant-concourant » ou du « chef de filât » permet de désigner une des forces – ou une direction générale - comme chef de file dans un domaine spécifique.

Tel est le cas de la DGSI, chef de file pour la lutte anti-terroriste. Mais ce chef de filât doit être correspondre à une vision partagée et un partenariat ouvert des différents acteurs et de ce point de vue force est de constater que les corporatismes ont encore « la peau dure ».

Souhaitons que la dynamique de rapprochement des forces et de synergies s'inspire à l'avenir davantage de l'intérêt général que des intérêts corporatistes.

2 - Une poursuite de la banalisation du statut militaire et sa disparition à la faveur de rapprochements successifs avec la PN et la fusion des FSI. Il s'agit évidemment d'une évolution qu'à titre personnel je ne souhaite pas, mais elle ne peut être exclue tant les politiques successives de mutualisations doctrinales et l'absence d'outil de prospective et de de vision à long terme au sein du ministère de l'intérieur mettent en place tous les ingrédients d'une intégration des différentes forces.

En tout état de cause, ces évolutions seront également influencées par l'évolution de la composante Police Municipale et sécurité privée. La montée en puissance de ces acteurs risque de faire « remonter » les FSI et donc la GN, vers les sujets du haut du spectre : cette évolution a déjà commencé, puisque l'État encourage la montée en puissance des PM qui sont de plus en plus vue et reconnue comme une force de proximité.

La GN a des atouts incontestables aujourd'hui, le principal étant sa proximité reconnue des citoyens. Je souhaite qu'elle poursuive son action de contact malgré les difficultés. La GN est une force de proximité et d'intervention : il ne faudrait pas qu'elle oublie le contact pour ne privilégier qu'une approche rationalisée de l'intervention car, dans ce cas, elle perdrait le soutien de la population qui trouvera naturellement dans les polices municipales les remplaçants.

La situation internationale actuelle démontre le besoin impératif pour nos démocraties de se préparer, non seulement sur le plan de la défense, mais également pour ce qui concerne la sécurité intérieure : les effets collatéraux du conflit en Ukraine peuvent susciter des troubles d'ordre public, des menaces cyber, voire une fracture sociétale en cas d'impact trop importants sur le quotidien de nos concitoyens. Que deviendra l'unité nationale sous la pression des événements ? Nul ne le sait aujourd'hui.

Après une période de doute qui a suscité les théories les plus contradictoires, nous sommes actuellement dans la phase de sidération qui inhibe également quelque peu la réflexion collective. La crainte évoquée d'un conflit avec une dimension nucléaire est évidemment d'un impact certain.

Cette phase de sidération va se terminer soit par la fin du conflit – non probable à ce stade – soit par la perception concrète de l'impact sur les citoyens. Nous pourrions assister à une fracture sociétale qui remplacerait la quasi-unanimité actuelle. L'unité nationale ne résistera pas à des conséquences individuelles fortes.

Ce conflit reste néanmoins une opportunité extraordinaire de faire évoluer les choses. Comme toujours, la crise conduit à franchir des étapes jugées auparavant infranchissables, telles que le changement de politique de défense de l'Allemagne et de l'Union européenne.

La gendarmerie, comme toutes les autres institutions, doit être prête à faire face à l'incertitude. Son organisation agile, reposant sur un socle territorial solide et une marge d'initiative des cadres de tous niveaux sera le déterminant de son efficacité.

Enfin, si l'on regarde encore plus loin comme le fait par exemple le rapport du GIEC de fin février 2022, le réchauffement climatique changera énormément de choses : migrations, crises de l'eau, crises sanitaires à répétition. La Gendarmerie devra savoir s'interfacer avec des institutions avec lesquelles il n'est pas forcément naturel de travailler actuellement, comme le MTES.



À propos de l'auteur de ce dossier :

Le CRSI remercie **le général Richard LIZUREY** (ci-contre) pour sa contribution.

Diplômé de l'École spéciale militaire de Saint-Cyr et de l'École des officiers de la Gendarmerie nationale de Melun, il débute sa carrière en 1981 à Berlin, comme lieutenant au commandement d'un peloton de l'escadron de sécurité chargé notamment des points de transit Ouest-Est.

Promu général de brigade en 2007, il est nommé commandant de la région de gendarmerie de Corse. De 2009 à 2012, il est affecté au cabinet du ministre de l'Intérieur. En juillet 2016, c'est en tant que général de corps d'armée qu'il est nommé directeur général de la Gendarmerie nationale. Le 19 juillet 2016, Richard Lizurey est nommé en conseil des ministres directeur général de la Gendarmerie nationale et élevé aux rang et appellation de général d'armée à compter du 1er septembre 2016 (le plus élevé dans la hiérarchie de l'armée française).

Son adieu aux armes a lieu le 15 octobre 2019, dans la cour d'honneur des Invalides.

En décembre 2020, déjà conseiller municipal, Richard Lizurey est élu 8e adjoint au maire de Chartres, Jean-Pierre Gorges, en charge de la « sécurité et de la tranquillité publique ». Il est également nommé vice-président délégué de la communauté d'agglomération Chartres Métropole.

Focus sur les unités de Police Secours,

Par Christelle GÉRARD, *Chef des Unités de Police Secours au sein du Commissariat de Villeneuve Saint Georges.*

Toute société moderne repose, au travers du contrat social, sur le respect de la règle, qui détermine l'ordre public et participe à la garantie de la paix. **Ainsi, dès 1896, Waldeck-Rousseau, sénateur et ancien ministre de l'Intérieur** rappelait que « *dans une société appelée à demander chaque jour à la science des révélations nouvelles, à conserver son rang dans un monde où se succèdent les révolutions économiques, l'individu veut, avant tout, être affranchi du soin de veiller à sa défense* ».

Il faisait écho à la devise de la Préfecture de Police de Paris : *Vigilat Ut Quiescant* (ils veillent pour qu'ils reposent). En effet, héritiers du Guet, corps de troupe qui constituait la police de Paris sous la monarchie, devenus la garde nationale sous la Révolution puis les sergents de ville, qui en 1829 furent les premiers à adopter un uniforme pour une meilleure distinction et reconnaissance de la population, les gardiens de la paix sont chargés d'une noble mission : la préservation de la paix publique. Ils portent aide, assistance et secours tout en veillant au respect des règles, l'action de la police se voulant vigilante et protectrice.

Les missions de la Police Nationale sont multiples et justifient sa structuration en plusieurs directions. La « police secours » renvoie à l'une de ces missions, indissociable de la modernisation de nos institutions, de la mission de police et de l'efficacité du secours aux personnes.

À la fin de la première guerre mondiale et devant le nombre important des blessés de guerre, les services d'urgences doivent se renforcer. Des gardes de nuit, puis de jour, sont organisées par les chirurgiens, qui demeurent toutefois difficiles à prévenir en urgence. Le service des urgences doit ainsi s'organiser. En 1928, le préfet de police de Paris donne naissance à « Secours Police » : les premières bornes d'appel police font leur apparition, suivies par le lancement du numéro d'appel 17. D'abord disséminées sur le territoire, ces bornes disparaîtront peu à peu avec le développement des lignes téléphoniques dans les années 70.

Après la seconde guerre mondiale, « Secours Police » devient « Police secours ». Dès les années 50, la brigade motocycliste parisienne se voit dotée de 2CV pour secourir les usagers de la route en situation de péril. Les véhicules sont peu à peu équipés de moyens radio qui permettent aux policiers de communiquer plus efficacement et d'être dirigés sur les interventions urgentes. En parallèle, un développement similaire s'opère en province et en zone gendarmerie. Les véhicules type H de Citroën et autres 2CV verront progressivement leur nombre renforcé pour être par la suite remplacés par les mythiques J7 et J9 qui seront équipés des premiers kit de secours d'urgence contenant bouée de sauvetage, brancard repliable et trousse de secours.

La création du SAMU et son développement au début des années 70 ainsi que le déploiement des véhicules de secours des pompiers de Paris dans les années 80, amèneront à la réduction de ces équipements, exception faite de la trousse de secours.

Les avancées technologiques que notre société a connues depuis ont également bénéficié aux policiers qui, désormais, sont équipés de moyens modernes et nomades adaptés à l'ensemble de leurs missions.

Aujourd'hui encore, cette adaptation du matériel de la police-secours aux avancées technologiques est essentielle tant ces policiers, dont le cœur de métier classique (protection des personnes et des biens, lutte contre la petite et moyenne délinquance), sont en réalité très souvent les primo-intervenants de situations de péril imminent et le relai de services spécialisés amenés à intervenir sur des situations périlleuses qu'ils figent jusqu'à leur arrivée (individu retranché, accident d'origine bactério-chimique, incendies, attentat ...).

Ainsi, les policiers de la Police Secours sont des généralistes du métier, qui se doivent d'être polyvalents, agiles et qui œuvrent anonymement à la noblesse de ce métier. Ils doivent s'adapter en permanence à toutes sortes de situations : tour à tour, et sans aucune transition, ils peuvent être amenés à sécuriser un accident de voie publique (matériel, corporel voire mortel), à faire cesser un tapage, à régler des différends entre usagers de la route ou de voisinage, à prendre en charge les victimes de toutes sortes de violences (rixes, vols avec violence, violences familiales, conjugales, agressions sexuelles, viols, harcèlement, racket), à intervenir sur des déclenchements d'alarme, à procéder aux constatations d'usage en cas de cambriolage, de dégradations, de découverte de cadavre ou encore à annoncer aux familles le décès d'un proche.

La police-secours est présente, au service de la population, 24h/24 pour recueillir des plaintes, patrouiller, lutter contre le trafic de stupéfiants, les squats, la délinquance routière, la prise en charge des individus en ivresse publique et manifeste, la recherche de personnes disparues et de mineurs en fugue. Leurs collègues de brigades restés au service ont, quant à eux, en charge l'accueil des victimes, 7 jours sur 7 et 24h/24, et la responsabilité des personnes interpellées, des personnes privées de liberté (garde-à-vue, rétention, écrou) au sein du commissariat de police. Ils peuvent se voir confier la surveillance d'un détenu hospitalisé ou la conduite à l'hôpital d'une personne privée de liberté pour examen médical.

Ces effectifs sont composés d'hommes et de femmes qui agissent quotidiennement au profit de la sécurité des citoyens. Tous les grades du corps d'encadrement et d'application sont représentés au sein des unités de police secours qui accueillent régulièrement des jeunes cadets de la République ou policiers adjoints en leur permettant de faire leurs premières armes avant de tenter le concours de gardien de la paix. Leurs vacations de travail sont riches, variées, imprévisibles, heureuses ou plus douloureuses. Interventions après interventions, les horreurs et la violence épaississent une carapace nécessaire qu'il convient de soulager afin qu'elle ne soit pas trop lourde à porter, par un esprit de corps et une solidarité ancrés dans le fameux "esprit Police", mais également par des débriefings opérationnels, des retours d'expérience et des actions de soutien psychologique permettant de mettre des mots sur le ressenti à l'issue des missions les plus traumatiques.

Au-delà du grade qu'il désigne, le terme "gardien de la paix" est l'essence-même du métier de policier dans toute sa noblesse avec une constante que l'on retrouve chez chaque policier de la "police-secours": en dépit de la pénibilité de leur métier, de la menace terroriste, des contestations sociales, leur engagement ne faiblit pas. **Gardant à cœur plus que jamais la devise de la Police Nationale "PRO PATRIA VIGILANT", ils ne cessent de veiller sur la paix publique pour que la patrie vive en paix et en sécurité.**

Quel cadre légal international en matière de cybercriminalité ? : enjeux et défis.

Par Marc-Olivier BOISSET et Jean LANGLOIS-BERTHELOT, *analystes au CRSI*

« *Immense opportunité, l'Internet sert hélas aussi à manipuler l'information. La cybercriminalité s'y répand. Les groupes terroristes y développent leur discours de haine et y recrutent des jeunes en rupture. Le principal risque aujourd'hui est l'écart entre les innovations et notre cadre juridique dont les concepts de base échappent à la dématérialisation* ».

Antonio Guterres, Secrétaire général des Nations Unies
Ouverture du Forum de Paris sur la paix, novembre 2019.

Le Comité des Ministres du Conseil de l'Europe a adopté le 17 novembre 2021, le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques. Pourquoi un protocole supplémentaire pour renforcer la lutte contre la cybercriminalité s'avère-t-il nécessaire ?

Les affaires de cybercriminalités revêtent la plupart du temps une dimension transnationale. Or, les pouvoirs judiciaires, en particulier la justice pénale, sont contraints par les frontières territoriales. Dans ce contexte, l'obtention des preuves électroniques s'avère très complexe : elles peuvent être « stockées dans des juridictions étrangères, multiples, changeantes ou inconnues » (1). De plus, cette problématique de l'extranéité impacte également la criminalité classique puisque la preuve numérique prend une place de plus en plus importante dans la résolution de ces affaires. Ainsi, les problèmes d'extranéité et d'accès à la preuve numérique ne sont plus l'apanage de la seule cybercriminalité, mais embrasse de plus en plus toute la criminalité.

Apparaissent ainsi de manière récurrente des problèmes d'extranéité : afin de pouvoir poursuivre le cyberattaquant à l'origine de l'infraction, l'État, ayant constaté celle-ci, est souvent dans l'obligation d'effectuer des demandes d'entraide judiciaire, en particulier pour avoir accès à la preuve numérique, et/ou des demandes d'extraditions vers l'État où est localisé le suspect.

En sus des problèmes d'extranéité, au niveau international, le droit du cyberespace est un véritable « millefeuille » de lois et de règlements superposés. Les procédures d'entraide judiciaire et les demandes d'extradition prennent trop de temps à être exécutées ce qui va ralentir voire rendre impossible l'actions judiciaires. Ainsi, le nombre de décisions de justice suite à des actes de cybercriminalité signalés demeurent très limités faute d'accès à la preuve numérique. L'exemple de l'affaire entre Twitter France et la préfecture des Yvelines jugée le 17 janvier 2022, constitue un cas emblématique dans ce domaine de l'accessibilité à la preuve numérique. Twitter France a été jugé dans cette affaire pour « refus de répondre à une réquisition du procureur ».

(1) Conseil de l'Europe. (2021). Nouveaux traités. Récupéré sur Conseil de l'Europe : https://www.coe.int/fr/web/Conventions/new-treaties

En effet, en 2021, dans le cadre d'une enquête pour injures, Twitter France n'a pas fourni les informations requises par le juge d'instruction. Ces informations étaient jugées nécessaires à l'identification des auteurs de celles-ci. Lors du jugement du 17 janvier, l'avocat de Twitter France a précisé que la transmission de ces informations à la justice « *dépend de la bonne volonté de Twitter International, qui est en dehors de la juridiction française et qui choisit de coopérer ou pas* » (2). Cette absence de coopération contribue au sentiment d'impunité des cybercriminels vis-à-vis des justices étatiques. Dès lors, « *il apparait important de mener une action résolue sur le plan international pour éviter l'évasion* » des cybercriminels « *vers des « paradis Internet* » » (3).

Pour améliorer la lutte contre la cybercriminalité sur le plan international, le protocole adopté par le Comité des Ministres du Conseil de l'Europe veut mettre en place à terme une base juridique commune concernant « la divulgation des informations relatives à l'enregistrement des noms de domaine et pour la coopération directe avec les fournisseurs de services pour les informations sur les abonnés, des moyens efficaces pour obtenir des informations sur les abonnés et des données relatives au trafic, la coopération immédiate en cas d'urgence, des outils d'entraide, mais aussi des garanties en matière de protection des données à caractère personnel » (4).

Avant de détailler ce nouveau protocole de la Convention de Budapest sur la cybercriminalité, il convient de détailler les procédures d'entraide judiciaire et de demande d'extradition ainsi que de revenir sur le contenu de la Convention de Budapest. Enfin, il conviendra d'analyser les limites de cette Convention dans la lutte contre la cybercriminalité.

Les problématiques liées à l'entraide judiciaire et à l'extradition dans les affaires de cybercriminalité

Les procédures d'entraide judiciaire et les protocoles de demandes d'extradition demeurent encore aujourd'hui plutôt inadaptés à la volatilité des preuves numériques et à la complexité de leur recueil. En effet, il n'existe pas à ce jour de procédures spécifiques pour les cybercrimes. De fait, ces processus demeurent trop long pour obtenir des résultats concrets permettant la mise en œuvre de poursuites judiciaires suite à des cybercrimes.

La mise en œuvre d'une entraide judiciaire entre deux Parties nécessite la plupart du temps un accord qui doit être transmis par la voie diplomatique. En France, par exemple dans son article 694, le Code de procédure pénal précise qu'en cas d'absence de Convention international :

« 1/ *Les demandes d'entraide émanant des autorités judiciaires françaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du ministère de la justice. Les pièces d'exécution sont renvoyées aux autorités de l'État requérant par la même voie* ;

(2) Stratégies. (2022, 01 18). Twitter France et son directeur général jugés pour ne pas avoir aidé la justice. Récupéré sur Stratégies: https://www.strategies.fr/actualites/marques/LQ121445C/twitter-france-et-son-directeur-general-juges-pour-ne-pas-avoir-aide-la-justice.html
(3) Féral-Schuhl, C. (2020). Cyberdroit 2020/2021. Paris: Dalloz.
(4) Féral-Schuhl, C. (2020). Cyberdroit 2020/2021. Paris: Dalloz.

2/ *Les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires françaises sont transmises par la voie diplomatique. Les pièces d'exécution sont renvoyées aux autorités de l'État requérant par la même voie.*

En cas d'urgence, les demandes d'entraide sollicitées par les autorités françaises ou étrangères peuvent être transmises directement aux autorités de l'État requis compétentes pour les exécuter. Le renvoi des pièces d'exécution aux autorités compétentes de l'État requérant est effectué selon les mêmes modalités. Toutefois, sauf Convention internationale en stipulant autrement, les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires françaises doivent faire l'objet d'un avis donné par la voie diplomatique par le gouvernement étranger intéressé. »

Ainsi, même en cas d'urgence, la voie diplomatique est censée donner son avis sur ce type de demande d'entraide. Cela ajoute une étape et donc ralenti l'exécution de la procédure permettant d'accéder à des preuves numériques par nature volatiles et éphémères.

En plus, de cette temporalité très longue, le manque de cadre commun sur le recueil de la preuve numérique s'avère également préjudiciable pour l'enquête judiciaire. En effet, contrairement aux preuves plus « classiques » (photographies, témoignages, etc.) la preuve numérique est particulièrement dépendante de la méthode de recueil. Ainsi, même si par chance, les traces numériques n'ont pas disparu une fois la demande acceptée, celles-ci peuvent être corrompues voir complétement inexploitables à cause de la mise en œuvre d'une méthode de recueil inadapté.

Concernant l'extradition d'un cybercriminel la procédure s'avère encore plus longue et plus fastidieuse à mettre en œuvre car elle dépend fortement des relations diplomatiques entre les parties surtout lorsqu'aucun traité d'extradition multilatéral ou bilatéral n'encadre celle-ci.

L'extradition est un mécanisme ou moyen juridique grâce auquel un État requis livre une personne localisée sur son territoire à un autre État requérant. Ce dernier peut faire la requête d'une extradition soit pour procéder à la traduction d'un suspect devant une juridiction compétente soit, parfois, directement pour l'exécution d'une peine. Ce mécanisme est au cœur de la coopération judiciaire entre les États au niveau international. Il fait l'objet de différents traités qui sont la plupart du temps bilatéraux.

Dans le domaine de l'extradition, la France a ratifié plusieurs traités bilatéraux et multilatéraux. Elle peut faire usage des accords d'extradition qu'elle possède avec tous les pays de l'Union Européenne. Elle a également signé des accords bilatéraux avec 50 pays dont les États-Unis, le Gabon ou encore la Chine.

Dans le cas où un traité d'extradition n'existe pas entre un État requérant et la France, c'est la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité dite « Perben II » qui est appliquée . On considère alors qu'« *en l'absence de Convention internationale en stipulant autrement, les conditions, la procédure et les effets de l'extradition sont déterminés par les dispositions du présent chapitre. Ces dispositions s'appliquent également aux points qui n'auraient pas été réglementés par les Conventions internationales* ».

Parmi les principaux principes retenus pour une extradition, une demande est généralement accordée si elle respecte à minima le principe de la double incrimination : les faits reprochés doivent être considérés comme un crime ou correspondent à un seuil minimum de gravité dans la législation française.

Enfin, comme le précise la loi du 9 mars 2004, l'extradition ne peut être accordée (Art. 696-4), « lorsque la personne réclamée a la nationalité française, cette dernière étant appréciée à l'époque de l'infraction pour laquelle l'extradition est requise » (République Française, 2004). Cette mesure est assez fréquente dans les accords d'extradition et peut constituer un frein à la poursuite des cybercriminels. A noter que dans le cas d'un refus pour cause de nationalité, conformément aux bonnes pratiques votées par les État du G8, l'État requis s'engage à confier l'affaire à ses autorités judiciaires nationales afin qu'elles engagent les poursuites contre la personne visée par la demande d'extradition.

De manière plus large la cybercriminalité profite directement du manque d'harmonisation des qualifications des infractions pénales. On peut penser notamment aux infractions liées aux droits d'auteurs ou à la pédopornographie. Par ailleurs, les moyens d'enquête et les procédures de jugement des infractions dans le cyberespace sont souvent très différents en fonction des États. Ces deux aspects rendent les poursuites et les jugements des affaires de cybercriminalité d'autant plus complexes. Actuellement, au niveau international, la seule réglementation contraignante qui va dans le sens d'une résolution de ces problèmes est la Convention de Budapest contre la cybercriminalité (5) (6).

La Convention de Budapest : une réponse internationale à la luttre contre la cybercriminalité ?

Au mois d'août 2021, depuis sa signature officielle le 23 novembre 2001, la Convention de Budapest a été ratifiée par 66 États et deux États l'ont signé sans la ratifier. Parmi les États signataires, 32 sont non membres du Conseil de l'Europe notamment les États-Unis, le Japon, Israël, le Canada, ou encore l'Australie. De plus, 12 pays, entre autres la Tunisie ou encore l'Afrique du Sud, sont également observateurs de la Convention et se sont engagés à la respecter (7). Par ailleurs, celle-ci a servi d'inspiration à d'autres États pour leur législation. En effet, « *plus de 70 pays supplémentaires ont pris la Convention comme source d'inspiration pour élaborer leur législation interne* » (8).

En sus des pays signataires, un certain nombre d'organisations internationales ont le statut d'observateur au sein de cette Convention (9) : Commission de l'Union Africaine (CUA), Union Européenne (commission et le conseil de l'UE, Eurojust, Europol, Agence de l'Union Européenne de Cybersécurité), Sous-groupe de la Criminalité de Haute-Technologie (HTCSG), Union Internationale des Télécommunication (UIT), Interpol, Organisation pour la Coopération et le développement économique (OCDE), Organisation pour la Sécurité et la Coopération en Europe (OSCE), Organisation des États américains (OEA),

(5) Conseil de l'Europe. (2001). Convention sur la cybercriminalité. Récupéré sur WIPO Ip portal : https://wipolex.wipo.int/fr/treaties/collection
(6) Féral-Schuhl, C. (2020). Cyberdroit 2020/2021. Paris: Dalloz.
(7) Conseil de l'Europe. (2021, août 15). Parties / Observateurs à la Convention de Budapest et Organisations Observateurs au T-CY. Récupéré sur Conseil de l'Europe : https://www.coe.int/fr/web/cybercrime/parties-observers
(8) Féral-Schuhl, C. (2020). Cyberdroit 2020/2021. Paris: Dalloz.
(9) Conseil de l'Europe. (2021, août 15). Parties / Observateurs à la Convention de Budapest et Organisations Observateurs au T-CY. Récupéré sur Conseil de l'Europe : https://www.coe.int/fr/web/cybercrime/parties-observers

Centre d'application de la loi de l'Europe du Sud-Est (CAES) et l'Office des Nations unies contre la drogue et le crime (ONUDC).

Ainsi, les États et les organisations ont pris fait et cause pour cette initiative du Conseil de l'Europe. Ils ont pleinement conscience que la lutte contre la cybercriminalité ne pourra être efficiente que si l'ensemble des États a la volonté de coopérer dans le cyberespace.

En préambule de la Convention, le législateur rappel qu'il est nécessaire : « *[…] de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale* ».

De plus, elle ajoute que : « *la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable* » (10).

Cette Convention a été complétée par un protocole additionnel le 7 novembre 2002. Dans celui-ci, l'effort est porté sur la lutte contre la diffusion de contenus à caractère raciste et xénophobe dans le cyberespace. Ce protocole additionnel plaide pour une harmonisation du droit pénal concernant ce domaine ainsi que pour une meilleure coopération internationale entre les États et en particulier concernant leurs forces de sécurité intérieure.

L'apport le plus important de cette Convention est qu'au-delà de l'habituel entraide entre services judiciaires étatiques et concours à l'extradition de cybercriminel, elle définit de nouveaux moyens de procédure constituant une nouvelle forme d'entraide judiciaire. A titre d'exemple, celle-ci prévoit qu'une perquisition puisse être réalisée pour le compte d'un État tiers et que les résultats de celle-ci devront être fournis à ce dernier pour les besoins de son enquête, notamment lorsque la cyberattaque a transité par le territoire d'un État où l'infraction ne pas être constatée. De plus, dans le domaine de l'extradition, la Convention prévoit que celle-ci ne peut être refusée que sur la base de la nationalité du cybercriminel recherché ou parce que l'État destinataire de la demande s'estime compétent pour cette infraction. A charge de ce dernier de tenir informé l'État demandeur des suites de l'affaire. Comme le souligne Féral-Schulhl, « *cet instrument juridique pourrait être considéré comme une norme de référence incontournable* » (Féral-Schuhl, 2020).

Néanmoins, cette Convention s'est avérée insuffisante pour faire face à l'augmentation exponentielle des actes de cybercriminalité. Ainsi, en s'appuyant sur l'article 46 de cette Convention, le Comité de la Convention sur la cybercriminalité (T-CY) a mis en place en 2012 un groupe dédié dit « *Groupe sur l'accès transfrontalier* » (11) afin d'étudier la question de l'accès transfrontalier aux données et celle de la compétence territoriale.

(10) Conseil de l'Europe. (2001). Convention sur la cybercriminalité. Récupéré sur WIPO Ip portal : https://wipolex.wipo.int/fr/treaties/collection
(11) Conseil de l'Europe. (2012). Le Groupe sur l'accès transfrontalier. Récupéré sur Conseil de l'Europe : https://www.coe.int/fr/web/cybercrime/tb

Un autre groupe dit « *Groupe sur les preuves dans le nuage* » ou « *Groupe de travail Preuves dans le Cloud* » a également vu le jour en 2015. Celui-ci avait pour objet d'étude l'accès à la preuve numérique en particulier dans le nuage ou cloud. Il convient d'ajouter qu'en plus des membres du bureau, le Groupe avait également des représentants du Japon et de la Mauritanie.

Ce Groupe a conclu en 2016 que « *le nombre de victimes ont atteint des proportions telles que seule une infime partie de la cybercriminalité ou autres infractions impliquant des preuves électroniques sera jamais enregistrée et donnera jamais lieu à des enquêtes* ». Ils ont ainsi fait le constat de l'impuissance des outils judiciaires actuels à lutter contre ce que l'on peut qualifier de « déferlante du crime dans le cyberespace ». Ils soulignent que cette difficulté est principalement liée à trois facteurs : le cloud, la territorialité et la compétence.

Suite aux conclusions de ces différents groupe de travail, les membres de la Convention n'ont pas jugé nécessaire de rédiger une nouvelle version de la Convention de Budapest. En revanche, ils ont décidé de lancer la rédaction d'un nouveau Protocole additionnel afin de renforcer l'efficacité des justices pénales et de préserver l'État de droit dans le cyberespace. Le T-CY a ainsi confié à un groupe de rédaction dédié, la conception de ce nouveau Protocole additionnel.

Ce groupe avait pour objectif de relever certains défis liés à la territorialité du droit pénal. Il devait en particulier trouver une solution pour faciliter les demandes d'entraides judiciaires entre États. En effet, aucune procédure spécifique aux preuves numériques n'existait jusqu'à aujourd'hui et les États s'appuyaient sur les procédures existantes pour les autres types de preuve. Il est également inadapté pour faire face au volume croissant des demandes de preuves électroniques. Mais la temporalité et les conditions de recueil des preuves dans le cyberespace étant très différentes, très souvent ces demandes ne fournissaient soit aucun élément soit des éléments inexploitables. Les rédacteurs du Protocole ont ainsi imaginé différents mécanismes, par exemple en cas d'urgence, dans le but de faciliter l'obtention de ces preuves numériques auprès notamment des fournisseurs de noms de domaine et des hébergeurs.

Il s'agit ainsi par exemple de pouvoir effectuer des demandes d'informations vers certaines entreprises afin d'identifier les personnes à l'origine de l'enregistrement d'un nom de domaine. De même, vis-à-vis des fournisseurs d'accès ou des hébergeurs, il s'agit de faciliter les demandes vers ceux-ci afin de récupérer plus rapidement les données de trafic et de connexion. Ainsi, ce nouveau protocole prévoit :

- une coopération directe avec les fournisseurs de services et les entités fournissant des services d'enregistrement de noms de domaine (article 6 & 7) pour la divulgation d'informations permettant d'identifier les suspects ;
- des formes accélérées de coopération entre les Parties pour la divulgation d'informations sur les abonnés et de données relatives au trafic (article 8) ;
- La coopération et la divulgation accélérées dans les situations d'urgence (articles 9 et 10) ;
- Des outils supplémentaires d'entraide (articles 11 et 12) ;
- La protection des données et d'autres garanties de l'État de droit (articles 13 et 14) (13).

(12) Conseil de l'Europe. (2015). Le Groupe sur les preuves dans le nuage. Récupéré sur Conseil de l'Europe : https://www.coe.int/fr/web/cybercrime/ceg

De plus, il convient de souligner que le champ de ce nouveau protocole est plus large que les simples infractions pénales concernant les systèmes informatiques eux même. En effet, il s'applique aussi pour les infractions pénales réalisées à l'aide de ce type de système. Ainsi, les procédures et mesures de coopération mise en place au travers de ce protocole additionnelle peuvent être utilisées pour récupérer toute preuve numérique liée à une infraction pénale. Par exemple dans le cas d'un homicide, il est possible de solliciter les parties pour récupérer les éventuelles preuves numériques qui permettraient de déterminer les différents coupables. Enfin, le Protocole énonce également plusieurs garanties afin de protéger la vie privée et d'encadrer le traitement des données à caractère personnel.

Enfin, le Protocole prévoit dans son article 12 intitulé « Équipes communes d'enquête et enquêtes communes », la mise en place de mesures de coopération dans le cas où il n'existe pas de traité international ou d'arrangement bilatéral entre les Parties incriminées dans l'enquête judiciaire. Ce volet est particulièrement intéressant car il permet de proposer à des Parties non signataires de la Convention, un cadre juridique immédiatement utilisable. Il pourrait ainsi permettre de réduire les délais de mise en place des partenariats dans ce type de cas.

Face aux zones lacunaires persistantes : vers la création d'un cadre international sous l'égide de l'ONU ?

Concernant la lutte contre la cybercriminalité, dès 2009, le commissaire divisionnaire Aghroum soulignait que « *face au risque que chaque pays ne déploie une sorte de cyberprotectionnisme, une ONU de l'Internet est nécessaire, avec de vrais pouvoirs d'intervention. Cette force aura à arbitrer la réponse informatique offensive qu'un État se verra contraint d'adopter face à des attaques* » (14). Il s'agissait pour lui d'avoir ici une approche globale de la réglementation du cyberespace sous l'égide de l'Organisation des Nations Unies. La première étape serait de construire un véritable droit international du cyberespace à l'image du droit maritime ou du droit aérien.

Jusqu'à maintenant, la Convention de Budapest constitue l'une des initiatives les plus prometteuses en matière de coopération dans la lutte contre la cybercriminalité en ce sens qu'elle concourt à améliorer l'harmonisation des législations au niveau international.

Néanmoins, celle-ci s'avère encore aujourd'hui toujours insuffisante pour lutter efficacement contre les cybercriminels et ne parvient pas à supprimer les zones lacunaires dans la prise en compte judiciaire et internationale de la cybercriminalité à la fois parce que les solutions proposées ne sont pas suffisamment contraignantes et qu'elles ne permettent pas d'harmoniser complètement le cadre législatif au niveau international.

Par exemple, l'exécution d'une commission rogatoire dans le cadre de cette Convention reste soumise à la loi nationale de l'État destinataire et au principe de la double incrimination.

(13) Comité de la Convention sur la cybercriminalité. (2021, avril 12). Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques. Récupéré sur Conseil de l'Europe : https://rm.coe.int/2nd-additional-protocol-budapest-convention/1680a2219b

(14) Aghroum, C. (2009, 10 30). Vers une cyber-ONU. Récupéré sur Bulletin de l'ILEC: https://www.ilec.asso.fr/article_bulletin_ilec/14659

Lors de la signature de la Convention, plusieurs États, comme les États-Unis ou encore la Suisse, ont émis des réserves concernant l'exécution de commission rogatoire, si, comme pour les extraditions, la condition de la double incrimination n'était pas remplie (15) (Conseil de l'Europe, 2001). Ce dernier point est particulièrement dimensionnant car de nombreuses infractions liées au cyberespace demeurent exclues de toute incrimination dans de nombreux États. Cette distorsion contribue à créer des zones lacunaires dans le cadre judiciaire du cyberespace et permet aux cyberattaquants par la même d'échapper aux poursuites.

De plus, la Convention ne regroupe aujourd'hui qu'une soixantaine de pays sur les plus de 190 Nations que compte la planète : les cybercriminels disposent donc encore de nombreux « *paradis Internet* » ou « *paradis du cyberespace* ». A titre d'exemple, l'Irlande qui héberge de plusieurs GAFAM n'est pas signataire de la Convention. Surtout, des nations de premier plan demeurent absentes de cette convention. Par exemple, la Chine, qui représente 1/7 de la population mondiale, et la Russie se refusent à adhérer à celle-ci car elle considère cette initiative comme ayant vocation à servir la puissance des pays occidentaux.

Ces 2 pays souhaitent ainsi plutôt la mise en place d'une initiative de lutte contre la cybercriminalité sous l'égide de l'ONU. C'est ainsi que le 27 juillet 2021, la Russie a soumis aux Nations Unis une proposition de projet de convention mondiale afin d'harmoniser au niveau international les lois contre la cybercriminalité. Cette convention vise notamment à élargir la liste des neuf cybercrimes de la Convention de Budapest : l'accès illégal, l'interception illégale, l'interférence de données, l'interférence de système, l'utilisation abusive d'appareils, la contrefaçon informatique, la fraude informatique, les infractions liées à la pédopornographie et les infractions liées à la violation du droit d'auteur et des droits connexes. Elle propose notamment d'y ajouter « *les crimes liés aux cryptomonnaies, aux produits médicaux contrefaits, à l'implication de mineurs dans des activités illégales* » (16).

De plus, il faudrait également élargir les prérogatives de la Cour Pénal International sur deux aspects au moins. D'une part, il sera nécessaire d'inclure dans son domaine de compétence les formes les plus grave de cybercriminalité qui touchent la communauté internationale. Aujourd'hui, la CPI ne peut instruire que les crimes précisés dans l'article 5 du statut de Rome : Génocide, Crime de guerre, Crime contre l'humanité, Agression. Ainsi, elle pourrait par exemple juger les affaires de cyberattaque contre des infrastructures critiques comme un réseau d'énergie ou un système de santé.

D'autre part, il sera nécessaire de rendre sa compétence subsidiaire comme l'ont été les Tribunaux Pénaux Internationaux antérieurs à la CPI. En effet, la CPI n'a pas primauté sur les juridictions internes des États. Par conséquent, elle ne se substitue pas au droit interne des États et ne sera mise en œuvre que si un État ne veut pas ou ne peut pas faire aboutir une procédure qui relève de sa compétence. On priorise ainsi ici le droit nationale et la mise en œuvre des tribunaux locaux plutôt que de la CPI.

(15) Conseil de l'Europe. (2001). Convention sur la cybercriminalité. Récupéré sur WIPO Ip portal: https://wipolex.wipo.int/fr/treaties/collection

(16) Brown, D. (2021, 08 13). Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. Récupéré sur Human Rights Watch: https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

Enfin, il serait nécessaire de disposer d'une commission rogatoire internationale spécifique pour les infractions liées au cyberespace. Aujourd'hui, lorsqu'une infraction présente un caractère international, il est possible pour une partie d'envoyer une commission rogatoire internationale vers une autre partie. Dans le cas de la France par exemple, cette dernière permet de déléguer la réalisation d'un acte d'instruction soit :

- à l'étranger et à la demande de l'État français,
- en France à la demande d'un État étranger.

Néanmoins, la procédure existante s'avère complexe et inadaptés aux infractions liées au cyberespace. Son inadaptation réside principalement dans le fait que celle-ci n'est pas encadrée correctement au niveau international : soit il n'y a pas d'accords bilatéraux ou multilatéraux encadrant ce type de demande soit ceux-ci existent mais ils ont tendances à trop limiter le domaine d'application de celle-ci et à ne pas répondre au besoin des enquêtes judiciaires pour les infractions liées au cyberespace.

Dans le cas où il n'y a pas d'accord entre les deux parties, il est possible pour un État d'envoyer une commission rogatoire à un autre État sans qu'il existe d'accord international bilatéral ou multilatéral entre ceux-ci à ce sujet. Cependant, l'État sollicité dans le cadre de cette commission rogatoire n'a aucune justification à fournir en cas de réponse négative à cette demande et peut tout à fait refuser la demande simplement en invoquant le principe de souveraineté. Des pays comme la Russie ou la Chine demeurent par exemple particulièrement réticent à coopérer et à fournir les données techniques issues de leurs hébergeurs.

Enfin, une autre difficulté concerne son exécution dans l'hypothèse où l'État recevant la demande accepte de l'exécuter. En effet, cette dernière sera mise en œuvre conformément aux procédures en vigueur sur le territoire de l'État. Or, dans ce domaine, faute d'accord préalable, il n'est pas tenu par une notion de délais pour sa réponse ce qui dans le cas de la preuve numérique s'avère un frein important de par sa nature éphémère.

De plus, il n'y aura pas d'harmonisation dans l'exécution de la procédure. Par exemple, le recueil de la preuve qu'elle soit numérique ou non fait l'objet de procédures strictes qui, si elles ne sont pas correctement respectées, risque d'entrainer un vice de forme lors des poursuites ou du procès. Ainsi, l'une des premières difficultés concerne la définition d'accord bilatéraux et multilatéraux adaptés aux infractions liées avec le cyberespace.

Dans le cas où il y a des accords, ceux-ci s'avèrent souvent inadaptés aux particularités du cyberespace. En Europe, par exemple, les pays membres du Conseil de l'Europe s'appuient sur la Convention européenne d'entraide judiciaire du 20 avril 1959 et sur son protocole additionnel du 8 novembre 2001.

Néanmoins, ce système demeure lent et fastidieux et ne permet pas de répondre efficacement aux infractions dans le cyberespace. En effet, le temps de la preuve numérique (éphémère et volatile) n'est pas celui de l'administration internationale. De plus, l'existence d'un tel accord ne garantis par pour autant que la commission rogatoire sera correctement réalisée même si elle est acceptée. En effet, comme ces traités dates d'une période antérieure à l'avènement du cyberespace, ils ne prennent pas en compte ses spécificités, notamment l'aspect éphémère et aisément falsifiable de la preuve numérique. Par exemple, ceux-ci peuvent parfois être limités à certaines actions comme l'audition de témoin ou la production de pièces à conviction ou encore à la fourniture de documents judiciaires.

Ainsi, la procédure de commission rogatoire tel qu'elle existe actuellement ne permet pas de répondre aux défis lancer par la cybercriminalité aux États. Il y a donc besoin de créer un outil dédié, par exemple une « commission rogatoire du cyberespace » dédiée aux infractions en lien avec le cyberespace.

Celle-ci pourrait par exemple être réalisée sous l'égide de la CPI. Il serait judicieux dans ce domaine de s'inspirer du mandat européen « *d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédures pénales* » (17). Décrit dans la décision-cadre n°2008/978/JAI adoptée le 18 décembre 2008 et signée par le Conseil de l'UE, il peut servir à « *[…] recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédures pénales pour lesquelles il peut être émis. Peuvent notamment être visés : les objets, documents ou données détenus par un tiers ou résultant de la perquisition, y compris au domicile d'un suspect, les relevés de l'utilisation de tous services, y compris de transactions financières, les procès-verbaux des dépositions, des interrogatoires et des auditions, et les autres documents, dont les résultats de techniques d'enquête spéciales* ». La mise en place d'une telle procédure au niveau internationale permettrait d'accélérer, à notre avis, les échanges de preuves numériques en les rendant possibles entre autorités compétentes sans avoir à passer par la voie diplomatique.

Pour conclure, la mise en place d'un tel niveau de coopération sous l'égide de l'ONU demeure à notre avis la solution la plus efficace pour lutter contre la cybercriminalité. Nous sommes conscients que l'instauration de ce type de coopération multilatérale renforcée ne sera pas aisée tant il faudra réussir à dépasser les réticences des États qui peuvent être de deux ordres.

D'une part, il y a la réticence de certains à abandonner une partie de leur souveraineté au profit d'une instance supra-étatique. D'autre part, certains États n'ont aucun intérêt à voir disparaitre ces zones lacunaires et se complaisent parfaitement à être un paradis du cyberespace au même titre que les paradis fiscaux.

À ce titre, nous pouvons noter que le 29 juin 2021 a eu lieu le premier débat formel sur la cybersécurité et les risques liés à l'utilisation malveillante des nouvelles technologies au sein du Conseil de sécurité de l'ONU. Est-ce le gage d'une prise en compte plus importante par l'ONU de ce problème dans un avenir proche ? Seul l'avenir nous le dira…

Marc-Olivier Boisset est expert en cybersécurité et analyste pour le CRSI.

Jean Langlois-Berthelot est un spécialiste en hacking éthique formé en droit et en mathématiques appliquées. Il est analyste pour le CRSI.

(17) Conseil de l'UE. (2008, décembre 18). Décision-cadre 2008/978/JAI. Récupéré sur Eur-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008F0978&from=FI

Cybersécurité : Focus sur le rapport annuel de l'Union européenne sur les cybermenaces

Par Guillaume LEFÈVRE

Le 9e rapport annuel sur le paysage des menaces de l'Agence de l'Union Européenne pour la Cybersécurité (ENISA Threat Landscape 2021) met en évidence l'augmentation de la cybercriminalité motivée par la monétisation à l'aide de ransomwares ou de cryptojacking.

Le contenu du rapport provient de sources ouvertes telles que des articles de presse, des opinions d'experts, des rapports de renseignement, des analyses d'incidents et des rapports de recherche sur la sécurité ; ainsi que par des entretiens avec des membres du groupe de travail ENISA sur les paysages des cybermenaces. À partir des informations recueillies, l'Agence produit sa propre analyse et ses vues du paysage des menaces qui sont censées être neutres pour l'industrie et les fournisseurs.

Le paysage des menaces de cybersécurité s'est développé en termes de sophistication des attaques, de complexité et d'impact. Une telle tendance est stimulée par une présence en ligne sans cesse croissante, la transition des infrastructures traditionnelles vers des solutions en ligne, l'interconnectivité avancée et l'exploitation des nouvelles fonctionnalités des technologies émergentes.

Sans surprise, les attaques de la chaîne d'approvisionnement figurent parmi les principales menaces en raison du potentiel important qu'elles ont d'induire des effets en cascade catastrophiques. Le risque est tel que l'ENISA a récemment produit un rapport sur le paysage des menaces dédié à cette catégorie spécifique de menaces.

Neuf principaux groupes de menaces ont été identifiés en raison de leur matérialisation importante au cours de la période de référence :

1. Logiciels de rançon
2. Logiciels malveillants
3. Cryptojacking
4. Menaces liées aux e-mails
5. Menaces contre les données
6. Menaces contre la disponibilité et l'intégrité
7. Désinformation - désinformation
8. Menaces non malveillantes
9. Attaques de la chaîne d'approvisionnement

La crise sanitaire du COVID-19 a créé des possibilités pour les adversaires qui ont utilisé la pandémie comme leurre dominant dans des campagnes d'attaques par e-mail, par exemple. La monétisation semble être le principal moteur de ces activités.

Les techniques auxquelles recourent les acteurs de la menace sont nombreuses. Il s'agit notamment des modèles commerciaux de type Ransomware en tant que service (RaaS), de multiples systèmes de rançongiciels d'extorsion, de la compromission des e-mails professionnels (BEC), du phishing en tant que service (PhaaS) et de la désinformation en tant que service (DaaS).

Menaces préoccupantes

Le ransomware est un type d'attaque malveillante où les attaquants cryptent les données d'une organisation et exigent un paiement pour restaurer l'accès. Les ransomwares ont été la principale menace au cours de la période considérée, avec plusieurs incidents très médiatisés et très médiatisés. L'importance et l'impact de la menace des rançongiciels sont également mis en évidence par une série d'initiatives politiques connexes dans l'Union européenne (UE) et dans le monde.

La compromission par le biais d'e-mails de phishing et le forçage brutal sur les services RDP (Remote Desktop Protocol) restent les deux vecteurs d'infection les plus courants. L'occurrence de systèmes de triple extorsion a également fortement augmenté en 2021 et la crypto-monnaie reste la méthode de paiement la plus courante pour les acteurs de la menace.
Le cryptojacking ou cryptomining caché est un type de cybercriminalité dans lequel un criminel utilise secrètement la puissance de calcul d'une victime pour générer de la crypto-monnaie. Avec la prolifération des crypto-monnaies et leur adoption toujours croissante par le grand public, une augmentation des incidents de cybersécurité correspondants a été observée. La crypto-monnaie reste la méthode de paiement la plus courante pour les acteurs de la menace.

La menace de mésinformation et de désinformation fait sa première apparition dans le rapport sur le paysage des menaces de l'ENISA.

Les campagnes de désinformation et de mésinformation se multiplient en raison de la présence accrue en ligne due à la pandémie de COVID-19 conduisant logiquement à une surutilisation des plateformes de médias sociaux et des médias en ligne.

Ces menaces sont d'une importance capitale dans le monde cybernétique. Les campagnes de désinformation et de mésinformation sont fréquemment utilisées dans les attaques hybrides pour favoriser le doute ou créer la confusion, réduisant ainsi la perception globale de confiance en conséquence et portant atteinte à ce principal promoteur de la cybersécurité dans le processus.

Acteurs de la menace : qui sont-ils ?

Les cybercriminels font partie intégrante du paysage des menaces. Ce sont des entités visant à commettre un acte malveillant en profitant des vulnérabilités existantes, avec l'intention de faire du mal à leurs victimes. Comprendre comment les acteurs de la menace pensent et agissent, quelles sont leurs motivations et leurs objectifs, est une étape importante vers une réponse plus efficace aux « cyber incidents ».

La surveillance des derniers développements en ce qui concerne les tactiques et techniques utilisées par les acteurs de la menace pour atteindre leurs objectifs est cruciale pour une défense efficace dans l'écosystème de cybersécurité d'aujourd'hui. Une telle évaluation des menaces permet à l'ENISA de hiérarchiser les contrôles de sécurité et de concevoir une stratégie adéquate basée sur l'impact potentiel et la probabilité de matérialisation de la menace.

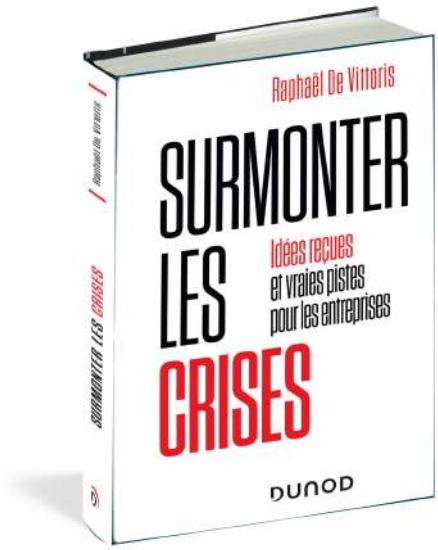
Aux fins du rapport 2021, l'accent a été mis sur quatre catégories d'acteurs menaçant la cybersécurité : les acteurs de la cybercriminalité, les acteurs de la cybercriminalité, les hackers pour compte d'autrui et les hacktivistes.

Lire le rapport complet à cette adresse :

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Lu pour vous : « *Surmonter les crises. Idées reçues et vraies pistes pour les entreprises* »,

de Raphaël de VITTORIS



Et si la crise était devenue la règle ?

Attentats, catastrophes industrielles, pandémie, cyberattaques, cataclysmes boursiers, conflits géopolitiques… La crise est partout. Elle fait partie intégrante du quotidien des entreprises.
Jeune discipline, la gestion de crise est devenue un thème central des organisations. La gestion de crise se structure autour de principes considérés comme incontournables, de la reconnaissance des signaux faibles, à l'identification d'un leader « chef de guerre », en passant par la sacralisation des retours d'expérience… Pourtant, les principes de gestion de crise ne sont pas si évidents, et encore moins infaillibles. Combien de fois les évènements ont contredit les théories ?
Raphaël de Vittoris s'attache ainsi à mettre à l'épreuve cinq idées reçues pour en proposer un angle de vue plus adapté aux crises modernes. En livrant de véritables pistes de survie, cet ouvrage aidera professionnels, managers et dirigeants à adopter la meilleure posture pour gérer les crises et les surmonter.
Il est impossible de gérer le chaos. En revanche, donnez-vous toutes les chances d'y survivre.

Dans cet ouvrage abordant des idées reçues majeures en gestion, cinq aspects sont évoqués en vue de proposer des pistes pour les entreprises. Ces cinq idées se complètent et sont abordées selon une approche chronologique :

Les signaux faibles sont détectables avant la crise

L'augmentation constante des processus de veille est une évidence et va de pair avec la multiplication des sous-traitants proposant de tels services. Toutefois, nous constatons en parallèle la répétition des exclamations de surprises face aux crises qui frappent nos organisations par ces mêmes gestionnaires.

La course aux signaux faibles n'est-elle pas une utopie contribuant à créer un sentiment injustifié de sécurité chez les dirigeants des organisations ?

Un leader « chef de guerre » est essentiel

L'analyse scientifique des cas de crises ainsi que l'expérience pratique nous amènent à une grande suspicion quant à cette vision fantasmée du leader. Une telle approche du leadership de crise nous semble constituer une porte ouverte à l'expression de biais profonds sans organe de contrôle ou de contre-pouvoir et peut expliquer nombre de décisions non pertinentes voire délétères dans des situations de crise. Nous proposons ainsi une notion de leadership pluriel, basé sur le désamorçage collectif de l'expression des biais pouvant louvoyer les interprétations de la cellule et donc ses décisions.

La temporalité des crises suit un pattern

Nombre d'ouvrages de la discipline segmentent la crise en différentes phases représentant une temporalité des évènements et une dynamique. Notre propos est de souligner que cette approche n'est pas en mesure de décrire les crises à la fois immédiates et holistiques telles que les cyberattaques les plus violentes.

Selon nous, c'est bien le jugement des événements qui dessine la dynamique des crises (en d'autres termes l'interprétation des membres de la cellule de crise et rien d'autre), où l'environnement d'équilibre d'origine ne sera probablement jamais retrouvé par les organisations.

La planification comme élément pivot de la réaction face à la crise

La planification revêt une valeur quasi-talismanique pour nombre de professionnels et experts de la crise. Elle possède une valeur rassurante pour les patrons, dirigeants et entrepreneurs qui pensent dès lors disposer d'un outil sur lequel se reposer lorsque le sol s'ouvrira sous leurs pieds. C'est bien par cette planification que nombre d'acteurs des organisations considèrent que toute la réponse à l'événement se base, se structure. Or, la confiance exagérée envers le protocole, identifiée par les chercheurs et confirmée par nos observations, est à l'origine d'un danger implicite, dissimulé, parfois aussi dangereux que la crise elle-même. Ce danger se matérialise par les biais cognitifs menant à des interprétations erronées ou des prises de décisions inadaptées conduisant à aggraver la situation.

Le retour d'expérience est gage de progrès

L'utilité du retour d'expérience est un élément incontesté parmi les concepts-cœurs basant la discipline de gestion de crise. Cependant, nous soulignons ce constat simple : au vu de l'importance et des bénéfices cruciaux des retours d'expérience aussi bien pour les individus que pour les organisations, comment se peut-il qu'après un nombre colossal de crises survenues à travers les pays et les organisations et ayant fait l'objet de retours d'expérience et même d'études scientifiques dans les cinquante dernières années ; nombre de cellules de crise semblent pourtant encore incapables de maîtriser les évènements ?

Présentation de l'auteur, **Raphaël de VITTORIS**



Group crisis manager de Michelin depuis 2015, **Raphaël De Vittoris** est aussi enseignant et chercheur en sciences de gestion sur les problématiques de gestion de crise, gestion des risques, communication de crise, négociation de crise et biais cognitifs en situation de crise.

Docteur en sciences de gestion et qualifié maître de conférences, diplômé d'un master en physiologie en environnement extrême, d'un master en administration d'entreprise et d'un master en hygiène, sécurité et environnement, il enseigne dans divers masters et il est membre du board de l'Institut d'études des crises et d'intelligence économique et stratégique de Lyon3. Il a vécu plus de 7 ans en Chine et parle le mandarin et a été le Directeur Hygiène, Sécurité et Environnement de la principale usine Michelin en Chine (Liaoning).

Thibault de MONTBRIAL invité dans Punchline sur CNews avec Laurence FERRARI (4 mai 2022)



Thibault de MONTBRIAL dans Calvi 3D sur BFM TV avec Yves CALVI (14 février 2022)



Thibault de MONTBRIAL invité de la grande interview de la Matinale de CNews (7 février 2022)



Thibault de MONTBRIAL invité dans Punchline sur CNews avec Laurence FERRARI (18 janvier 2022)





MENTIONS LÉGALES
La Lettre de la Sécurité Intérieure © Juin 2022
Tous droits réservés
Directeur de la publication : Thibault de MONTBRIAL
Conception, rédaction, réalisation : Guillaume LEFÈVRE, Florent OMNÈS
Crédit photos : CRSI
Centre de Réflexion sur la Sécurité Intérieure (CRSI)
10 rue Cimarosa – 75116 PARIS – France
Association Loi 1901 – N° enregistrement W751227813
Paris Tél : + 33 (0) 1 43 80 15 25- Fax : +33 (0)1 43 80 15 05
Contact : gl@crsi-paris.fr Web : https://www.crsi-paris.fr/

https://twitter.com/CRSI_Paris

www.linkedin.com/company/centre-réflexion-sécurité-intérieure/

www.crsi-paris.fr