

Mai 2024

La **LETTRE** de la **SÉCURITÉ INTÉRIEURE**

CRSI
CENTRE DE RÉFLEXION SUR LA SÉCURITÉ INTÉRIEURE

L'ÉDITO DU PRÉSIDENT 3
LE MOT DU SECRÉTAIRE GÉNÉRAL 4
L'ACTUALITÉ DU CRSI 5
L'événement 5
Le CRSI en province 6
Au quotidien 11
Dans les médias 12
DANS LES COULISSES DU CRSI 16
Général Patrick Collet, membre du comité stratégique depuis 2023 16
SÉCURITÉ INTÉRIEURE : RECENSION 18
Le rapport du Sénat sur les émeutes de juin 2023 18
Violences à l'hôpital 20
Les chiffres de l'insécurité 21
EXCLUSIVITÉ CRSI
TRIBUNE DE JEAN-ÉRIC SCHOETTL 31
Un sursaut d'autorité pour combattre l'ensauvagement ? 31
DOSSIER CYBERSÉCURITÉ 43
Télécommunications : un enjeu clé de la cyber 43
Une brève histoire de la cybersécurité 46
Cybercriminalité, la fin de l'insouciance numérique 49
L'État face à la cybercriminalité 62
La cybersécurité dans la stratégie militaire française 66
Intelligence artificielle et cyber-conflictualité 70
Les entreprises et professions libérales face à la cybercriminalité 74
Des métiers de la cybersécurité en pleine mutation 78
TRIBUNE 83
La cybercriminalité, fraude, pédopornographie, et cyberguerre 83
TÉMOIGNAGE 85
Résilience,la fondation au service des blessés de la vie 85
EN BREF 89
Parole aux jeunes du CRSI 89
Développement du CRSI 90
Dernières publications 91

L'ÉDITO DU PRÉSIDENT



THIBAULT DE MONTBRIAL

Chers amis,

Alors que nous terminons ce nouveau numéro de notre LSI, le jeune **Matisse**, **15 ans**, était **assassiné** à Châteauroux de 5 coups de couteau par un jeune afghan connu de la justice pour des précédents violents.

Ce nouveau drame illustre la hausse continue des **violences graves** commises dans notre pays, en particulier par les étrangers et par les mineurs. Il s'agit d'une **tendance de fond** qu'il est urgent d'enrayer par la mise en œuvre d'un véritable choc d'autorité coordonné par l'Intérieur et la Justice.

S'il était encore besoin de s'en convaincre, nous publions la compilation édifiante des principaux faits commis en France entre le 1er janvier et le 30 avril.

Pour nourrir la réflexion, vous trouverez dans cette lettre une tribune passionnante du constitutionnaliste **Jean-Éric Schoettl** "**Un sursaut d'autorité pour combattre l'ensauvagement ?**".

Le dossier de ce numéro est consacré à la **cybersécurité**, sujet majeur s'il en est, tant le domaine cyber constitue à la fois l'artère qui irrigue le fonctionnement de notre société, et son tendon d'achille.

Vous retrouverez également les **actualités du CRSI** pour ces deux derniers mois ainsi que nos réflexions habituelles avec en particulier une analyse du **bilan sénatorial des émeutes** de l'été 2023.

Le CRSI continue à se développer, et je remercie vivement ceux qui y contribuent.

N'hésitez pas à partager largement cette LSI autour de vous.

Bonne lecture !

Thibault de MONTBRIAL
Président du CRSI

LE MOT DU SECRÉTAIRE GÉNÉRAL



GUILLAUME LEFÈVRE

Chers lecteurs, chers amis,

Un plaisir toujours renouvelé que de vous présenter notre nouvelle Lettre de la Sécurité Intérieure.

Cette édition est quelque peu particulière puisqu'elle donne la part belle sur un sujet qui nous tenait à cœur depuis quelque temps déjà, la **cybersécurité**.

La cybersécurité n'est bien sûr plus qu'une tendance, elle nous préoccupe dorénavant quotidiennement.

En effet, qui dit **nouvelles technologies** (intelligence artificielle, objets connectés, industrie 4.0, cloud, informatique quantique, métavers,…) dit aussi dorénavant : **nouvelles menaces** !

Intensification des ransomwares, professionnalisation des hackers, pénurie chez les fournisseurs de solutions, développement de la cyberassurance, réglementation évolutive (NIS2, DORA,…) amplifient les contraintes et augmentent le terrain de jeu des cyberattaquants et pas que les **individuels** ou "**privés**", mais aussi ceux qui se cachent derrière un **État** ou une **organisation** s'en approchant.

On pense par exemple à Anonymous Sudan et bien d'autres encore qui défient la chronique par leurs actions contre des sites ou institutions très ciblées françaises ou européennes.

Les conflits actuels (particulièrement celui entre l'Ukraine et la Russie) renforcent ces cybermenaces, on parle dorénavant même de **cyberguerre**.
Notre souveraineté (numérique) est donc bien un élément clé de notre souveraineté globale et de notre sécurité

Souveraineté, résilience, sont en résumé, les maîtres mots de cette nouvelle Lettre de la Sécurité Intérieure.

Merci à tous pour votre fidélité, et excellente lecture à tous !

Guillaume LEFEVRE
Secrétaire général du CRSI

L'ACTUALITÉ DU CRSI

L'ÉVÉNEMENT



Le **mardi 19 mars**, le CRSI a eu le plaisir de recevoir le Préfet de police de Paris **Laurent Nunez** au siège d'Intériale Mutuelle et de Continuum Lab, partenaires privilégiés du Centre.

Après un mot d'accueil de **Gilles Bachelier**, Président du Groupe Intériale, le Préfet de police a pu répondre aux questions de **Dominique Rizet** (journaliste expert police justice).

Au cœur des discussions : **la sécurité des Jeux olympiques 2024**, un événement crucial pour la France et son image dans le monde.

La lutte contre la **délinquance**, l'**immigration clandestine**, le **trafic de stupéfiants,** et les **opérations places nettes,** ont fait l'objet d'échanges approfondis. La question des mineurs non accompagnés a aussi été abordée.

Face à des enjeux aussi vastes, le CRSI et le Préfet de police ont appelé à une réflexion globale et à l'élaboration de solutions concrètes. Ils ont insisté sur la nécessité de remettre de l'autorité au sein du pays pour garantir la cohésion nationale et construire un avenir commun.

Thibault de Montbrial a conclu cette matinée en annonçant une évolution importante pour le CRSI, dont les travaux vont désormais s'étendre à tous les sujets de souveraineté de la France (relations internationales, militaires, énergie, alimentaire, etc.). Cette évolution illustre la place croissante prise par le CRSI dans le débat national.

LE CRSI EN PROVINCE

Périgueux (Dordogne)



Le **jeudi 14 mars**, Thibault de Montbrial donnait une conférence à Périgueux autour des sujets régaliens, sécurité, police, justice, immigration, souveraineté.



Plus de **200 personnes** sont venues l'écouter et le questionner.

À l'issue de l'intervention, les participants ont pu échanger avec Thibault de Montbrial pour partager avec lui leurs préoccupations.

Thibault de Montbrial en a profité pour se **rendre sur le terrain**, notamment dans des exploitations locales. Dans un cadre naturel et chaleureux, des échanges passionnants ont eu lieu sur les thématiques de la souveraineté alimentaire et de la sécurité en zone rurale.

Objectif : **comprendre les réalités de chacun**.











Lyon (Rhône)



Le mardi 26 mars, Thibault de Montbrial s'est rendu à l'invitation de l'**Université Catholique de Lyon** pour animer une conférence sur l'importance de la sécurité intérieure à l'approche des Jeux Olympiques de Paris. Devant un auditoire de **150 étudiants** et quelques enseignants, Thibault de Montbrial a dressé un état de la menace, tout en proposant des solutions concrètes pour les contrer. Il a abordé ces enjeux en les restituant dans un contexte général.

"C'était un plaisir d'être avec les étudiants. C'est l'occasion unique de poser des questions aux personnes que je rencontre, sur leurs expériences, leurs attentes, leurs inquiétudes et leurs espoirs.
Je me nourris de ces échanges pour enrichir mes réflexions."



"Thibault de Montbrial, par sa connaissance pointue des sujets abordés a permis à nos étudiants de ressortir de cette conférence avec une bien meilleure compréhension des enjeux de sécurité intérieure, et pour cela, nous tenons à nouveau à lui adresser nos chaleureux remerciements."

Nathan, 2ème année de licence de droit à l'UCLy

"Nous avons connu Thibault de Montbrial par l'intermédiaire des différentes prestations télévisuelles. Son discours est précis, clair, il se base sur des éléments chiffrés, ce qui rend également son discours plus crédible et audible. Nous étions curieux de le rencontrer lors d'une de ces conférences du CRSI sur la sécurité intérieure, notamment sur les prochains Jeux Olympiques de Paris. Le fait d'assister à ces conférences nous a permis de constater que ***Thibault de Montbrial est une personne animée par l'amour de la France*** *et son expertise technique nous permet de mieux comprendre quels seront les prochains enjeux. Nous avons particulièrement apprécié ce monsieur qui est à l'écoute des gens, il n'hésite pas à discuter et échanger. Suite à ces fructueux échanges,* ***nous avons été motivés à adhérer au CRSI****. Nous conseillons vivement ces conférences qui sont très intéressantes et accessibles au plus grand nombre !"*

Carine et Enrico, venus assister à la conférence

La Roche-sur-Yon (Vendée)



Le **2 avril**, le CRSI était invité par l'une des associations étudiantes de l'**ICES** (La Roche-sur-Yon), pour donner une conférence sur un sujet d'actualité :

La violence urbaine, un mal occidental ?

Une **centaine d'étudiants** sont venus y assister ce qui a donné lieu à des échanges nourris.



Un tableau sans concession de la **violence urbaine** a été fait, depuis ses origines jusqu'à son ampleur et les dangers qu'elle représente pour la société.

Thibault de Montbrial a insisté sur la nécessité d'une approche pragmatique de ce phénomène, en s'attaquant aux causes profondes et en refusant d'abdiquer devant ces maux. Il a notamment mis en avant **le rôle crucial des forces de sécurité**, qui doivent être dotées des moyens nécessaires et soutenus juridiquement pour accomplir leur mission avec efficacité.

*"En ce qui concerne le sujet de la sécurité intérieure, il est difficile de trouver un meilleur connaisseur que Thibault de Montbrial. Les étudiants ont grandement apprécié son **engagement pour la protection de nos concitoyens** ainsi que son **dévouement pour la cause nationale**."*

Sacha, 3ème année de licence en science politique

AU QUOTIDIEN

Réunion de travail à l'IFRI

Le **5 mars**, une matinée de travail consacrée aux questions de défense s'est tenue à l'Institut français des relations internationales (IFRI). Accueilli par Thomas Gomart, Directeur Général de l'IFRI, l'événement a réuni le chef d'état-major de l'armée de Terre (CEMAT) ainsi que de nombreux chercheurs et officiers de l'armée de terre.





Conférence pour le Cercle des Administrateurs

Le **12 mars**, le CRSI était invité par le Cercle des Administrateurs que préside Caroline Ruellan (Présidente SONJ Conseil et Membre du Conseil de surveillance Ardian) pour un petit-déjeuner débat sur la sécurité intérieure de la France.

Une conférence portant sur la question sécuritaire à l'approche des Jeux Olympiques a été donnée.

Visite d'une délégation de l'Académie militaire de Saint-Cyr Coëtquidan au CRSI

Le **13 mars**, Ronan Doaré, directeur général de l'enseignement et de la recherche de l'Académie militaire de Saint-Cyr, Stéphane Baudens, directeur du Centre de recherche de Coëtquidan (CReC) et sept élèves-officiers du 2e bataillon de l'école militaire de Saint-Cyr sont venus échanger au CRSI autour d'un solide petit-déjeuner.



Conférences / dédicaces de Béatrice Brugère



À l'occasion de la sortie de son livre Béatrice Brugère a donné de nombreuses **conférences/dédicaces** dans **toute la France**, dont :

- Conférence au théâtre Alexandre III (Association des conférences d'enseignement supérieur de Cannes), le 12 avril.
- Festival du livre de Paris 2024, le 13 avril.
- 33ème salon du livre politique (Assemblée Nationale), le 27 avril.
- Dédicace interview Image et Droit à la librairie Dalloz, le 27 avril.

"Dans un environnement instable et violent nous avons besoin plus que jamais d'une institution forte et protectrice pour les plus fragiles en accord avec les attentes des citoyens pour retrouver un cap, une vision et une légitimité.

(...) Cet essai explore les raisons profondes et systémiques des crises et des mécanismes à l'œuvre qui nous empêchent de retrouver une institution qui réponde rapidement et avec justesse au besoin de justice."

Béatrice Brugère

Pour commander son livre, RDV ici.

Pour ne rien manquer de notre actualité,
vous pouvez nous suivre sur les réseaux sociaux

DANS LES COULISSES DU CRSI

GÉNÉRAL PATRICK COLLET, MEMBRE DU COMITÉ STRATÉGIQUE DEPUIS 2023



Saint-Cyrien, **parachutiste**, ancien chef de corps du 1er Régiment de chasseurs parachutistes et patron de la 11e Brigade parachutiste, le général de corps d'armée (2S) Patrick Collet a servi dans les Armées pendant près de 40 ans.

Son parcours est marqué par de multiples engagements opérationnels en **Afrique**, dans les **Balkans**, en **Afghanistan**, mais aussi sur le **territoire national**, en métropole et outre-mer.



Il a achevé sa carrière à l'été 2023 au poste d'**inspecteur de l'armée de terre** et à ce titre membre de son COSTRAT, après avoir commandé la 11ème brigade parachutiste et l'Académie militaire de Saint-Cyr Coëtquidan.

Désormais à la tête d'Art militaire et stratégie-Conseil, il exerce une activité de **conseil** dans différents milieux, professionnels ou associatifs, et **enseigne** la stratégie et le leadership à Sciences -Po Paris.

Expert auprès de l'Association pour le progrès du management, il participe enfin à la formation de chefs d'entreprises de tous domaines.

Ses nombreuses années à la tête de jeunes soldats et de futurs officiers en formation l'ont amené à développer sa réflexion sur ce qui préoccupe de plus en plus les Français : **cohésion nationale**, **éducation**, exercice de l'**autorité** et emploi de la **force légitime** au **service de la Nation**.

Désireux de poursuivre l'engagement d'une vie au service de la France, il rejoint le CRSI en 2023, soutenant le projet porté par son ami de longue date, Thibault de Montbrial.



POUR ADHÉRER AU CRSI :

helloasso

SÉCURITÉ INTÉRIEURE : RECENSION

LE RAPPORT DU SÉNAT SUR LES ÉMEUTES DE JUIN 2023

Du 27 juin au 7 juillet 2023, notre pays a connu un déferlement de violences que le Sénat a analysé en détail.

Un dramatique bilan humain et de lourds dégâts matériels

Le Sénat chiffre à **793 millions d'euros** le coût des émeutes de 2023, soit quatre fois plus qu'en 2005.[1]

- **40%** des sinistres déclarés concernent l'Île-de-France
- **42,5%** du coût total des émeutes concerne l'Île-de-France
- **12 031** véhicules incendiés



Deux personnes décédées et plus d'un millier de blessés.

782 agents des forces de l'ordre blessés en neuf jours, soit près de quatre fois plus qu'au cours des vingt-cinq nuits d'émeutes de 2005.

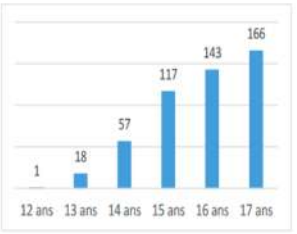
- 674 policiers
- 108 gendarmes
- 3 sapeurs-pompiers

Le profil-type des émeutiers

50 000 émeutiers,
la plupart des mineurs
29% d'étrangers

Âge des mineurs déférés lors des émeutes de l'été 2023

âge	Nombre	Pourcentage
12 ans	1	0,2 %
13 ans	18	3,6 %
14 ans	57	11,4 %
15 ans	117	23,3 %
16 ans	143	28,5 %
17 ans	166	33,1 %
Total	**502**	100 %
Non-réponse (NR) : 11		



Source : Direction de la protection judiciaire de la jeunesse

91% des auteurs sont des hommes
71% sont de nationalité française
Une moyenne d'âge **entre 17 et 18 ans.**

Un tiers des 3 500 personnes interpellées sont des mineurs

Le travail d'enquête judiciaire se poursuit. Il concerne souvent des personnes déjà connues des services de police.

[1] Le Parisien, 10 avril 2024

Des motivations protéiformes : entre défiance de l'autorité et opportunisme

Pourcentage des individus justifiant leur participation aux émeutes :

Motif de participation	Pourcentage
Décès du jeune homme	8%
Contestation de l'action des forces de l'ordre	10%

Une amplitude géographique qui dépasse les seuls quartiers "sensibles"

Si les quartiers sensibles ont été les plus durement touchés par les émeutes de juin 2023, l'impact de ces violences s'est étendu bien au-delà.

- 38,9% des sinistres déclarés aux assureurs concernaient l'Île-de-France, mais cette région n'est pas la seule à avoir été frappée.

- L'Auvergne-Rhône-Alpes et les Hauts-de-France ont également subi de lourdes dégradations, avec respectivement 13,1% et 8,6% des sinistres.
- Aucune région n'a été épargnée

Au total, **672 communes** réparties dans **95 départements** ont été touchées par les violences.

Le rôle déterminant joué par les réseaux sociaux

Ces événements ont représenté près de **15% de l'activité totale des réseaux** en France pendant cette période.

Des plateformes telles que X (Twitter), Facebook et Snapchat ont été utilisées pour :

- **Diffuser** des informations et des images en temps réel
- **Coordonner** les rassemblements et les actions, facilitant la mobilisation et la propagation des émeutes
- **Répandre** des rumeurs et de la désinformation

Violent affrontement contre les forces de l'ordre

- **Des milliers de tirs** de mortiers d'artifice recensés.

- **47 attaques** de casernes de gendarmerie enregistrées.

Augmentation de la population carcérale

- Création de **30 000 nouvelles places de prison** annoncée par le gouvernement (sans calendrier)

- **15 000 places de prison prévues d'ici 2027** par le ministère de la Justice

VIOLENCES À L'HÔPITAL

Le 9 avril, un brancardier a été violemment agressé au centre hospitalier de Challans (Vendée). L'agresseur, un patient de 35 ans, l'a insulté et frappé à plusieurs reprises, lui causant des blessures au visage et au thorax. Cet acte n'est pas anecdotique.

Chiffres clés[2]

- **+ 23% de violences** envers les médecins en 2022
- **2/3 des infirmiers** ont été victimes de violences[3]
- **32% des victimes** de violences physiques ont porté plainte en 2021.
- **20% des victimes** de violences verbales ont porté plainte en 2021

En 2022, le nombre de violences envers les médecins a augmenté de 23% et deux tiers des infirmiers ont été victimes d'agressions.

Conséquences

- Traumatisme psychologique pour les victimes.
- Départ de certains professionnels de la santé.
- Détérioration de la qualité des soins.

Proposition de loi en cours

La violence à l'égard des professionnels de santé est devenue un problème majeur. Une proposition de loi a été adoptée en première lecture à l'Assemblée Nationale en **mars 2024**. Son objectif est de dissuader les agressions et de faciliter les démarches pour les victimes.

Cette proposition de loi renforce d'abord les sanctions. Les peines encourues pour les violences commises contre les personnels soignants et non-soignants seront plus sévères, que ce soit à l'hôpital, en clinique, dans un cabinet médical ou encore en pharmacie. Le vol de matériel médical sera également puni plus lourdement. Un nouveau délit d'outrage spécifique aux professionnels de santé sera créé.

Les professionnels de santé victimes de violences pourront désormais être soutenus par leur employeur. Ce dernier aura la possibilité de porter plainte à la place de la victime (avec leur accord). Les personnes agressées pourront déclarer l'adresse de leur ordre professionnel comme domicile au moment du dépôt de plainte, pour éviter de renseigner une adresse personnelle.[4]

[2] Observatoire de la sécurité des médecins, dans le Le Parisien, 10 avril 2024
[3] Libération, 25 mai 2023
[4] Vie publique, 15 mars 2024

LES CHIFFRES DE L'INSÉCURITÉ

FOCUS 1ER TRIMESTRE 2024 [5]

Nature d'infraction	Nombre d'infractions	Variation (%)
Homicides	266	-13
Coups et blessures volontaires sur personnes de 15 ans ou plus	97809	+2
Violences sexuelles	24006	-1
Vols avec armes	2368	0
Vols violents sans arme	13017	3
Vols sans violence contre des personnes entendue	156395	-2
Cambriolages de logements	55986	+2
Vols de véhicules	36.796	0
Vols dans les véhicules	66403	+3
Vols d'accessoires sur véhicules	21025	-4
Destructions et dégradations volontaires	133316	+1
Usage de stupéfiants	64900	+4
Trafic de stupéfiants	12361	0
Escroqueries	121697	4

Tableau précédent : Analyse des crimes et délits enregistrés par la police et la gendarmerie à la fin du mois de mars 2024 grâce à un cumul des trois derniers mois (janvier à mars 2024), rapporté au cumul des trois mois précédents (octobre à décembre 2023).

[5] Service statistique ministériel de la sécurité intérieure

Quelques faits marquants

Le 8 janvier, 3 personnes sont tuées par balle à Bastia (Haute-Corse). Un homme, grièvement blessé lors de l'attaque, décède des suites de ses blessures à l'hôpital. La piste du règlement de compte sur fond de trafic de drogue est privilégiée par les enquêteurs. L'un des hommes tués était déjà connu des services de police pour des faits de trafic de stupéfiants.

Le 9 janvier, un braquage à main armée a lieu dans une armurerie à Eslettes (Seine-Maritime). 3 malfaiteurs tentent de voler des armes lorsqu'un employé riposte par des tirs. L'un des malfaiteurs, âgé de 18 ans, est tué sur place. Les deux autres prennent la fuite. Le jeune décédé était déjà recherché par la police pour le meurtre d'un adolescent de 17 ans à Valenton en décembre dernier.

Le 9 janvier, un policier hors service est reconnu, agressé et menacé de mort par deux hommes à Hennebont (Morbihan). Ses jours ne sont pas en danger.

Le 9 janvier, une saisie de 150 kg de résine de cannabis est réalisée près d'Orange (Vaucluse), deux suspects sont interpellés (un homme et une femme de 21 ans), soupçonnés d'alimenter des points de deal du Vaucluse.

Le 10 janvier, trois policiers sont violemment agressés par 3 prévenus lors d'un jugement pour des faits de vol au tribunal de Paris.

Le 11 janvier, un homme jette un pavé sur une voiture en patrouille à Paris (14e) en criant "Allah Akbar je vais tuer du flic".

Le 13 janvier, un adolescent de 16 ans est tué d'une balle dans la tête à Limoges (Haute-Vienne), à proximité d'un point de deal. La piste du règlement de comptes est privilégiée par les enquêteurs, car la victime était déjà connue des services de police pour des faits de petite délinquance.

Le 13 janvier, un groupe d'une dizaine d'individus tend un guet-apens à une patrouille de police à Étampes (Essonne). Les policiers essuient des tirs de mortiers d'artifice et des jets de cocktails Molotov. Trois fonctionnaires sont légèrement blessés et sont pris en charge par les secours. Les assaillants prennent la fuite avant l'arrivée de renforts.

Le 13 janvier, le corps d'une adolescente de 15 ans est retrouvé à Bain-de-Bretagne (Ille-et-Vilaine). Un adolescent de 15 ans est mis en examen pour le viol et le meurtre de cette jeune fille de sa famille.

Le 14 janvier, le chauffard d'une voiture faussement immatriculée, impliqué dans plusieurs faits de vols, refuse de s'arrêter à Dreux (Eure-et-Loir) et fonce sur les policiers qui ouvrent le feu.

Le 16 janvier, une violente agression a lieu devant un lycée à Saint-Denis (Seine-Saint-Denis). Farid, un lycéen de 17 ans, succombe à ses blessures.

Le 16 janvier, un conducteur sans permis et sous bracelet électronique est interpellé par les policiers de la BRAV-M dans le 5e arrondissement de Paris. Il transportait une arme de poing approvisionnée, suspectée d'appartenir à la gendarmerie nationale.

Le 17 janvier, un homme s'introduit dans la caserne de gendarmerie de Saint-Cyr-sur-Mer (Var), avant de pénétrer dans le logement de fonction d'un gendarme et sa famille, et de les agresser en hurlant "Allah Akbar".

Le 17 janvier, un jeune garçon de 14 ans est poignardé à mort à Saint-Denis dans la station de métro Basilique de Saint-Denis, sur la ligne 13.

Le 18 janvier, une opération de police a lieu au lycée Marguerite-de-Valois d'Angoulême (Charente), plusieurs hommes s'introduisent dans l'établissement et agressent une enseignante. La victime est aspergée de gaz lacrymogène et est légèrement blessée. Deux suspects âgés de 15 et 17 ans sont interpellés.

Le 19 janvier, Luca, un jeune homme de 20 ans, disparaît. Sa voiture est retrouvée incendiée à Cardeilhac (Haute-Garonne) et son corps est découvert dans le lac Saint-André à Fabas. Trois suspects, âgés de 19 à 21 ans, et déjà connus pour du trafic de stupéfiants, sont arrêtés.

Le 20 janvier, un homme de 31 ans, au volant d'une voiture, refuse d'obtempérer aux policiers à Argenteuil (Val-d'Oise), alors qu'il vient de commettre un vol dans un supermarché, agressant un agent de sécurité. Le suspect, qui est sous l'emprise de cocaïne, est interpellé après une course-poursuite. L'homme, de nationalité algérienne, fait l'objet de deux fiches de recherche et est en situation irrégulière en France.

Le 20 janvier, un homme de 52 ans est retrouvé mort calciné près d'une voiture en feu dans le 15e arrondissement de Marseille (Bouches-du-Rhône).

Le 21 janvier, 3 hommes agressent un policier adjoint qui vient de quitter son travail à Montpellier (Hérault). Ils le conduisent jusqu'à un distributeur à billets sous la menace d'un couteau pour le forcer à retirer de l'argent, puis lui volent sa voiture et prennent la fuite.

Le 23 janvier, un chauffard qui consommait du protoxyde d'azote démarre brutalement alors qu'un policier hors service de 22 ans le rappelle à l'ordre à Vénissieux (métropole de Lyon). Le fonctionnaire est traîné sur environ 200 mètres. Le suspect de 21 ans est interpellé peu après.

Le 23 janvier, un chauffard et ses passagers sont interpellés après avoir foncé sur un point de blocage des agriculteurs sur la RD119 à Pamiers (Ariège) et avoir tué une agricultrice, Alexandra Sonac (37 ans), décédée des suites de ses blessures, avec sa fille.

Le 23 janvier, un chauffard refuse d'obtempérer aux policiers à Pau (Pyrénées-Atlantiques). Le suspect et les passagers se débarrassent de deux armes à feu durant leur fuite. Les policiers sont la cible de jets de projectiles durant leur intervention.

Le 24 janvier, trois policiers de la BAC sont blessés à Arpajon (Essonne) lors d'une intervention visant à récupérer une moto volée. L'opération mène à l'interpellation de trois suspects, tandis que trois autres prennent la fuite, l'un d'eux fonçant sur les forces de l'ordre et percutant une voiture de policiers.

Le 25 janvier, les policiers interviennent pour un différend conjugal à Aulnay-sous-Bois (Seine-Saint-Denis). L'un d'eux, resté seul dans le véhicule, est agressé par une quinzaine d'individus armés de barres de fer, qui utilisent également des mortiers d'artifice.

Le 28 janvier, le corps sans vie d'Alicia, 28 ans, est découvert à son domicile de Beussent, (Pas-de-Calais). Son compagnon, âgé de 30 ans, avoue le meurtre, souhaitant concrétiser une relation virtuelle avec une femme qui s'est avérée être un escroc.

Le 29 janvier, un homme de 55 ans est sauvagement tué chez lui par ses deux beaux-fils et sa compagne à Plainfaing (Vosges). Les trois accusés, âgés de 27, 30 et 54 ans, sont mis en examen pour homicide aggravé.

Le 30 janvier, un chauffard et deux passagers cagoulés, armés de machettes, sont difficilement interpellés au terme d'une course-poursuite dans le quartier de l'Ariane à Nice (Alpes-Maritimes). Quatre policiers sont blessés lors de l'opération.

Le 2 février, deux policiers sont blessés à Istres (Bouches-du-Rhône) lors de l'interpellation d'un jeune homme de 18 ans circulant à scooter sans casque. Le scooter était volé et le suspect avait quelques grammes de cannabis en sa possession.

Le 3 février, trois personnes sont blessées, dont une grièvement, lors d'une agression à la gare de Lyon. L'homme, armé d'un couteau et d'un marteau, est interpellé par les forces de l'ordre. Fiché S au titre de la prévention de la radicalisation islamiste, il souffre de schizophrénie.

Le 5 février, un homme muni de lames de cutter s'introduit dans une école maternelle du 12e arrondissement de Paris et est difficilement interpellé par les policiers. Cet homme, de nationalité tunisienne, est visé par une obligation de quitter le territoire français (OQTF).

Le 6 février, un adolescent de 16 ans est poignardé à mort près du lycée Jules-Guesdes, et 6 suspects, âgés de 15 à 21 ans, sont placés en garde à vue à Montpellier (Hérault).

Le 7 février, un homme ouvre le feu sur les policiers de la BAC à Noisy-le-Grand (Seine-Saint-Denis) alors qu'ils interviennent pour une femme ayant déclenché son téléphone "grave danger". Un fonctionnaire est blessé. Les forces de l'ordre ripostent, blessant mortellement leur agresseur. Le suspect, sous contrôle judiciaire, devait être jugé en juin prochain pour violences conjugales.

Le 8 février, un jeune homme tente d'étrangler une policière devant le ministère de l'Intérieur, place Beauvau à Paris (8e), en essayant d'y pénétrer, avant d'être maîtrisé.

Le 10 février, cinq policiers sont blessés (dont deux sérieusement) par un chauffard au volant d'une voiture volée, refusant d'obtempérer, qui percute trois véhicules de police à Villeurbanne (Rhône).

Le 11 février, le corps d'une femme partiellement calcinée et ligotée est découvert dans une maison inhabitée à Sainte-Foy-lès-Lyon (métropole de Lyon). Il s'agirait de Cynthia Paveaux, âgée de 45 ans, disparue le 8 février.

Le 11 février, un homme est poignardé à six reprises en pleine rue dans le 14e arrondissement de Paris, avec la piste d'un acte antisémite privilégiée. La victime déclare connaître son agresseur depuis l'enfance et affirme que celui-ci faisait "une fixette" sur ses origines juives. Il ajoute avoir déjà déposé une plainte à son encontre par le passé.

Le 12 février, un homme de 36 ans, visé par une obligation de quitter le territoire, tente de tuer sa compagne de 47 ans à coups de couteau à Bordeaux.

Le 12 février, un homme de 20 ans tire à 17 reprises sur la porte de secours de l'Accord Arena à Paris (12e) avec une arme de poing semi-automatique. Il est appréhendé par les agents de sécurité qui lui ont refusé l'accès à la salle, étant donné qu'il n'avait pas de place pour assister au concert de la chanteuse italienne Laura Pausini.

Le 13 février, un jeune homme de 23 ans, connu des services de police pour des faits d'usage et détention de produits stupéfiants est abattu d'une balle dans la tête à Nangis (Seine-et-Marne). Une enquête pour "assassinat" a été ouverte.

Le 13 février, un homme de 21 ans armé d'un couteau agresse un policier à l'accueil du commissariat de La Rochelle. Il est maitrisé et placé en garde à vue pour tentative de meurtre.

Le 13 février, un chauffard refuse d'obtempérer à un contrôle de police à Porte de Bercy (Paris 12e). Il prend la fuite et se dirige vers Créteil où il fonce sur des policiers qui tentent de l'intercepter. L'un des policiers a ouvert le feu, blessant le suspect.

Le 13 février, un jeune homme de 26 ans est poignardé à 11 reprises en pleine rue à Arnouville (Val-d'Oise). Son pronostic vital était engagé mais il a pu être sauvé.

Le 14 février, le corps d'un homme entièrement calciné est découvert dans le 16e arrondissement de Marseille (Bouches-du-Rhône).

Le 17 février, une jeune femme est tuée à Vénissieux (métropole de Lyon) par son ex-petit ami, qui filme le meurtre, et tente de mettre fin à ses jours. Il est hospitalisé avec un pronostic vital engagé.

Le 17 février, une femme de 82 ans est victime d'un viol à son domicile, à La Penne-sur-Huveaune (Bouches-du-Rhône). L'homme de 35 ans soupçonné de s'être introduit dans le domicile de femme et de l'avoir violé était visé par une obligation de quitter le territoire (OQTF).

Le 19 février, un adolescent de 16 ans, passager d'un chauffard ayant refusé d'obtempérer, est entre la vie et la mort à l'hôpital. Le conducteur de 19 ans, drogué et sans permis, a violemment percuté une voiture en stationnement dans sa fuite, à Paray-Vieille-Poste (Essonne).

Le 19 février, une professeure d'histoire-géographie du lycée Pothier d'Orléans est agressée par une élève à qui elle a confisqué le téléphone portable.

Le 19 février, un jeune homme de 19 ans est blessé par arme à feu et par des coups à l'arme blanche, en pleine rue à Montpellier. Ce jeune homme de nationalité algérienne, déjà connu des services de police, est en situation irrégulière sur le territoire français. Questionné par les policiers, il n'a pas souhaité donner de précisions au sujet de ce qui lui est arrivé. Les auteurs sont en fuite.

Le 20 février, un père de famille de 39 ans est abattu devant son fils de 8 ans à Nîmes (Gard). Les policiers de Marseille ont interpellé trois suspects armés qui pourraient être les tueurs, à bord d'une voiture signalée volée, armés d'une Kalachnikov. Ils ont été placés en garde à vue.

Le 20 février, les policiers interpellent un lycéen de 16 ans à Armentières (Nord) soupçonné d'avoir menacé de mort l'un de ses enseignants. Durant des échanges avec ses camarades sur un réseau social, ce lycéen aurait fait part de son intention d'égorger l'un de ses professeurs.

Le 21 février, le corps de Pauline Le Denmat, disparue le 17 février à Lorient (Morbihan) est découvert. Son petit ami, qui avait alerté la police à la suite de cette disparition, est placé en garde à vue et livre des aveux, indiquant où se trouve la dépouille de la victime, tuée par plusieurs coups de couteau.

Le 22 février, le corps de Mayliss, âgée de 18 ans, portée disparue depuis le 14 février dernier, dans le Val-de-Marne, est découvert à Chilly-Mazarin (Essonne). L'ex-petit ami de la victime, âgé de 17 ans, est placé en garde à vue.

Le 22 février, un équipage de police de la brigade des réseaux franciliens (BRF) est intervenu pour une rixe dans le 18e arrondissement de Paris. Les forces de l'ordre interpellent un homme de 17 ans, armé d'un couteau qui tente de poignarder un fonctionnaire lors de son arrestation. D'après les premiers éléments, le suspect est en situation irrégulière sur le territoire français.

Le 24 février, les policiers interpellent un homme en train d'imposer une fellation à une jeune femme de 28 ans, ivre et à peine consciente, dans le 18e arrondissement de Paris. Il était visé par une obligation de quitter le territoire français.

Le 26 février, un collégien de 11 ans résidant à Goussainville (Val-d'Oise) est présenté à un juge des enfants, après la diffusion d'une vidéo sur TikTok dans laquelle il menace une de ses professeures. Il aurait également fait l'apologie d'un groupe terroriste.

Le 27 février, un homme de 29 ans en situation irrégulière, est soupçonné d'avoir violé une jeune femme de 20 ans sur un parking à Bordeaux. Il est interpellé et placé en garde à vue.

Le 28 février, le proviseur du lycée Maurice-Ravel situé dans le 20e arrondissement de Paris est visé par des menaces de mort sur les réseaux sociaux, après avoir demandé à une élève de retirer son voile. Le proviseur à quitté ses fonctions.

Le 1er mars, un homme d'une soixantaine d'années est violemment agressé et traité de "sale juif" alors qu'il sort de la synagogue, dans le 20e arrondissement de Paris.

Le 1er mars, un chauffard refuse d'obtempérer aux policiers à Thionville (Moselle). Sans permis, ivre et drogué, il a été interpellé et placé en garde à vue.

Le 4 mars, un adolescent de 16 ans est roué de coups par un groupe de jeunes agresseurs, en pleine rue, dans le 4e arrondissement de Paris. Il reçoit également des coups à l'arme blanche et est évacué à l'hôpital en état d'urgence absolue.

Le 6 mars, une adolescente de 15 ans est violemment percutée par le conducteur d'un deux-roues à Lyon, qui fuit la police (sans plaque d'immatriculation). Grièvement blessée, la victime est hospitalisée dans un état critique. Dans le scooter, les policiers découvrent un sac à dos contenant 2 armes de poing, dont une approvisionnée, ainsi que des munitions.

Le 7 mars, un adolescent de 15 ans est placé en garde à vue à Quimper (Finistère), soupçonné de violences sexuelles et de viols sur sa petite sœur âgée de 8 ans.

Le 7 mars, trois fonctionnaires sont blessés dont l'un très sérieusement à Carcassonne (Aude) suite à un appel pour une agression à l'arme blanche qui s'est transformé en guet-apens.

Le 7 mars, un chauffard de 17 ans est interpellé à la suite d'un refus d'obtempérer et d'une course-poursuite avec les policiers à Cergy (Val-d'Oise). Le mineur est actuellement sous bracelet électronique. Un des agents à moto est heurté. Les fonctionnaires ouvrent le feu à 7 reprises au total pour stopper le chauffard. Il est interpellé et n'est pas blessé.

Le 9 mars, une jeune femme de 20 ans est agressée par un homme armé d'un cutter à Lagny-sur-Marne (Seine-et-Marne).

Le 10 mars, des explosifs sont saisis dans un appartement avant d'être détruits par les démineurs à Lyon (8e). Un couple, déjà connu des services de police, est interpellé avant d'être placé en garde à vue. La femme était soupçonnée de confectionner des explosifs dans son appartement et de les revendre via les réseaux sociaux.

Le 12 mars, un jeune homme de 19 ans est poignardé à mort en pleine rue dans le 18e arrondissement de Paris. Un suspect de 17 ans est interpellé peu après et est placé en garde à vue.

Le 13 mars, un jeune homme de 18 ans est grièvement blessé lors d'une collision avec un véhicule de police à Aubervilliers (Seine-Saint-Denis). Le jeune homme à scooter aurait refusé d'obtempérer à un contrôle de police à La Courneuve, déclenchant une course-poursuite qui s'est terminée par la collision à Aubervilliers. Il a succombé à ses blessures.

Le 15 mars, un adolescent de 15 ans est interpellé après avoir menacé avec un couteau la principale de son établissement, le collège Edouard-Herriot à Chenôve, dans la banlieue de Dijon (Côte-d'Or). Il est placé en garde à vue. Il a rédigé un courrier de menaces, dans lequel il évoque les attentats de 2015.

Le 15 mars, un homme porté plainte après avoir été victime d'une agression homophobe violente et filmée, dans le 10e arrondissement de Paris.

Le 16 mars, un adolescent de 14 ans est soupçonné d'avoir violé une femme de 70 ans en pleine rue, à Villeneuve-sur-Lot (Lot-et-Garonne).

Le 17 mars, le commissariat de La Courneuve (Seine-Saint-Denis) est attaqué par des dizaines d'individus. Les agresseurs tirent des mortiers d'artifice sur le bâtiment et jettent des cocktails Molotov. Au moins 6 suspects sont interpellés. Ces actes font suite au décès de Wanys (le 13 mars).

Le 17 mars, le corps d'un homme de 28 ans tué d'une balle dans la tête est découvert dans une voiture en feu à Villeneuve d'Ascq (Nord). La victime était connue des services de police pour des faits liés aux stupéfiants. La piste d'un règlement de comptes est privilégiée.

Le 18 mars, une saisie majeure de cocaïne, d'un total de 2,7 tonnes, est réalisée au port du Havre (Seine-Maritime) dans un conteneur en provenance de la Guadeloupe.

Le 18 mars, un homme de 41 ans est grièvement blessé par balle en pleine rue, à Grenoble (Isère). Les deux auteurs à scooter ont pris la fuite.

Le 18 mars, une intervention de police difficile a lieu à Corbeil-Essonnes (Essonne). Les forces de l'ordre sont violemment prises à partie par une cinquantaine d'individus, à la suite d'un refus d'obtempérer commis par un homme à scooter. Durant les affrontements, l'un des policiers de la BST est blessé à la tête par le jet d'une trottinette. Les trois suspects interpellés, âgés de 18, 22 et 35 ans, sont placés en garde à vue.

Le 21 mars, une importante saisie de drogue a lieu dans l'Essonne, trois suspects sont interpellés à La Ville-du-Bois. Les policiers ont découvert 372 kilos de cocaïne dans un fourgon.

Le 22 mars, plusieurs armes à feu et de l'explosif sont découverts dans une voiture à Neuilly-sur-Marne (Seine-Saint-Denis) par les policiers de la brigade de répression du banditisme (BRB) de la direction de la police judiciaire de Paris au cours d'une opération. Un lance-roquettes, un fusil de type Kalachnikov, au moins une arme de poing et de l'explosif qui serait de type C4.

Le 23 mars, un chauffard de 51 ans refuse d'obtempérer aux policiers, à Mont-Saint-Martin (Meurthe-et-Moselle). Il percuté une voiture de police et blesse les deux fonctionnaires qui se trouvent à l'intérieur. Son permis de conduire était annulé et un test de dépistage a montré qu'il avait consommé de la drogue.

Le 24 mars, une adolescente de 16 ans est grièvement blessée à l'arme blanche dans le 11e arrondissement de Marseille, évacuée à l'hôpital dans une état grave. Son petit ami de 17 ans est placé en garde à vue et a reconnu les faits.

Le 25 mars, une jeune femme de 23 ans est victime d'un viol à Nantes (Loire-Atlantique), l'auteur présumé des faits, un sans domicile fixe de 18 ans l'entraine de force dans le local poubelles d'un immeuble et l'a viole. Il a déjà été condamné à 12 reprises alors qu'il était mineur, pour des faits de vol aggravé et de violences, ainsi qu'une fois pour agression sexuelle. Bien connu de la justice, le suspect venait de sortir de prison.

Le 26 mars, un policier est percuté et projeté sur le capot d'un chauffard refusant d'obtempérer près de Valenciennes (Nord).

Le 28 mars, un gendarme et sa compagne sont blessés après un coup de feu visant le logement de fonction du militaire à Marie-Galante (Guadeloupe).

Le 28 mars, deux frères de 16 et 18 ans sont interpellés à Malakoff (Haut-de-Seine) dans le cadre de l'enquête sur les piratages des espaces numériques de travail (ENT) dans les lycées et des menaces terroristes. Plus de 150 établissements ont été concernés par ces piratages en France. 323 menaces ont été recensées dans 44 départements et 20 académies.

Le 29 mars, deux équipages BAC sont violemment agressés par une trentaine d'individus au cours d'une intervention à Ris-Orangis (Essonne), ils sont la cible de jets de projectiles. Six suspects sont interpellés au total, dont un dealer présumé.

Le 29 mars, un adolescent de 16 ans est grièvement blessé à coups de couteau alors qu'il se trouve dans une rame du RER D. Il est évacué à l'hôpital en urgence absolue.

Le 2 avril, un chauffard de 24 ans sans permis qui se livrant à du rodéo sauvage au volant d'une voiture à Brest (Finistère) percute mortellement une jeune femme de 24 ans.

Le 2 avril, trois policiers sont sérieusement blessés par un chauffard refusant d'obtempérer à Val-de-Reuil (Eure). Le chauffard et son passager ont pris la fuite à pied après la collision.

Le 2 avril, Samara, 13 ans, est victime d'une violente agression menée par plusieurs personnes, devant le collège Arthur-Rimbaud à Montpellier. L'adolescente est rouée de coups par un groupe de jeunes hommes à sa sortie des cours.

Le 4 avril, une voiture de police sérigraphiée est incendiée devant le commissariat de la rue Félix-Pyat dans le 3e arrondissement de Marseille, par un groupe d'une dizaine d'individus. Quatre véhicules au total sont dégradés. Cet acte fait suite aux interventions répétées des policiers de la BST du 3e arrondissement qui ont fait "Place nette".

Le 4 avril, un adolescent de 15 ans est violemment agressé à Viry-Châtillon (Essonne). Roué de coups par trois agresseurs qui l'attendaient à la sortie du collège, Shamseddine a succombé à ses blessures le 5 avril.

Le 5 avril, un homme de 50 ans est mort égorgé à Muret (près de Toulouse -Haute-Garonne). Un adolescent de 15 ans, qui est le petit ami de la fille de la victime, est placé en garde à vue.

Le 7 avril, un adolescent de 16 ans est pris en charge aux urgences du centre hospitalier de Melun (Seine-et-Marne). Il présente des brûlures sur les jambes et explique avoir été séquestré et torturé avec un chalumeau. Il a été amené de force dans une cave par plusieurs agresseurs.

Le 7 avril, un incendie s'est déclaré dans un immeuble rue de Charonne, dans le 11e arrondissement de Paris. Le feu a fait trois victimes (des Afghans), dont deux ont été retrouvées avec des plaies par balle à la tête. L'enquête, initialement ouverte pour incendie, a rapidement pris un tournant criminel. La piste d'un homicide volontaire est privilégiée.

Le 8 avril, un homme âgé de 76 ans est interpellé à Tomblaine (Meurthe-et-Moselle), pour des agressions sexuelles et un viol sur une enfant de 10 ans. Le suspect, qui résidait dans un foyer pour personnes âgées, avait parfois la garde de la fillette pour la nuit et a été pris en flagrant délit par la police. Le septuagénaire avait déjà été condamné à 12 ans de réclusion pour viol sur mineur en 2004.

Le 9 avril, un petit garçon de 2 ans est mortellement percuté par un chauffard, un homme de 40 ans, sans permis à Rennes (Ille-et-Vilaine).

Le 9 avril, Zakaria, 15 ans, est poignardé à mort dans le quartier de la Monnaie à Romans-sur-Isère (Drôme).

Déclaration de Marie-Hélène Thoraval, maire de Romans-sur-Isère, membre du comité stratégique du CRSI :

"Le constat que j'avais fait après le drame de Crépol sur l'ensauvagement d'une certaine jeunesse reste malheureusement tristement d'actualité. Dans ce contexte, au-delà des belles déclarations, je veux dire avec force que rien n'avance et que les élus, au plus proche de la réalité du terrain, restent si peu écoutés par celles et ceux qui sont censés nous gouverner. Il y a pourtant urgence."

Le 10 avril, un homme, demandeur d'asile afghan de 25 ans, attaque deux hommes algériens sur les quais de Bordeaux. L'agresseur reproche aux victimes de boire de l'alcool pendant l'Aïd avant de les poignarder. L'un des hommes, Rachid Bouach (37 ans), meurt des suites de ses blessures. L'autre, Saleh Kharat (28 ans), est grièvement blessé (état depuis stabilisé). L'agresseur est abattu par la police après avoir pris la fuite.

Le 10 avril, un jeune homme de 18 ans est mis en examen pour le meurtre d'un couple de retraités dans leur maison (Combres - Eure-et-Loir). Il affirme avoir agi "*pour passer sa colère*" après une dispute avec son père.

Le 11 avril, un homme avoue avoir tué ses deux enfants âgés de 3 ans et 19 mois. Le suspect est interpellé après une tentative de suicide à Forges-les-Bains (Essonne). Les corps des enfants sont découverts dans le coffre d'un véhicule près d'une déchetterie.

Le 11 avril, deux hommes, âgés de 17 et 18 ans, sont interpellés à la gare RER de Villeparisis (Seine-et-Marne) alors que l'un des deux est armé d'une carabine dissimulée sous sa djellaba.

Le 12 avril, 7 policiers sont blessés lors d'une course-poursuite avec trois malfaiteurs soupçonnés d'avoir commis un home-jacking dans l'Essonne. Les trois individus sont finalement interpellés et placés en garde à vue.

Le 15 avril, la directrice de l'école de la Millière à Marseille est violemment agressée par une mère et sa fille (majeure), en raison d'un différend lié à une sortie scolaire. La victime s'est vu attribuer cinq jours d'incapacité totale de travail (ITT).

Dans la nuit du 15 au 16 avril, Philippe Coopman, 22 ans, est tué dans un guet-apens à Grande-Synthe (Nord). Il est violemment agressé à l'aide d'une hache et d'une batte de baseball. Deux mineurs, âgés de 14 et 15 ans, sont mis en examen pour assassinat quelques jours après le drame. Un troisième mineur est interpellé le 24 avril.

Dans la nuit du 19 au 20 avril, un homme sans domicile fixe, âgé de 24 ans, et en situation irrégulière séquestre, frappe et viole une femme de 49 ans à son domicile (Saint-Herblain), près de Nantes (Loire-Atlantique). Cette dernière est impliquée dans une association venant en aide aux sans-abri. Le suspect avait déjà été condamné à quatre reprises.

Le 20 avril, à la suite de l'incendie de l'immeuble survenu le 7 avril, où des victimes afghanes avaient été retrouvées avec des plaies par balle, une manifestation en hommage aux victimes dégénère dans Paris.

Le 21 avril, un homme de 74 ans est violemment agressé et poignardé dans la cité du Mail à Marseille (14e arrondissement) après avoir demandé à un groupe de jeunes de ne pas faire de bruit et de ne pas fumer de cannabis dans le hall de son immeuble. Trois suspects, dont un jeune homme de 18 ans et deux adolescents de 15 et 16 ans, sont interpellés et placés en garde à vue.

Le 27 avril, Matisse, un adolescent de 15 ans, est mortellement poignardé à Châteauroux (Indre). Le suspect, un afghan, âgé de 15 ans, avait déjà été mis en examen pour "vol aggravé avec violence" la semaine précédente. Il avait aussi été mis en cause dans une affaire de vol en réunion en février. La mère du suspect a également été interpellée, soupçonnée d'avoir participé au meurtre. Une enquête pour homicide volontaire est toujours en cours.

EXCLUSIVITÉ CRSI
TRIBUNE DE JEAN-ÉRIC SCHOETTL

Secrétaire général du Conseil constitutionnel de 1997 à 2007

UN SURSAUT D'AUTORITÉ POUR COMBATTRE L'ENSAUVAGEMENT ?

Le Premier ministre a raison : face à la montée de la violence des mineurs, nous ne pouvons plus nous bercer de mots ou nous contenter de demi-mesures. Mais il nous faut plus qu'un sursaut d'autorité. Il nous faut la réinventer. Et revoir de fond en comble plusieurs de nos politiques publiques. Est-il encore temps ?

Le mélange explosif formé par la violence juvénile, d'une part, la délinquance courante et les crimes communautaires et religieux, d'autre part, nous plonge dans un tel désarroi que nous sommes tentés, pour nous rassurer, d'attribuer la violence des mineurs à une cause unique (la drogue, les réseaux sociaux…) et d'en tirer une médication simple et expédiente. C'est la tentation de beaucoup de commentateurs et de personnalités politiques. Mais la réalité est autrement complexe. Le simplisme du diagnostic ne peut conduire qu'à l'insuffisance de la thérapeutique. Pour y voir plus clair et, si possible, entrer en voie de résilience, il faut au moins répondre aux questions suivantes.

Comment caractériser la violence des mineurs qui sévit actuellement à l'extérieur comme à l'intérieur de l'univers scolaire ?

Une partie de la violence des mineurs tient à l'environnement culturel contemporain, dans lequel baigne l'ensemble de la jeune génération. On en connaît les principaux traits : individualisme tout-puissant, indifférence à l'autre, hédonisme, consumérisme, dégradation du niveau scolaire, effondrement de la lecture remplacée par l'addiction aux écrans, enfermement narcissique dans les réseaux sociaux, exposition précoce aux contenus violents et pornographiques. Une autre composante de la violence des mineurs trouve sa source dans la déstructuration du tissu social, alliant pauvreté et monoparentalité, cas fréquent dans la population d'origine sahélienne.

> Une forte proportion des mineurs interpellés lors des émeutes de l'été 2023 provenait de familles monoparentales pauvres.

Une autre encore est liée à la consommation ou au trafic de drogue, et à tout son halo de délinquance courante. Une quatrième forme de violence, communautaire et confessionnelle, est le produit d'un endoctrinement fériste et salafiste qui touche désormais un nombre malheureusement non négligeable de familles musulmanes.

Ces différentes composantes de la violence juvénile sont d'intensités différentes. Les réseaux sociaux par exemple sont loin de tout expliquer : ils peuvent être vecteurs et catalyseurs de violence, mais n'en sont pas la cause première. Ces composantes sont en outre

de natures très différentes : l'anomie, au sein de la société globale, est un facteur de violence, mais l'excès de normes, au sein des communautés d'appartenance, en est un autre, non moins puissant. Ces composantes n'en sont pas moins inter-corrélées et elles sont toutes favorisées par la faiblesse des réponses que leur oppose le monde adulte. En s'interdisant d'être coercitive à l'égard des mineurs, la société - c'est-à-dire les parents, les maîtres et l'Etat - laisse libre cours à chacune de ces composantes de la violence juvénile.

Le lien entre carence de l'autorité (entendue comme une absence ou une insuffisance de coercition légale) et ensauvagement (pas seulement des mineurs) se manifeste dans d'autres domaines, tous plus ou moins liés à la crise de l'intégration. On pourrait parler de la justice des mineurs (le problème principal, à cet égard, étant non celui de l'excuse de minorité, mais celui de l'effectivité et de la célérité de la sanction, auquel le récent code pénal des mineurs apporte une réponse contre-productive), du faible nombre et de la gestion (aujourd'hui défectueuse) des centres éducatifs fermés, du maintien de l'ordre en général et du contrôle des manifestations sur la voie publique en particulier. Sans oublier le traitement des émeutes urbaines et la conduite à tenir par les forces de police et de gendarmerie en cas de refus d'obtempérer. Et l'ombre qui plane sur tout cela : la politique migratoire (ou plutôt son absence).

Une autre illustration de cette causalité entre défaut de coercition légale et ensauvagement du tissu social vient d'être mise en évidence par le préfet Michel Auboin dans son rapport sur les étrangers extra-communautaires et le logement social en France (Fondation pour l'innovation politique et Observatoire de l'immigration et de la démographie). Le bailleur public, et mieux encore le maire, "doit s'assurer que les locataires vivent en paix, ce qui suppose qu'il ait la capacité d'agir pour faire cesser les troubles graves à l'ordre public (agressions, trafic de drogue, rodéos...) qui naissent au sein de son patrimoine". Il faut donc remettre en cause le dogme du maintien dans les lieux, notamment en instituant un bail à durée limitée permettant, indépendamment de mesures plus coercitives (expulsions locatives), de ne pas renouveler un bail en cas de mauvais comportement. La recherche de la mixité sociale impose en outre de confier aux maires plutôt qu'aux algorithmes préfectoraux l'attribution des logements sociaux. Remplaçons "bailleur social" par "proviseur" et "révocation du bail du locataire fauteur de troubles" par "renvoi de l'élève fauteur de troubles" : les solutions se valent mutatis mutandis. De même, ne plus s'obliger à recaser dans un établissement scolaire ordinaire un élève renvoyé en raison de son comportement agressif se justifie autant que ne plus attribuer de logement HLM à un locataire incivil.

Faut-il mettre en cause la responsabilité pénale des parents ?

Ce serait non seulement cruel, mais encore inopérant, lorsque les parents sont dépassés par les évènements, ce qui est le cas de ces mères célibataires travaillant loin de leur domicile pour subvenir aux besoins d'une nombreuse nichée abandonnée à elle-même la plupart du temps. Mais il y a des situations où, oui, la famille doit être déclarée responsable parce qu'elle est en effet complice, passive ou active, des agissements de ses enfants. Il en est ainsi lorsqu'elle laisse ses rejetons commettre certains actes tout en ayant conscience de leur caractère délictueux, notamment en matière de trafic de drogue. Il en est ainsi a fortiori lorsqu'elle les y incite par esprit de lucre. Ou lorsqu'elle endoctrine ses enfants en leur inspirant la haine de la France ou de telle ou

telle catégorie de Français, voire en les mettant sur le chemin du djihad. En pareilles circonstances, il est à la fois juste et efficace de responsabiliser les parents sur le plan pénal et pas seulement du point de vue de leur responsabilité civile.

A la suite des émeutes urbaines de juin 2023, le garde des sceaux, avait pris une circulaire invitant les parents à exercer leur devoir de surveillance sur la conduite de leurs enfants et leur rappelant non seulement qu'ils peuvent être obligés à indemniser les victimes, mais aussi les risques pénaux qu'ils encourent (selon la circulaire) en application de l'article 227-17 du code pénal. Celui-ci punit de deux ans d'emprisonnement et de 30 000 € d'amende "le fait, par le père ou la mère, de se soustraire, sans motif légitime, à ses obligations légales au point de compromettre la santé, la sécurité, la moralité ou l'éducation de son enfant mineur", obligations définies par l'article 371-1 du code civil (protéger l'enfant dans "sa sécurité, sa santé et sa moralité, pour assurer son éducation et permettre son développement").

Mais il n'est pas sûr, au regard de ses termes et de la jurisprudence, que l'article 227-17 du code pénal, qui vise le délaissement des enfants par leurs parents, permette de poursuivre les parents à raison des actes criminels ou délictuels de leurs enfants. Le lien causal entre les agissements du mineur et la défaillance parentale serait la plupart du temps difficile à établir. Au demeurant, il ne semble pas que la responsabilité pénale des parents des émeutiers de 2023 ait été beaucoup recherchée et encore moins reconnue.

Aussi convient-il d'expliciter par un texte la responsabilité pénale des parents à raison des actes commis par leurs enfants. Tel était le sens de la proposition de loi "tendant à renforcer la responsabilité pénale des personnes qui exercent l'autorité parentale sur un mineur délinquant" déposée voici une vingtaine d'années par le sénateur centriste Nicolas About. Cette proposition insérait dans le code pénal un article 227-17 bis disposant que "Le fait, pour une personne qui exerce l'autorité parentale sur un mineur, d'avoir laissé ce mineur commettre une infraction pénale, par imprudence, négligence ou manquement grave à ses obligations parentales, est passible des mêmes peines que si elle s'était rendue coupable de complicité." Mais cette initiative s'est heurtée à un de ces nombreux tabous qui piègent tout débat sur la justice des mineurs.

Le tabou pourrait cette fois être levé si le parti progressiste et le Conseil constitutionnel n'y font pas barrage. Le projet de loi "relatif à la responsabilité parentale et à la réponse pénale en matière de délinquance des mineurs", que défendra Eric Dupont Moretti devant le Parlement, sanctionne en effet les parents lorsque leur négligence éducative a conduit leur enfant à commettre plusieurs crimes ou délits.

> La peine encourue est de trois ans d'emprisonnement et 45 000 euros d'amende, sans préjudice d'une peine complémentaire de travail d'intérêt général.

D'autres pays démocratiques, confrontés à la violence des mineurs, ont déjà sauté le pas. C'est le cas des Etats Unis. Ainsi, le code pénal de Californie, Etat progressiste, prévoit un emprisonnement d'un an et une amende de 2.500 $, ou l'imposition d'une période de probation, pour les parents ayant failli à leur devoir en laissant, en connaissance de cause, leur enfant commettre une infraction. Cette défaillance est en effet considérée comme confinant à la complicité ou au défaut grave de surveillance ayant causé aux tiers des dommages corporels ou matériels. L'Etat du

Michigan n'est pas en reste : tout récemment (9 avril 2024), la cour criminelle de Pontiac a condamné les deux époux Crumbley à dix à quinze ans de prison, à la suite du quadruple meurtre commis par leur fils, âgé de quinze ans, avec une arme qu'ils lui avaient offerte alors qu'ils connaissaient ses troubles de comportement.

La mise en cause de la responsabilité parentale, au pénal comme au civil, peut donc, dans certaines situations, constituer un élément de réponse à la délinquance des mineurs. Toutefois, compte tenu des caractéristiques actuelles de la violence juvénile, qui sont multifactorielles, il est illusoire d'en faire la panacée que certains voient en elle.

La défaillance de l'autorité explique-t-elle les phénomènes actuels ?

Carence de l'autorité (des parents, des maîtres et de l'Etat) : pour expliquer la montée de la violence chez les mineurs, ce diagnostic est désormais largement partagé. Les événements récents ont décillé beaucoup d'yeux. À Viry-Châtillon, le 18 avril, le Premier ministre fustige la "culture de l'excuse" et reprend son leitmotiv :

> *"Tu casses, tu répares, tu salis, tu nettoies, défies l'autorité, on t'apprend à la respecter."*

Il y a loin, bien sûr, de ces fortes paroles aux actes et des actes aux résultats. Mais, en attendant, elles marquent une victoire de la lucidité sur le déni. Hier encore, la référence au déficit d'autorité aurait été taxée de fantasme réactionnaire. En 2016, l'actuelle ministre de l'éducation, Nicole Belloubet, raillait "les fariboles sur la restauration de l'autorité ou le port de la blouse". Il est symptomatique que soit aujourd'hui portée au crédit de Gabriel Attal par la grande majorité de l'opinion une mesure prohibitive - l'interdiction de l'abaya – qui aurait été jugée stigmatisante par tous les bons esprits il y a quelques années. Nous venons de loin.

Toutefois, pour trouver une thérapeutique opérante, il faut aller jusqu'au bout du diagnostic. La nostalgie de l'autorité perdue ne suffira pas à remonter la pente. Pour que l'autorité s'affirme, il faut que la société dote sans réticence son titulaire des moyens effectifs et suffisants (matériels, juridiques, statutaires, psychologiques) d'exercer sa fonction. Ce n'est pas le cas aujourd'hui et cela donne la mesure de l'effort à accomplir pour restaurer ce qui peut l'être de l'autorité perdue.

La société contemporaine refuse-t-elle au dépositaire de l'autorité les moyens de sa fonction ?

Oui. Prenons le cas du proviseur du lycée Maurice Ravel, à Paris, confronté à l'élève qui refuse de retirer son voile dans l'enceinte de l'établissement. Peut-il, face à ce refus, déclencher des poursuites disciplinaires ? Les circulaires n'évoquent de telles sanctions que d'une plume tremblante, mettant sans cesse en avant la nécessité impérieuse du "dialogue" (avec l'élève, avec les parents). Hier l'élève insolent était consigné et, de surcroît, réprimandé par ses parents. C'était la double peine. Aujourd'hui beaucoup de parents demandent des comptes (lorsqu'ils ne le bousculent pas) au professeur qui ose admonester leur progéniture. Aujourd'hui, une suspension de plusieurs jours pour comportement illicite, agressif ou injurieux impose de réunir un conseil de discipline dont la composition n'est nullement acquise aux

responsables scolaires. Dans les quartiers à forte population immigrée, une certaine paranoïa communautaire paralyse les responsables scolaires lorsqu'ils auraient des velléités de sévir.

Et que faire face à une attitude provocatrice caractérisée ? Le proviseur du lycée Maurice Ravel pouvait-il, comme cela aurait paru naturel y a quelques décennies, contraindre physiquement l'élève à ôter son voile ou, à défaut, la saisir par le bras pour la mener à une salle de retenue ou à la porte de l'établissement ? Une telle "contrainte par corps" est ce que le droit administratif classique nomme "privilège d'exécution d'office". C'est, en théorie, celui de tout détenteur de l'autorité publique confronté à un refus d'obtempérer. Mais il a été implicitement aboli dans les établissements scolaires autant que dans les lieux publics.

Jusque dans les années soixante-dix, les gardiens de square, avec leurs casquettes, leurs houppelandes et leurs sifflets (panoplie des signes visibles et audibles de l'autorité), n'hésitaient pas à agripper un chenapan par l'oreille s'il piétinait une plate bande. Cela ne choquait personne. Aujourd'hui, le gardien de square serait révoqué et poursuivi pénalement s'il osait une telle manifestation d'autorité. Et, aujourd'hui, un policier ou un gendarme qui utilise son arme, même en respectant les conditions d'emploi, sera très souvent poursuivi pour homicide si un drame survient.

Si le proviseur du lycée Maurice Ravel s'était livré au quart de ce dont l'accuse, sur les réseaux sociaux, l'élève voilée, les autorités académiques l'auraient désavoué au motif que le souci de faire respecter la loi ne justifie aucun geste brutal. La doctrine est gravée dans le marbre des bons sentiments humanistes et pédagogistes : il faut toujours privilégier le dialogue sur la coercition lorsque sont en cause des questions aussi délicates que celles intéressant la personnalité et les convictions. Agripper la rebelle voilée par le bras ? Groupes militants et médias crieraient à la maltraitance islamophobe. Dans le contexte non pas multiconfessionnel, mais religieusement homogène, qui est celui de beaucoup de quartiers dont la population est issue du monde musulman (Maghreb, Sahel, Turquie, Caucase, Proche- Orient et Moyen-Orient), une partie significative des élèves verrait une héroïne dans la révoltée et une partie significative des parents, exposés aux discours communautaristes et aux prêches intégristes (l'interdiction du voile est une brimade contre les musulmans), en ferait une martyre. On imagine la suite. Si une simple sommation de respecter la loi a fait pleuvoir des menaces de mort sur le proviseur, le poussant à la démission, on n'ose penser à ce qu'une manifestation d'autorité musclée, banale il y a une cinquantaine d'années, aurait pu provoquer.

Le statut des titulaires de l'autorité doit-il être revu, y compris en dehors du monde enseignant ?

Rétablir l'autorité, c'est vrai au-delà de l'enseignement, suppose que la collectivité s'en remette beaucoup plus amplement qu'aujourd'hui au dépositaire de l'autorité. Et donc remplir celui-ci de la plénitude de ses prérogatives, y compris des plus traditionnelles d'entre elles, tel le "privilège d'exécution d'office". Sa latitude décisionnelle doit être sensiblement élargie, ce qui impose de se passer de ces encadrements sourcilleux censés interdire l'arbitraire. Quant au risque d'usage abusif du pouvoir délégué, inhérent à toute large délégation, il peut être combattu par un contrôle a posteriori sensible aux difficultés de la fonction.

A l'inverse, refuser de faire confiance au titulaire de l'autorité, refuser de lui déléguer un pouvoir de contrainte, c'est abdiquer l'essence même de l'autorité. Le législateur, comme les tutelles administratives et juridictionnelles, doivent le comprendre.

Comment la société peut-elle aider les professeurs confrontés, au sein même de leurs classes, à l'indiscipline, à la violence ou à la contestation des enseignements ?

Aide-toi et la société t'aidera. La communauté éducative doit pouvoir compter sur la société, mais elle doit d'abord rassembler et employer ses propres forces.

Des cours d'empathie et d'initiation aux valeurs de la République ne rétabliront pas la sérénité lorsqu'elle est sérieusement atteinte. Seule serait opérante une volonté farouche et solidaire de la communauté éducative de ne plus rien laisser passer en matière de violation des règles de la vie scolaire, qu'il s'agisse d'indiscipline, de harcèlement ou d'atteintes à la laïcité.

Ceci implique le pouvoir hiérarchique donné au proviseur ou au principal de se séparer d'un enseignant ou d'un surveillant hostile aux exigences de cette solidarité ; la fluidité de l'information entre professeurs, proviseurs, rectorat et, au-delà, avec tous les acteurs responsables de l'ordre public au sens large (police, justice, services sociaux) ; l'intervention de la police ou de la justice en direction de la famille ou du milieu pour contrer les représailles communautariste, punir les auteurs de discours de haine sur les réseaux sociaux ou pour mettre en cause, le cas échéant, la responsabilité civile ou pénale des parents ; la présence d'assistants d'éducation (terme symptomatiquement substitué à celui de "surveillants" il y a une vingtaine d'années) aptes moralement et physiquement à inspirer du respect aux élèves ; l'exercice par le dirigeant de l'établissement d'un pouvoir disciplinaire autonome allant jusqu'à la radiation de l'élève ; la remise en vigueur des codes de courtoisie passés (se lever à l'entrée du professeur, se mettre en rangs dans la cour avant de pénétrer en classe, vouvoyer le professeur…) ; l'attribution à chaque élève d'une note de conduite, inscrite à son bulletin ; l'uniforme scolaire ; la symbolique patriotique (distribution des prix, Marseillaise, salut aux couleurs…) ; la multiplication des internats et des placements d'office en internat des élèves qui, dans leur propre intérêt, comme dans celui de la collectivité, doivent être soustraits à leur milieu ; la garde des élèves dans les établissements d'enseignement après les heures de cours (comme le souhaite à juste titre Gabriel Attal) ; le transfert des établissements d'enseignement en dehors des cités problématiques ; l'inscription des élèves renvoyés dans des établissements spécialisés.

A quoi il faut ajouter un allègement de la tutelle juridictionnelle sur les décisions quotidiennement prises par les autorités scolaires, décisions qui, jusqu'à une date récente, étaient considérées comme des "actes d'ordre intérieur" échappant au contrôle du juge.

Programme indigeste ? Impossibilité de faire rentrer le dentifrice dans le tube ? Peut-être. Mais sans un big bang de l'autorité, la violence étendra ses quartiers dans l'univers scolaire. Dire qu'il est "trop tard" est un alibi trop commode pour éluder le changement de paradigme qui s'impose. Rattraper tant d'années de négligence, de lâcheté et de complaisance oblige l'école, et la société tout entière, à émettre aujourd'hui un message net et fort de retour à l'ordre. Il est peut-être trop tard, mais le déraillement est certain si nous ne

tentons même pas de changer le cours des choses.

N'est-ce pas prôner le retour à un passé scolaire idéalisé ?

Restaurer l'autorité à l'école, c'est en effet reconstruire l'estrade malencontreusement supprimée après 1968. C'est revenir à Jules Ferry : replacer l'enseignant en surplomb, refaire de lui "celui qui institue".

L'enseignant doit tirer l'élève vers le haut, en faire un être rationnel et un citoyen. Il doit l'intégrer au monde des adultes, le connecter à tout ce que la nation tisse entre nous de commune appartenance, à commencer par ce "riche legs de souvenirs" et cette "volonté de continuer à faire valoir l'héritage qu'on a reçu indivis" dont parlait Ernest Renan dans "Qu'est-ce qu'une nation ?". L'enseignant doit transmettre des connaissances, une mémoire et des valeurs, avec ce que cette fonction de transmission implique d'unilatéralisme.

L'enseignant doit redevenir le "maître", dans les deux sens du terme.

Cela ne doit pas le conduire bien sûr à délaisser la pédagogie ou à négliger le sentiment de l'enfant. Mais ce n'est pas à l'enfant de piloter sa propre éducation.

Pendant le temps éducatif, le monde adulte, en la personne du maître, doit tenir la barre, afin de pouvoir un jour la confier à l'élève devenu adulte. Tenir la barre, c'est faire œuvre de capitaine, et donc conduire, animer et inspirer. Mais aussi, le cas échéant, prévenir ou mâter des mutineries. Tout ne peut reposer sur le charisme personnel de l'enseignant. Aussi l'école doit-elle réapprendre à punir. Outre qu'elle garantit à tous les conditions d'une bonne transmission des connaissances, la sanction a, par elle-même, une vertu éducative sur l'élève fautif. On a trop confondu, pendant des années, autorité et autoritarisme.

S'il y a un domaine où on peut dire, sans gros risque de se tromper, que "c'était mieux avant", c'est celui de l'éducation publique.

Quelle est la part de l'immigration dans la montée de la violence juvénile ?

L'immigration n'explique pas toute la violence juvénile, mais elle y contribue substantiellement. On le voit bien avec les mineurs isolés étrangers. On l'observe dans les quartiers à forte population immigrée avec le trafic de drogue, les règlements de comptes, le vandalisme, les agressions sexuelles et les rodéos. On l'a constaté lors des émeutes urbaines de 2023, même s'il se trouvait en effet des Kevin et Matteo parmi les casseurs et les pillards.

C'est vrai aussi à l'école. Beaucoup de faits récents de violence survenus dans l'univers scolaire ou sa périphérie ont des connotations ethno-religieuses : enseignants agressés dans les salles de classe pour des propos jugés impies, passages à tabac d'élèves trop bien intégrés, remise en cause véhémente des enseignements et des règles de la vie scolaire. Y sont impliqués non seulement des élèves, mais leurs familles.

Un des traits communs de ces évènements est de révéler combien les cultures d'origine des populations nouvellement établies sur notre sol entretiennent avec l'Etat une relation différente de celle de la population native. Ces cultures d'origine considèrent généralement que l'Etat n'a pas à interférer avec la norme familiale et religieuse. Elles estiment, souvent en toute

candeur, que la règle religieuse et communautaire prévaut sur la loi française, laquelle est fréquemment ignorée ou mal comprise par les familles immigrées. Elles récusent pour cette raison le recours à la justice légale et se défient d'institutions nationales qu'elles perçoivent comme mystérieuses ou hostiles.

Qui plus est, contrairement à la société d'accueil, la plupart des cultures d'origine n'ont pas répudié le recours à la violence privée et en sacralisent même certaines formes, que ce soit pour des motifs religieux (guerre sainte, châtiment des blasphémateurs et des apostats) ou pour se conformer à des codes claniques (crimes d'honneur et vendettas). Ajoutons-y la jalousie d'adolescents étouffés par un carcan familial, communautaire et religieux à l'égard de celui (et surtout de celle) qui s'affranchit des interdits tribaux en adoptant les mœurs de la société d'accueil. Cette jalousie semble être à l'origine des agressions subies par Samara à Montpellier et par Shamseddine à Viry-Châtillon. Le crime du "miroir d'eau" à Bordeaux, le 10 avril, pourrait être de la même veine : des musulmans trinquant avec des kouffars à la fin du ramadan ont pu apparaître, aux yeux du jeune Afghan intégriste qui les a poignardés, comme des renégats lui inspirant une haine ambivalente à base de répulsion et d'attirance. Comprenons aussi que le refoulement sexuel des jeunes gens élevés dans un milieu musulman rigoriste, induit par l'inaccessibilité des partenaires féminins (a fortiori parmi les jeunes hommes célibataires qui composent une forte proportion des demandeurs d'asile), est une source de violence, notamment à l'égard des femmes.

Cette violence latente, de nature culturelle, a un effet inhibiteur sur l'exercice de l'autorité à l'école. Le scénario conduisant à l'assassinat de Samuel Paty est dans toutes les têtes. Il s'agit non d'une crainte isolée, mais d'une peur collective et permanente : comme le révèle une enquête du syndicat national des directions de l'Education nationale, un principal de collège ou proviseur du lycée sur quatre a vu l'enseignement dispensé dans son établissement ou les règles de vie de son établissement contestés au nom de l'islam. Dans ce lourd contexte, toute intimidation, devant être prise au sérieux, est susceptible de conduire à l'autocensure.

Par culpabilité post-coloniale, par peur de stigmatiser et d'amalgamer, par paresse, par lâcheté ou par embarras, la République a pratiqué jusqu'ici un irénisme préjudiciable tant à l'équilibre de la société française qu'à la bonne intégration des nouveaux venus. Il faut désormais non plus seulement cesser de pousser la poussière sous le tapis, non plus seulement accompagner psychologiquement nos enseignants, non plus seulement diffuser des guides de vivre ensemble et des vademecum sur la laïcité, mais encore couper les têtes de l'hydre islamiste plus vite qu'elles ne repoussent.

Combat régalien, mais aussi culturel et social. Il faut être intraitable à l'égard des activistes, mais aussi améliorer les conditions de vie et conquérir les cœurs de ceux qu'ils cherchent à rallier. L'école ne pourra redevenir cette fabrique de citoyens qu'évoquait Jean Jaurès dans sa lettre aux instituteurs de 1888 que si elle redevient un ascenseur social et si elle donne un contenu positif et attractif aux idéaux de liberté, d'égalité et de fraternité.

La France doit apprendre à se faire aimer de ses nouveaux enfants. Mais il faut, pour cela, qu'elle réapprenne à s'aimer elle-même. C'est ici que le bât blesse. Que peut faire l'éducation nationale si, pour un tiers d'entre eux (comme cela semble être le cas), les jeunes enseignants adhèrent au gauchisme woke, souscrivent à la vulgate décoloniale, dénigrent le récit national

et voient dans la laïcité un pavillon de complaisance de la xénophobie ?

En tout état de cause, la nation doit répliquer avec plus de détermination aux provocations de l'islamisme. Il aura fallu attendre quinze ans, entre l'affaire des foulards de Creil de 1989 et la loi de 2004, pour que la République ose interdire le port de signes religieux ostentatoires dans l'enseignement public. Il aura fallu des années de tergiversations et de disputes institutionnelles internes pour qu'elle prohibe l'occultation du visage dans l'espace public. Des délais de réponse aussi longs, de pareils états d'âme, la préparent mal aux batailles à venir.

En quoi un changement de la politique migratoire pourrait-il changer la donne ?

Un demi-million d'étrangers d'origine extra-européenne s'installent en France chaque année à divers titres (arrivées légales, asile, entrées clandestines).

Un afflux de cette ampleur compromet l'intégration de ceux qui s'entassent déjà sur son territoire.

Dans l'état du monde contemporain, avec la conquête du monde musulman par l'islamisme comme phénomène géopolitique durable et l'explosion démographique en Afrique, une immigration massive en provenance d'outre Méditerranée est ingérable. A court terme, elle déborde nos dispositifs d'accueil ; à moyen terme, elle compromet l'assimilation ; à plus long terme, elle expose la société française à de graves déchirements.

Bien sûr, une partie de ce flux s'intégrera, et parfois très bien. Mais notre devoir à l'égard des générations futures est de regarder en face les évidences quantitatives et la prégnance des facteurs culturels. La conduite exemplaire d'un Mamoudou Gassama (ce jeune malien sans papier qui sauva en 2018 un petit garçon suspendu à une fenêtre, en escaladant quatre étages à mains nues) ne doit pas être l'arbre héroïque cachant la forêt des ghettos et des fermentations toxiques dont ils sont le chaudron. Nombre d'enseignants professent aujourd'hui devant des classes composées exclusivement d'enfants de famille musulmane. Il est autrement plus difficile de "faire France" dans ces conditions que lorsque les petits Ali côtoient les petits Alain.

Donner ses chances à l'intégration impose de réduire significativement la pression migratoire. Pour prendre une image triviale, un plombier ne peut déboucher un lavabo s'il n'a pas d'abord fermé le robinet.

Cela suppose des révisions que la bien-pensance jugera, comme à l'accoutumée, "faire le jeu de l'extrême droite", alors que ce serait lui ôter le monopole de l'expression du sentiment populaire.

Les mesures à prendre sont sans mystère : limitation des visas et du regroupement familial, évaluation sérieuse des capacités d'intégration lors de la première délivrance d'un titre de séjour, suppression de l'automaticité du renouvellement de la carte de résident, simplification de la procédure de reconduite à la frontière pour rendre celle-ci plus effective, pression accrue sur les pays d'origine pour coopérer au rapatriement de leurs ressortissants, expulsion de tout étranger présentant une menace pour l'ordre public, déchéance de nationalité pour les binationaux ayant manifesté leur haine de la France, limitation de l'attractivité sociale de notre pays.

En matière d'asile, il nous faut prendre beaucoup mieux en compte le risque qu'incarnent, pour l'ordre public, non seulement ceux qui ont commis ou participé à des actes terroristes, mais également ceux qui adhèrent à l'idéologie qui en constitue le terreau. Il faut imposer, dans tous les cas d'accès à la nationalité, une vérification rigoureuse de l'assimilation. Enfin, il faut instituer un service national obligatoire pour les jeunes des deux sexes de manière à reproduire, sur le plan social et culturel, le brassage que l'ancien service militaire réalisait sur le plan social.

Un tel programme est un Himalaya à gravir, dira-t-on non sans raison.

L'instauration d'un service national obligatoire pose à lui seul une montagne de problèmes logistiques et financiers. Par ailleurs, une politique migratoire aussi ferme que celle évoquée ci-dessus nous mettrait en délicatesse avec la doxa. Elle serait en contradiction avec le lénifiant pacte migratoire européen, en voie de conclusion, qui n'aura pas pour effet, et n'a d'ailleurs pas véritablement pour objet, de réduire l'immigration. Un tel programme nous exposerait à de sérieuses difficultés diplomatiques, à des sanctions européennes et à une campagne dénonçant un virage illibéral de la France.

Et que dire des modifications juridiques ici proposées ? Elles se heurtent aujourd'hui à des obstacles constitutionnels ou conventionnels qui, pour être de nature souvent jurisprudentielle, n'en sont pas moins formidables. Nos cinq cours suprêmes, trois nationales (Conseil constitutionnel, Conseil d'Etat et Cour de cassation) et deux européennes (Cour de justice de l'Union européenne et Cour européenne des droits de l'homme), convergent, au titre de leurs divers chefs de compétence et sur divers terrains juridiques, pour entraver toute fermeté des pouvoirs publics en la matière. Au nom d'une vision abstraite et absolutiste des droits de l'homme, les droits de l'immigrant, cet "Autre" magnifié, prévalent sur les intérêts de la collectivité. C'est la revanche d'Antigone sur Créon. On l'a vu, tout récemment encore, avec le Conseil constitutionnel pour la loi immigration et pour l'initiative référendaire (RIP) des parlementaires LR. Ou avec la Cour de justice de l'Union européenne et le Conseil d'Etat pour le refoulement des irréguliers à la frontière franco-italienne. Ou avec la Cour européenne des droits de l'homme pour l'expulsion des islamistes caucasiens et pour le retour en France des femmes de nationalité française parties rejoindre Daech.

Franchir ces impressionnants obstacles est cependant vital pour l'identité, la sécurité et la souveraineté nationales. Il ne faut pas s'interdire de "renverser la table" par des "lits de justice" ou par la résistance aux jurisprudences inacceptables des cours supranationales. Un traité se renégocie ou se dénonce. La Constitution se révise. Il faut rétablir la primauté de la loi nationale lorsque le législateur, en toute conscience et en toute connaissance de cause, entend déroger au traité. Il faut instaurer un "dernier mot parlementaire" contre les jurisprudences incompatibles avec les intérêts supérieurs de la nation.

Le Royaume-Uni compose avec le communautarisme depuis longtemps. Pourquoi la France n'agirait-elle pas de même ?

Le Royaume-Uni compose en effet depuis longtemps avec le communautarisme, sans être épargné pour autant par la violence islamiste. Et ces accommodements produisent des résultats qui n'ont rien de raisonnable : importation du droit coranique en matière de

relations familiales, banalisation des accoutrements religieux jusque dans la police, manifestations pro-palestiniennes imposantes scandant des slogans antisémites, impunité des "grooming gangs" (bandes de violeurs d'origine pakistanaise) pour cause de political correctness. Cerise sur le gâteau : un premier ministre écossais islamo-woke qui fait voter une loi réprimant non seulement l'incitation à la haine, mais tout propos, même tenu en privé, susceptible d'être ressenti comme offensant par une minorité. La liberté d'expression menacée sur les terres qui l'ont vu naître : Robert Burns, David Hume, Adam Smith et Thomas Reid doivent se retourner dans leurs tombes. Pendant ce temps, le Danemark réinvente le délit de blasphème. Et, dans les communes bruxelloises à fortes populations turque et marocaine, travaillées par la propagande frériste, les autorités municipales, pour acheter la paix civile et être réélues, se plient à tous les désidératas communautaires. C'est toute l'Europe qui risque de se renier au nom du vivre ensemble. La bigoterie islamo-woke fait régresser l'Occident.

Nous n'en sommes pas arrivés là en France, mais, par endroits, nous glissons sur cette pente. Il faut la remonter. Pour ne pas "éteindre les Lumières", il ne faut transiger avec le communautarisme ni à l'école, ni dans les autres services publics, ni dans l'espace public. Aucune société ne peut vivre sans un ordre symbolique. Nous devons réapprendre à faire respecter le nôtre. Y compris dans nos entreprises et nos associations. Il faut soutenir celles d'entre elles qui prennent des règlements intérieurs pour soumettre leur personnel à des obligations de neutralité. A cet effet, il faut donner sa pleine portée à l'article L. 1321-2-1 introduit dans le Code du travail par la loi El Khomri ("Le règlement intérieur (de l'entreprise) peut contenir des dispositions inscrivant le principe de neutralité et restreignant la manifestation des convictions des salariés si ces restrictions sont justifiées par l'exercice d'autres libertés et droits fondamentaux ou par les nécessités du bon fonctionnement de l'entreprise et si elles sont proportionnées au but recherché"), sans le limiter aux personnels en rapport direct avec le public (ce qui est la tendance du juge judiciaire, comme l'illustre l'arrêt Camaïeu du 14 avril 2021 de la chambre sociale de la Cour de cassation).

La bonne nouvelle est que les imams éclairés existent, et que leur apport théologique pourrait inspirer un islam de France compatible avec la laïcité à la française, laquelle a une dimension non seulement juridique mais aussi coutumière. La mauvaise nouvelle est que les imams éclairés n'ont guère d'influence sur toute une partie des jeunes issus de l'immigration. Ceux-ci importent des idées théologiques du moyen âge parce qu'ils sont dans une logique d'affrontement manichéen avec la société française et qu'ils font de l'islam guerrier et de la lecture littérale du Coran leur oriflamme identitaire. Cette réalité est niée par les idiots utiles de l'islamisme, mais les imams éclairés, eux, en ont douloureusement conscience.

Que faire, en résumé, pour ne pas injurier l'avenir ?

Face à la montée de la violence en général et à celle des mineurs en particulier, face au fanatisme qui séduit si souvent la jeunesse, nous ne pouvons plus nous bercer de mots et nous contenter de demi-mesures. Il nous faut un "choc d'autorité". Il nous faut aussi revoir de fond en comble plusieurs de nos politiques publiques et non des moindres : logement social, politique de la ville, immigration, sécurité intérieure (s'agissant non seulement de la lutte contre le terrorisme, mais encore de la

prévention et de la répression de ce "djihadisme d'atmosphère" dont parle Gilles Kepel). Il nous faut enfin rééquilibrer nos mécanismes institutionnels dans le sens de la restauration de la souveraineté nationale et populaire, qu'il s'agisse des relations entre droit national et droit européen, de la place de la justice ou de la séparation des pouvoirs.

La contention de la violence est au fondement du pacte social. Si, en cette matière, cruciale pour l'avenir du pays, nous renonçons aux moyens de nos fins, il ne faudra plus larmoyer sur l'état de décivilisation dans lequel il s'enfonce.

Jean-Éric Schoettl est un haut fonctionnaire français et constitutionnaliste de renom, principalement connu pour avoir été le secrétaire général du Conseil constitutionnel de 1997 à 2007.

Il est l'auteur de *La Démocratie au péril des prétoires* (Gallimard, "Le Débat", 2022) et publie régulièrement des articles dans la presse.

Enfin, il est Commandeur de la Légion d'honneur.



DOSSIER CYBERSÉCURITÉ

TÉLÉCOMMUNICATIONS : UN ENJEU CLÉ DE LA CYBER

Contributeur anonymisé à sa demande. Il travaille depuis 40 ans dans le secteur des télécoms au sein d'entreprises publiques et privées.

Sécurité et souveraineté

Les technologies du numérique ont accéléré la transformation de nos entreprises, mais également de notre société, au travers de trois phénomènes majeurs :

La généralisation des solutions multi Cloud, qui ont pour effet d'opérer un grand nombre de services numériques sur des infrastructures partagées (dites de Cloud Publics, par opposition au solution de Cloud Privatif, dans lesquelles les infrastructures reste la propriété du client, les données étant hébergées dans des centre de données qui lui sont propres). Cela est vrai pour des solutions grand public (streaming avec Netflix, Apple TV…) mais également pour les entreprises (Microsoft Azure, Amazon, Google, Salesforces).

Le développement du télétravail avec un grand nombre de salariés qui travaillent à distance, plusieurs jours par semaine, en se connectant au système de l'entreprise via internet. Celui-ci a joué un rôle majeur pendant la crise du COVID, permettant à la plupart de nos entreprises de continuer à fonctionner en période de confinement, sans impact majeur sur la qualité du service rendue aux clients.

L'émergence de l'internet, des objets avec de plus en plus d'applications dans le monde industriel, (l'exemple le plus connu étant celui du compteur Linky d'EDF, mais des solutions semblables existent pour la relève des compteurs d'eau et de gaz, et plus généralement dans le monde industriel grâce au déploiement des réseaux 5G), mais également dans le monde de la santé (le patient connecté) ou encore celui des collectivités locales (les smarts cities).

Ces grandes transformations technologiques mais aussi sociétales ont toutes pour caractéristique commune d'utiliser les infrastructures de télécommunications. Elles sont le catalyseur du progrès économique et social des 30 dernières années et un enjeu de sécurité nationale.

En effet, sans des infrastructures réseaux sécurisées et résilientes, c'est l'activité économique toute entière de la nation qui risquerait de s'arrêter. Il est donc essentiel d'en conserver la maîtrise et d'en garantir la résilience et enfin, d'en assurer la sécurité.

Notre État doit donc répondre à de multiples défis :

- Maîtriser le développement de nos réseaux de télécommunications, pour faire face à une demande accrue de connectivité de la part des citoyens pour leurs activités quotidiennes, qu'elles soient professionnelles ou personnelles,
- Renforcer la résilience de nos infrastructures de télécommunications,
- Sécuriser la chaîne d'approvisionnement des fournisseurs de réseaux,
- Développer un écosystème de cybersécurité afin de préparer le pays à répondre aux cyberattaques.

Maîtriser le développement de nos réseaux de télécommunications

Les opérateurs de télécommunications doivent investir en permanence dans des réseaux de nouvelle génération (fibre, 4G, 5G…), avec des débits en constante augmentation et des prix à l'usager toujours plus bas, pendant que les GAFAMS récoltent les fruits de ces investissements en monétisant leurs services de contenus.

Or, les infrastructures de télécommunications coûtent cher : un opérateur doit faire face à des investissements toujours plus lourds pour suivre les évolutions technologiques, avec des retours sur investissement plus lointains. La fuite en avant consistant à favoriser la concurrence et la multiplication des opérateurs télécom dans une logique de prix bas pour le seul bénéfice du consommateur est un non-sens sur le plan stratégique, car elle affaiblit nos opérateurs sur le plan économique et met en péril à terme leur capacité à déployer les réseaux du futur, et par conséquent, notre souveraineté.

Pour éviter l'obsolescence de nos infrastructures de télécommunications, un assouplissement de la réglementation européenne est nécessaire pour autoriser une consolidation du marché, vecteur d'économies d'échelle pour les opérateurs.

Renforcer la résilience de nos infrastructures réseaux

Un seul chiffre résume la fragilité et la criticité des infrastructures de télécommunications :

99% du trafic internet intercontinental passe par des câbles sous-marins.

La destruction récente du gazoduc Nordstream 2 nous rappelle combien le risque de sabotage est réel, plaçant les infrastructures de télécommunications au cœur des enjeux de cybersécurité et de souveraineté de la nation.

Pour éviter toute perte de continuité de service, et même si une certaine redondance mise en œuvre permet d'assurer la résilience des réseaux les plus critiques, la gestion de risque doit nous inciter à renforcer la sécurité de bout en bout et la surveillance de ces infrastructures, à maintenir notre capacité à déployer les câbles sous-marins (Orange Marine est l'un des derniers acteurs européen sur le marché), et à proposer des routes alternatives comme les communications satellites.

Sécuriser la chaîne d'approvisionnement

La résilience de nos infrastructures commence par notre capacité à nous procurer les technologies en toute indépendance. Or, sécuriser la chaîne d'approvisionnement des différents composants de nos réseaux telecom est devenu un défi majeur pour la France et l'Europe. La dépendance vis-à-vis des fournisseurs américains et chinois, est particulièrement notable dans le domaine des équipements télécoms, (il ne reste que deux équipementiers en Europe, Nokia et Ericsson, aucun acteur français depuis la vente d'Alcatel en 2016) et il est indispensable d'assurer l'existence d'acteurs européens.

La sécurisation de la chaîne d'approvisionnement est encore plus critique dans le domaine de la cybersécurité, qui nécessite de nombreux outils, compte tenu de la multiplicité des cybermenaces pesant sur les services numériques, mais également en raison d'une pression réglementaire accrue de la part des institutions européennes. Il en résulte un

marché de la cybersécurité très fragmenté, avec une prédominance des acteurs américains (Cisco, McAfee, Fortinet, Symantec, Palo Alto Networks).

La résilience de nos réseaux télécoms passe par le déploiement de ces solutions techniques, mais aussi par la capacité des entreprises à se les approprier. Pour y parvenir, une sensibilisation à grande échelle des chefs d'entreprises et des salariés est indispensable. Si la plupart des grands groupes sont déjà préparés face aux menaces cyber, les TPE et PME le sont beaucoup moins et sont de fait beaucoup plus vulnérables. Or, selon une étude de l'opérateur britannique Vodafone, 50% des attaques cyber concernent les TPE et PME. Des campagnes de formation et de sensibilisation doivent être menées auprès de leurs dirigeants pour prioriser leurs investissements dans le domaine de la cybersécurité.

Développer un écosystème de la cybersécurité français

Les institutions européennes sont devenus le leader mondial en matière de normalisation et réglementations, qui se traduisent pour nos entreprises par un poids toujours plus grand en termes de coûts pour parvenir à respecter les contraintes réglementaires, pendant que les Etats-Unis restent le berceau de l'innovation technologique et de la création d'entreprises dans le domaine du numérique.

La réglementation est nécessaire, en particulier pour harmoniser les choix technologiques, mais elle ne doit pas être un frein au développement économique de nos entreprises. Une politique publique ciblée doit permettre l'émergence d'acteurs français innovants et compétitifs en termes de prix pour éviter toute dépendance vis-à-vis des fournisseurs de solution de cybersécurité. L'État français a un rôle à jouer, en accompagnant le développement des entreprises, en baissant les charges salariales, en appliquant un plan de cybersécurité aux entreprises publiques et collectivités locales et en développant la formation avec un tissu d'écoles spécialisées dans la cybersécurité.

Malgré la prédominance des GAFAM américains, il n'est pas trop tard pour prendre les mesures nécessaires à l'émergence d'acteurs français innovants dans le domaine de la cybersécurité. Le monde du numérique est en mouvement permanent. Qui connaissait l'IA générative il y 4 ans ? Le rapport Villani sur l'IA n'en parlait même pas !

Après des études universitaires à Paris, l'auteur a travaillé pendant près de 40 ans dans le secteur des télécoms au sein d'entreprises publiques et privées, en France et à l'international (aux États Unis , en Allemagne , en Belgique et en Angleterre). Il a occupé différentes fonctions opérationnelles et commerciales dans le secteur B2B et a également participé à de nombreux projets d'outsourcing et de fusions acquisition pour le compte d'opérateurs de télécommunications européens.



UNE BRÈVE HISTOIRE DE LA CYBERSÉCURITÉ

L'histoire de la cybersécurité est en constante évolution, intimement liée à l'essor des technologies de l'information et de la communication. Des premiers virus informatiques des années 1970 aux cyberattaques sophistiquées d'aujourd'hui, la cybersécurité s'est imposée comme un enjeu majeur pour les individus, les entreprises et les gouvernements.

1/ Les origines (1960-1970)

Dès les années 1960, des réflexions sur la sécurité des systèmes informatiques ont commencé à émerger.

En 1969, le projet **ARPANET**, précurseur d'internet, a vu le jour. Il a permis aux chercheurs et aux scientifiques de différentes universités et institutions de communiquer et de partager des informations. Cependant, il a également ouvert la voie à de nouvelles menaces.

En 1971, Bob Thomas a développé **Creeper**, un programme inoffensif conçu pour se propager d'un ordinateur à l'autre sur ARPANET. Ce programme a démontré la possibilité pour un code de se propager sur un réseau, jetant les bases des virus informatiques ultérieurs.

En 1974, le premier virus malveillant, "Elk Cloner", a été créé par un étudiant pour infecter les systèmes Apple II.

2/ L'essor de la menace (1980-1990)

Les années 1980 et 1990 ont connu une explosion de la cybercriminalité.

En 1983, en réponse à l'épidémie du virus Elk Cloner, John McAfee développe **VirusScan**, le premier antivirus commercial.

En 1988, un événement majeur attire l'attention du monde entier sur la gravité de la cybercriminalité : **le virus Morris**, créé par inadvertance par un étudiant de Cornell University.

> Ce virus infecte plus de 6 000 ordinateurs connectés à internet.

Les années 1990 voient l'émergence de groupes de hackers célèbres, comme le Chaos Computer Club et Legion of Doom.

Cet essor de la cybercriminalité dans les années 1980 et 1990 a eu plusieurs conséquences importantes :

- Prise de conscience accrue par les entreprises et les gouvernements.
- Investissement dans la sécurité pour contrer les menaces croissantes.
- Une collaboration internationale pour lutter contre la cybercriminalité devient évidente.

3/ Mise en place d'une réglementation (années 2000)

Les années 2000 ont vu l'émergence de la cybercriminalité organisée. Des groupes structurés, comme le Russian Business Network, ont exploité des vulnérabilités

logicielles pour voler des données sensibles et extorquer des fonds aux entreprises.

Des attaques ciblées ont commencé à viser des infrastructures critiques, telles que les centrales électriques et les réseaux de transport.

En réponse aux menaces croissantes, la décennie 2000 a connu un effort accru de normalisation et de réglementation en matière de cybersécurité.

La **loi Gramm-Leach-Bliley** (GLBA) aux États-Unis en 1999 ont imposé des obligations aux entreprises de protéger les données financières des clients.

Cette période a également été marquée par l'essor de la cybersécurité en tant que profession à part entière. La demande croissante en experts qualifiés a conduit à la création de formations spécialisées et de certifications professionnelles en cybersécurité.

4/ Défis contemporains (années 2010 à nos jours)

Le paysage de la cybersécurité n'a cessé d'évoluer au cours des années 2010 et continue de se complexifier aujourd'hui. L'essor de nouvelles technologies et tendances a créé de nouveaux défis et exigences en matière de sécurité.

92% des Français accèdent à Internet tous les jours

5/ Quelques exemples marquants de cyberattaques

Attaque de TV5Monde en 2015

Le 8 avril 2015, TV5Monde a été la cible d'une cyberattaque de grande envergure qui a perturbé la diffusion des programmes pendant plusieurs heures et a également touché ses sites web et ses réseaux sociaux.

Nombre de personnes touchées : 1 milliard.[6]

Les auteurs de l'attaque se sont identifiés comme étant le "Cybercalifat", un groupe de pirates informatiques affiliés à l'organisation terroriste État islamique.

Attaque de Yahoo

En décembre 2016, Yahoo a révélé qu'une cyberattaque avait eu lieu en 2013.

Elle a affecté l'ensemble des 3 milliards de comptes d'utilisateurs, sans que l'entreprise ne s'en aperçoive.

Les pirates informatiques, soupçonnés d'être liés à un groupe russe, ont réussi à mettre la main sur une quantité effarante de données personnelles. Noms, adresses email, numéros de téléphone,

L'entreprise a été condamnée à payer 35 millions de dollars et a été contrainte d'engager des sommes colossales pour renforcer ses systèmes de sécurité.

[6] Estimation de TV5 Monde

Attaque de WannaCry en 2017

L'attaque de WannaCry a été une cyberattaque mondiale de grande envergure repérée pour la première fois en mai 2017.

Le ransomware WannaCry a infecté plus de 230 000 ordinateurs dans 150 pays.

De nombreuses entreprises ont été contraintes de suspendre leurs activités pendant plusieurs jours, ce qui a entraîné des pertes financières importantes. Des hôpitaux ont également été touchés, ce qui a mis en danger la vie de patients.

Cette attaque aurait fait perdre plus de 4 milliards de dollars à travers le monde.

Attaque de l'hôpital de Dax en 2022

Le 8 février 2022, l'hôpital de Dax a été victime d'une cyberattaque. Il est probable que les pirates informatiques aient utilisé un ransomware pour infecter les systèmes de l'hôpital, qui crypte les fichiers des utilisateurs et exige une rançon pour les déchiffrer. L'hôpital a été contraint d'annuler des opérations chirurgicales et des consultations.

Attaque du Centre Hospitalier Sud Francilien en 2022

Le groupe Lockbit 3.0 a piraté les systèmes informatiques de l'hôpital, chiffrant ses données et exigeant une rançon de plusieurs millions de dollars.

Face au refus de payer, ils ont publié en septembre 2022 sur internet 11 Go de données sensibles dérobées : des numéros de sécurité sociale et des informations médicales de patients.

L'activité de l'hôpital a été fortement perturbée pendant plusieurs semaines. Les systèmes informatiques étant hors d'usage, l'ensemble du personnel a dû se rabattre sur l'utilisation du papier et des crayons pour enregistrer les informations des patients. Une situation qui a considérablement ralenti les opérations hospitalières.

À la suite de cette attaque, le CHSF a renforcé sa sécurité informatique pour éviter de nouveaux incidents. Cet événement met en lumière la vulnérabilité des établissements de santé face aux cybercriminels et la nécessité pour eux d'avoir des plans de réponse solides en cas d'attaque.

Attaque de France Travail en 2024

France Travail (anciennement Pôle Emploi) a été victime d'une cyberattaque massive entre le 6 février et le 5 mars 2024.

Cette attaque a entraîné le vol des données personnelles 43 millions de comptes.

Les données compromises incluent des noms, adresses, numéros de sécurité sociale, dates de naissance, et des informations sur les situations professionnelles.

Cette cyberattaque est l'une des plus importantes jamais subie par une administration française.

CYBERCRIMINALITÉ, LA FIN DE L'INSOUCIANCE NUMÉRIQUE

Après une décennie d'intensification continue de la cybercriminalité, la sophistication des attaques couplée à la généralisation des usages numériques fait craindre une accélération brutale du phénomène. Or l'imminence des JO, événement planétaire unique, cristallise l'attention de nombreux acteurs. Dans ce contexte, les auteurs proposent un état des lieux des menaces et des parades, illustrées par des exemples frappants. L'article décrypte les profils des attaquants et leurs motivations. Les auteurs plaident pour une formation des décideurs et pour une stratégie de sécurité globale fondée sur des stratégies défensives à la fois centralisées et décentralisées, afin de préserver le numérique comme vecteur de croissance, de souveraineté et de liberté.

Par Antoine Duboscq et Timothée Demoures, dirigeants de Wimi (suite collaborative française).

Introduction

Dans le panorama contemporain de la sécurité, la cybercriminalité émerge comme une force prédominante caractérisée par son caractère insidieux et son potentiel de destruction massif. Sous l'égide de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), la surveillance révèle une augmentation régulière des incidents rapportés, témoignant d'une réalité alarmante.

> En 2023, on note +22% sur les piratages de comptes ou encore +30% sur les attaques par rançongiciels[7].

Cette tendance lourde soulève des questions pressantes quant à la préparation et à la résilience de nos infrastructures numériques et de nos organisations face à une menace en expansion et en actuellement en forte mutation.

Or, à l'exception des professionnels des systèmes d'informations et des experts en intelligence économique, l'attitude la plus répandue au sujet de la sécurité numérique est jusqu'à présent, une forme d'insouciance numérique. Bien compréhensible en raison de l'expérience quotidienne du numérique, cette posture passive de nombreux décideurs ne disparaît que lorsqu'une menace se matérialise dans leur quotidien, comme cela se produit de plus en plus souvent.

"Jusqu'ici, l'ANSSI se concentrait sur 500 à 700 acteurs régulés: Etat, acteurs liés à la sûreté nationale, opérateurs d'importance vitale+ et de services essentiels. C'est généralement contre eux que se concentraient les attaques. Mais, désormais, les attaquants pêchent au chalut. Il n'y a plus de particuliers, de PME, de collectivités, d'établissements de santé qui puissent se considérer comme à l'abri. (...) On ne peut plus faire l'impasse sur quoi que ce soit. (...) Nous devons complètement changer d'échelle et de manière de fonctionner pour traiter cette menace de masse."

Vincent Strubel, Directeur Général de l'ANSSI[8]

[7] ANSSI : "Panorama de la cyber menace 2023-2024", février 2024

[8] "Cyberattaques: L'Anssi doit traiter les menaces de masse, selon son patron V. Strubel, avril 2023

Au-delà des chiffres se profilent des récits poignants d'incursions cybernétiques d'envergure, dont les effets résonnent bien au-delà des sphères virtuelles…

Chacun se remémore l'épisode emblématique du piratage réussi des centrifugeuses nucléaires iraniennes, opéré dans le cadre de l'**opération Stuxnet**. Ce cyber-assaut, révélé en 2010 et ayant eu lieu en 2001, non seulement entrava les capacités d'enrichissement d'uranium de l'Iran, mais surtout, incarna une démonstration éloquente de la capacité de l'arme cyber à transgresser les frontières du virtuel pour impacter puissamment le monde tangible.[9]

Aux Etats-Unis, le pipeline Colonial, pilier vital de l'infrastructure énergétique, fut en 2021 la cible d'une attaque : des cybercriminels exploitèrent une faille dans la sécurité informatique de Colonial Pipeline Company, au moyen d'un logiciel malveillant de type ransomware consistant à bloquer l'accès aux systèmes de l'entreprise. Face à cette menace, fut prise la décision difficile de fermer temporairement l'ensemble de son réseau de pipelines afin de prévenir une propagation ultérieure du malware et d'évaluer l'étendue des dégâts. Cette décision entraîna des répercussions immédiates sur l'approvisionnement en carburant de la côte Est des États-Unis. Les consommateurs furent confrontés à des pénuries locales de carburant, des files d'attente interminables dans les stations-service et une flambée des prix de l'essence. Les gouvernements locaux furent contraints de prendre des mesures d'urgence, y compris le rationnement du carburant.[10]

Ainsi, au sein d'une ère numérique en constante évolution, il devient impératif d'appréhender la nature protéiforme des menaces cybernétiques et d'élaborer des stratégies d'atténuation à la hauteur des défis. Pour y contribuer, nous proposons ici une photographie des diverses manifestations de la cybercriminalité, de leurs répercussions dévastatrices et des mécanismes de défense disponibles. Se former est essentiel pour esquisser les contours d'une réponse collective et éclairée, visant à protéger les personnes et les biens, préserver la continuité de l'action de l'Etat et des acteurs économiques, en un mot garantir la pérennité de sociétés toujours plus interconnectées.

Dans cette optique, les deux tableaux ci-dessous se proposent d'examiner les diverses formes de cybercriminalité. Y sont listées menaces, typologie des attaquants et exemples historiques évocateurs.

1/ Les attaques

Pour les décideurs la première étape consiste à se familiariser avec les différents types d'attaques. C'est la raison pour laquelle nous avons conçu ce tableau de synthèse à partir de diverses sources. Le tableau offre une vue panoramique des 10 principales menaces de cybersécurité, regroupées en 4 catégories.

Pour chaque menace, nous indiquons la définition communément admise, les mobiles principaux des attaquants ainsi qu'un exemple, qui peut être approfondi à travers les liens vers les articles sources.

[9] Incyber, janvier 2024
[10] Figaro, mais 2021

Catégories	Menace	Définition	Mobiles	Exemple
Attaques ciblant la sécurité des données	Hameçonnage	Méthode d'attaque où les cybercriminels se font passer pour des entités légitimes (via courriels, SMS…) pour inciter à divulguer des informations sensibles ou à effectuer des actions nuisibles.	Gain financier Impact politique Activisme	Attaque de Nordea (2017). Des emails frauduleux ont incité les clients à installer un prétendu anti-spam, qui en réalité contenait le cheval de Troie "haxdoor", enregistrant les frappes clavier et redirigeant vers un faux site bancaire pour voler les identifiants de connexion.
	Attaque par mot de passe	Obtenir les mots de passe des utilisateurs pour compromettre leurs comptes et accéder à des informations sensibles, utilisant des techniques telles que l'ingénierie sociale et la surveillance du trafic réseau	Gain financier Espionnage industriel Espionnage étatique Notoriété, défi	Attaque de LinkedIn (2012). 100 millions de mots de passe d'utilisateurs ont été piratés. Ils étaient stockés sous forme de hashes SHA-1, méthode de cryptage sans salage, vulnérable à des attaques par force brute et à techniques de déchiffrement.
	Attaque de l'homme au milieu	Un pirate informatique s'insère dans les communications entre un client et un serveur afin de voler des informations sensibles, telles que le détournement de session.	Gain financier	KRACK (Key Reinstallation Attacks) en 2017, affectait le protocole de sécurité WPA2, utilisé par la majorité des réseaux Wi-Fi. Cette faille permettait aux attaquants d'intercepter les communications entre les appareils des utilisateurs et le routeur Wi-Fi, même si ces communications étaient cryptées.
	Rançongiciel	Un logiciel malveillant qui chiffre les données de l'utilisateur ou bloque l'accès à son appareil en échange d'une rançon.	Gain financier Impact politique Activisme Sabotage Acte de guerre cyber Notoriété, défi	Attaque du Colonial Pipeline (2021). Le rançongiciel DarkSide a paralysé l'un des plus grands pipelines de carburant aux Etats-Unis. 100 Go de données ont été volées, conduisant à un paiement de 5 millions USD pour récupérer l'accès aux données et rétablir le service.
Logiciels malveillants et programmes nuisibles	Infection par un malware	La contamination d'un système informatique par un logiciel malveillant conçu pour perturber son fonctionnement et voler des informations sensibles.	Espionnage industriel Espionnage étatique Idéologie politique Sabotage Guerre Cybernétique Notoriété, défi	NotPetya (2017) a ciblé des entreprises en Ukraine, mais il s'est rapidement propagé dans le monde. Le malware, déguisé en une mise à jour de logiciel de comptabilité populaire, a utilisé des outils de cyberespionnage russes pour se propager, détruisant les données des ordinateurs ciblés et provoquant des perturbations et pertes financières massives.
	Attaque par téléchargement furtif	Consiste à diffuser un logiciel malveillant en exploitant les vulnérabilités des plateformes web et des systèmes d'exploitation, sans nécessiter d'action de la part de l'utilisateur.	Espionnage industriel Espionnage étatique Sabotage Notoriété, défi	En 2021, des chercheurs en cyber-sécurité ont révélé que de faux téléchargements d'applications mobiles (ex : Viber, WeChat ou BattleField) téléchargeaient des logiciels malveillants, volant les mots de passe, créent des portes dérobées et enregistrant les activités de l'écran de l'utilisateur.
Attaques sur la disponibilité et l'intégrité du service	Attaque en déni de service (DDoS)	Vise à perturber les services d'une entreprise en saturant son infrastructure informatique de trafic web malveillant, entraînant des interruptions de service et des répercussions négatives.	Espionnage industriel Espionnage étatique Impact politique Activisme Sabotage Guerre Cybernétique Notoriété, défi	Attaque contre un client anonyme d'AWS (Amazon Web Services) en 2020. Une attaque DDoS a amplifié les données envoyées via CLDAP à la victime jusqu'à 70 fois, atteignant un pic de 2,3 téraoctets par seconde sur 3 jours, l'une des attaques les plus massives connues.

Escroqueries et ingénierie sociale	Arnaque au président	Une forme d'attaque où un escroc se fait passer pour un dirigeant d'entreprise afin de tromper les employés en leur faisant divulguer des informations confidentielles ou en les incitants à effectuer des actions nuisibles.	Gain financier Espionnage industriel Espionnage étatique	En 2023, une entreprise de région parisienne a été victime d'une arnaque au "faux président", dans laquelle les escrocs ont obtenu des virements de 38 millions d'euros.
	Le faux conseiller bancaire	Envoi d'e-mails prétendant signaler une activité suspecte sur le compte bancaire de la victime, incitant à appeler un faux conseiller bancaire qui tente de soutirer des informations personnelles pour vider les comptes.	Gain financier	En France, les arnaques au faux conseillé bancaire ont augmenté de 78% en 2023 vs 2022 atteignant 5,000 signalements. La Banque de France rapporte que 628 millions d'euros ont été volés aux victimes de fraudes au paiement sur T1 2023.
	Attaque par écoute illicite	Intercepter le trafic réseau pour obtenir des informations confidentielles, comme des mots de passe ou des données de paiement.	Espionnage industriel Espionnage étatique Guerre Cybernétique	En 2015, plus de 25,000 applications iOS ont été exposées à des attaques par écoute à cause d'un bug dans la bibliothèque de code source ouverte AFNetworking. Ce bug permettait de désactiver le chiffrement HTTPS, exposant les utilisateurs à des risques d'interception de données. [1]

2/ Les attaquants

Les attaquants sont divers par leurs profils, leurs mobiles et leurs moyens. Nous offrons ici une typologie qui synthétise le point de vue des experts sur ce sujet. A noter, les frontières entre profils sont parfois floues, avec des acteurs 'entre-deux'. Par ailleurs, certains acteurs agissent sous faux-drapeau, par exemple pour masquer des mobiles étatiques.

La professionnalisation des attaquants

La professionnalisation croissante des cyberattaquants se manifeste par l'adoption de structures organisationnelles similaires à celles des entreprises conventionnelles. Leurs structures se dotent ainsi de départements dédiés à la recherche et développement, aux ressources humaines et au juridique. Cette évolution témoigne de la hausse des profits, illustrée par l'augmentation du nombre et surtout du montant moyen des rançons que les organisations cibles sont prêtes à verser pour récupérer leurs données.

> En 2023, selon le rapport de Sophos effectué sur 14 pays[11], la proportion des rançons supérieures à 1 million de dollars atteint 40%, comparée à 11% l'année précédente.

S'agissant des secteurs et les pays les plus touchés, selon "l'Office of the Director of US National Intelligence" , la recherche de profit guide la stratégie des attaquants, qui privilégient des secteurs comme la défense, les administrations et la communication, ainsi que les régions Amérique du Nord (72% des attaques) et Europe (66%)[12].

[11] SCMAFAZINE, août 2023

[12] Office of the director of us national intelligence, octobre 2023

Typologie des attaquants	Définition	Mobiles	Exemple
Hackers Éthiques	Souvent appelés "white hats", ces cyberattaquants utilisent leurs compétences pour améliorer la sécurité des systèmes informatiques. Ils identifient les vulnérabilités et aident les organisations à les corriger avant que des acteurs malveillants ne les exploitent.	Notoriété, défi Espionnage industriel Espionnage étatique	Créé en 2014, le « projet Zero » de Google est une équipe de sécurité dédiée à trouver des vulnérabilités dans divers logiciels, y compris ceux d'autres entreprises. A ces débuts, cette équipe en a notamment découvert une série sur Windows et a averti Microsoft de la vulnérabilité.
Cybercriminels	Ce groupe utilise ses compétences pour des gains financiers illégaux. Cela peut inclure le vol d'identités, l'accès frauduleux à des comptes bancaires, ou encore la distribution de logiciels malveillants contre rançon ("rançongiciel").	Gain financier Espionnage industriel Espionnage étatique	En mai 2021, Colonial Pipeline, opérateur d'un des plus grands réseaux de pipelines aux Etats-Unis, a été visé par une attaque de rançongiciel orchestrée par DarkSide, un groupe de cybercriminels organisé. Cette cyberattaque a causé l'arrêt temporaire de l'acheminement de carburant, provoquant des pénuries d'essence, de diesel et de kérosène sur la côte Est américaine. Face à cette urgence, Colonial Pipeline a payé une rançon de 5 millions de dollars pour restaurer ses opérations.
Hacktivistes	Les hacktivistes sont motivés par des convictions politiques ou sociales. Ils ciblent souvent des gouvernements, des entreprises ou des organisations qu'ils considèrent comme contraires à leurs valeurs, utilisant leurs attaques pour protester ou faire passer un message.	Impact politique Activisme	En 2012, le président de la République française a loué la fermeture par le FBI des sites de téléchargement et de streaming de Megaupload. En réaction, le collectif de hackers Anonymous a rapidement lancé des représailles contre des sites français. Le site de la présidence, Elysee.fr, a été la première cible, affichant le slogan « We are legion » des pirates.
Espions Etatiques	Ces acteurs sont parrainés par des États et visent à voler des secrets industriels ou des informations gouvernementales sensibles pour avantager leur pays d'origine sur la scène mondiale.	Espionnage industriel ou gouvernemental Sabotage Guerre Cybernétique	L'attaque Stuxnet, révélée en 2010, a ciblé les centrifugeuses d'enrichissement d'uranium de l'Iran, utilisant un ver informatique sophistiqué. Ce malware, présumé développé par les États-Unis et Israël, était programmé pour perturber les systèmes de contrôle Siemens des centrifugeuses. Il modifiait les vitesses de rotation, causant leur défaillance et destruction progressive, afin de retarder le programme nucléaire iranien.
Cyber-terroristes	Ce type de cyberattaquants cherche à créer de la peur et du chaos, souvent pour des motifs idéologiques. Leurs cibles incluent les infrastructures critiques, les réseaux de communication, et les bases de données gouvernementales.	Sabotage Guerre Cybernétique	En avril 2015, la chaîne de télévision française TV5 Monde fut la cible d'une cyberattaque majeure par un groupe se réclamant de l'État islamique. L'attaque perturba la diffusion de la chaîne, mettant hors service ses émissions pendant plusieurs heures, en plus de compromettre ses sites web et comptes de réseaux sociaux. Les pirates publièrent des messages menaçants et du contenu de propagande djihadiste.

Un stratagème puissant : les attaques "dormantes"

Une augmentation significative des cyberattaques d'origine étatique, notamment celles qualifiées de "dormantes", est observée au cours des cinq dernières années selon les données de l'Atlas 2022 de Thalès[13]. Avec ce procédé d'attaque, les cybercriminels implantent discrètement un logiciel malveillant dans le système d'information de l'entité ciblée, pour accéder aux données depuis l'extérieur sans être détectés. Ce stratagème est en particulier prisé pour la mise en place d'opérations d'espionnage à long terme, en

[13] Thales, 2022

visant des dommages élevés. Les attaques dormantes peuvent se dérouler sur des périodes prolongées allant de deux ans à plus d'une décennie. Elles sont favorisées par un contexte d'intégration croissante entre les États et certaines entreprises privées.

Les attaquants s'adaptent…

Parallèlement à leur professionnalisation, les attaquants évoluent constamment pour s'adapter aux parades et identifier de nouvelles opportunités. Parmi les facteurs clés de leur évolution : l'extension des commanditaires, les nouvelles possibilités technologiques, l'identification de nouveaux segments de victimes, les évolutions des politiques de sécurité et des comportements.

L'article de McKinsey & Company[14] et le résumé entre autres de Simplilearn fournissent une synthèse intéressante des facteurs d'évolution du côté des attaquants :

Avancées technologiques : L'introduction de nouvelles technologies, matérielles ou logicielles, crée de nouvelles vulnérabilités, qui facilitent le contournement des défenses existantes, le temps que celles-ci mûrissent et s'adaptent. Par exemple, l'essor de l'internet des objets (IoT) a ouvert de nouvelles portes pour les attaques ciblant des appareils connectés mal sécurisés.

Adaptation aux mesures de sécurité : Face à des mesures de sécurité plus sophistiquées, les cyberattaquants innovent pour les contourner, notamment par l'exploitation de failles zero-day (encore non corrigées) et l'utilisation de techniques avancées de persistance et d'évasion.

Diversification des motivations : Si historiquement, beaucoup d'attaques étaient motivées par le gain financier direct, aujourd'hui les motivations incluent l'espionnage industriel, la guerre informatique entre États, le militantisme (hacktivisme) ou simplement la recherche de notoriété, comme l'illustre notre tableau plus haut.

Évolution de la législation et des politiques publiques : Les changements dans les réglementations poussent les cyberattaquants à modifier leurs approches. Par exemple, le renforcement des lois sur la protection des données personnelles (RGPD en Europe) entraîne la mise au point de méthodes plus sophistiquées de vol d'informations.

Armes cyber clés en mains : Le 'dark web' offre des outils et services de cyberattaque "clés en main", permettant à des individus sans compétences techniques avancées de lancer leurs attaques. Ce phénomène élargit le profil et le nombre des attaquants.

Conflits internationaux : De tactiques, les cyberattaques sont devenues également des outils de nature stratégique. Dans les rapports de force géopolitiques, les cybermenaces influencent, déstabilisent, recueillent des renseignements visant d'autres nations ou groupes politiques essentiels. Dans une guerre hybride, le champ cyber offre de nouvelles potentialités d'attaque, pour frapper les lignes arrières, décrédibiliser un adversaire, créer des dommages sans avoir à déclarer des hostilités ouvertes.

[14] Mckinsey & Company, mars 2022

3/ Intelligence Artificielle, quels impacts ?

L'intégration de l'intelligence artificielle dans le domaine de la cybersécurité implique autant les méthodes de défense que d'attaque. Pour les défenseurs, des outils émergent (détection améliorée des menaces, réponses automatiques, anticipation...) mais dans l'immédiat ce sont avant tout de nouveaux risques à prendre en compte (malware plus intelligents, automatisation des attaques, exploitation des biais de l'IA, baisse de l'amateurisme dans la syntaxe verbale ...)[15][16][17]. Parmi les cas d'emploi malveillants de l'IA, sont évoqués par Cybermalveillance.gouv.fr, incubé par l'ANSSI, *"des hypertrucages (deepfakes) audio, vidéo ou photo visant à détourner l'image de célébrités à des fins d'escroquerie, des personnalités politiques à des fins de manipulation de l'opinion, ou encore de cyberharcèlement à caractère pornographique..."*.

4/ Les parades

Le spectre des parades est extrêmement large : composants, architectures physiques, couches bases logicielles, logiciels de surveillance, chiffrement... Impossible de les lister ici. L'Europe à elle seule compte environ 60 000 entreprises et 660 centres d'expertise en cybersécurité.

Cependant pour les décideurs généralistes, non experts en SI, nous proposons ici une vue générale de 4 grands types de mesures défensives employées au sein des grandes organisations, publiques ou privées.

Diagnostic de l'état de santé numérique

Le point clé consiste ici dans l'identification des vulnérabilités. Les audits réguliers, les 'pain tests', 'hackathons' et les simulations 'war-game' font partie de la panoplie des outils.

Sensibilisation des collaborateurs

Les mesures consistent en formations, diffusions de bonnes pratiques[18], dispositifs pour recueillir les signes d'alertes et la prise en compte en amont de la cybersécurité dans les phases de conception des projets de l'organisation. Les moyens abondent pour stimuler une 'hygiène de vie cyber' : jeux, tests en conditions réelles, voire sanctions amicales pour les négligents – par exemple les fameux écrans "retournés", ou les "je paye les croissants demain à tout le monde", tapés sur l'ordinateur resté malencontreusement ouvert…

Veille cyber

La veille porte sur les flux numériques internes, et se nourrit par des sources spécialisées telles que les organismes gouvernementaux, certains fournisseurs et des experts spécialisées en cybersécurité, mais aussi sur la surveillance des réseaux sociaux et blogs pour repérer des menaces émergentes pour l'acteur concerné. Les RSSI (Responsables de la sécurité des systèmes d'information) jouent un rôle croissant dans les organisations ; des RSSI mutualisés apparaissent pour les PME / TPE.

Élaboration d'un PRA / PCA

Le PRA (Plan de reprise d'activité) et le PCA (Plan de continuité d'activité) permettent d'assurer une gestion efficace des cyberattaques

[15] Pluralsight, novembre 2023
[16] Cloud security alliance, mars 2024
[17] World economic forum, juin 2023
[18] Kit de sensibilisation aux risques numériques, 2019

en période de crise effective. Ces plans doivent inclure des mesures claires sur la manière d'agir en cas d'incident, telles que la désignation des responsables, la sensibilisation de l'équipe aux cybermenaces et la définition d'un protocole de communication pour informer les parties prenantes en cas de violation de données. Il est également crucial de tester régulièrement les systèmes et de souscrire à une cyber-assurance pour couvrir les éventuelles pertes financières causées par une attaque.

A ces mesures, viennent s'ajouter à l'étage supérieur des réponses de politique publique. Parmi les outils réglementaires mis en avant par les régulateurs, il n'est pas inutile de connaître l'existence des cinq suivants :

Qualification SecNumCloud

Établie par l'ANSSI (France), cette norme est destinée à assurer la sécurité des services de cloud computing (SaaS, IaaS, PaaS). Cette norme garantit que les fournisseurs de services cloud respectent des exigences strictes en matière de protection des données, de processus de recrutement, de résilience et de disponibilité des services, afin de protéger les infrastructures critiques et les données sensibles hébergées.[19]

Loi SREN

La loi Française SREN (Sécurisation et Régulation de l'Espace Numérique), votée en première lecture (Assemblée Nationale et Sénat) en octobre 2023, vise à encadrer plus strictement l'espace numérique en France, notamment pour la protection des mineurs en ligne et la lutte contre les contenus illicites sur les réseaux sociaux. Elle introduit des obligations de modération pour les plateformes, des sanctions pour la diffusion de deepfakes sans consentement, et renforce le contrôle sur l'accès aux sites pornographiques par la vérification obligatoire de l'âge des utilisateurs. La loi prévoit des peines de bannissement des réseaux sociaux pour les cyberharceleurs et augmente les amendes pour les infractions numériques graves.[20]

Certification EUCS (European Union Cloud Services) : L'EUCS est un projet de certification de l'Union européenne visant à harmoniser les normes de sécurité pour les services cloud à travers les États membres. Cette initiative vise à renforcer la confiance dans les services cloud en établissant des critères clairs de sécurité et de protection des données, facilitant ainsi leur adoption sécurisée par les entreprises et les organismes publics européens.[21]

Règlement DORA (Digital Operational Resilience Act) : DORA est un règlement proposé par l'Union européenne pour renforcer la résilience opérationnelle numérique des entités du secteur financier. Ce cadre réglementaire oblige les entreprises à établir des mesures robustes pour prévenir, atténuer et gérer les risques liés aux TIC (Technologies de l'information et de la communication), incluant des exigences strictes sur la gestion des incidents cybernétiques et la surveillance continue des menaces. À partir de janvier 2025, cette réglementation s'appliquera aux 27 États membres de l'Union européenne[22].

[19] ANSSI, septembre 2023

[20] L'Express, octobre 2023

[21] It for business, avril 2024

[22] Incyber, août 2023

Directive NIS 2 (Network and Information Security, version 2) : Succédant à la directive NIS, NIS 2 est une mise à jour significative qui élargit les exigences de sécurité et de notification des incidents pour les opérateurs essentiels (anciennement OIV et OSE en France) et les fournisseurs de services numériques. Elle vise à améliorer la coopération entre les États membres sur la cybersécurité, renforcer la sécurité des réseaux et des systèmes d'information. NIS 2 devrait entrer en application dans le droit national à partir d'octobre 2024.[23]

Par ailleurs, impulsé par les politiques publiques, l'écosystème de la cybersécurité en France connaît un développement notable, exacerbé par la pandémie de COVID-19 et l'augmentation notoire de données sensibles stockées sur le cloud. Ainsi, l'ANSSI a rapporté une escalade de 255% des incidents de sécurité en 2020[24], et cette tendance n'a pas fléchi les années suivantes. Ce focus permet de mettre en lumière les différentes strates d'évolution au sein de ce secteur crucial en France :

Plan d'investissement stratégique : l'État français a mis sur la table en 2021 1 milliard d'euros[25] pour soutenir l'innovation technologique, sécuriser les infrastructures critiques et stimuler l'économie numérique sécurisée.

Éducation : Création de programmes spécialisés dans des institutions de formation (ex : nouveaux programmes à l'École Polytechnique[26] ou création du Master cyberdéfense à l'École Hexagone[27]). Ces initiatives répondent à une pénurie de compétences, avec un secteur qui manque déjà au niveau mondial 4 millions de professionnels qualifiés selon l'étude *"Cybersecurity Workforce Study"*, réalisée par l'ISC2 fin 2023.[28]

Financements privés : L'évaluation menée par Wavestone en 2023 révèle un fort dynamisme du secteur[29], avec une augmentation des levées de fonds de +35% en France(**55**), dans un contexte de financement pourtant difficile pour l'innovation. La multiplication des salons de cybersécurité comme InCyber (FIC), les assises de la cybersécurité, la European Cyber Week, le Paris Cyber Show... n'en sont que le reflet.

Pôles d'excellence : Le Campus Cyber, inauguré en 2021 à la Défense, est devenu un pôle collaboratif réunissant plus de 160 entités[30], combinant les efforts de l'industrie, de l'académie et du secteur public. Aussi, pour maximiser leurs synergies, les industriels se structurent en groupements et associations professionnelles (ex : Hexatrust , l'Open Internet Project ou le GINUM).

Coopération internationale : La France a intensifié ses efforts et participe à des initiatives européennes et mondiales pour renforcer les capacités de réponse[31], permettant d'élaborer des normes et pratiques communes.

[23] ANSSI, juin 2023
[24] CERT-FR, octobre 2021
[25] Economie.gouv, février 2022
[26] Ecole Polytechnique, janvier 2024
[27] Le Monde Informatique, janvier 2022
[28] Le monde informatique, novembre 2023
[29] Le Monde Informatique, juin 2023
[30] Maddyness, février 2022
[31] France Diplomatie, janvier 2022

5/ Centralisation vs décentralisation des réponses :

Le choix entre centralisation et décentralisation des réponses aux menaces cybernétiques, tant au niveau des organisations que des politiques publiques, ne se limite pas à une opposition binaire, mais plutôt à une décision stratégique qui dépend de plusieurs facteurs : la taille et la structure de l'organisation, la nature des informations manipulées, la réglementation en vigueur et le budget alloué à la cybersécurité. Par exemple, une grande entreprise multinationale pourrait bénéficier d'une approche hybride, avec un SOC central (Centre Opérationnel de Sécurité), des politiques de sécurité[32] adaptées localement dans ses différentes filiales et l'intervention de hackers éthiques[33], tout en se conformant aux réglementations en vigueur et aux conseils d'une structure centralisée telle que l'ANSSI.

6/ Enjeux de guerre économique

D'après Charlotte Pillard Pouget, de l'Ecole de Guerre économique (EGE), la rivalité entre les États-Unis et la Chine dans le domaine de la technologie, notamment en ce qui concerne le déploiement de la 5G, a évolué en une forme de guerre technologique et économique. Par exemple, en 2018-2019 par crainte d'espionnage et de cyberattaques potentielles de la part de la Chine, l'administration Trump a interdit le marché de la 5G au géant chinois de l'électronique, Huawei, étendant ainsi le conflit au-delà du domaine commercial pour protéger les données sensibles américaines.[34]

Cette rivalité met en lumière la question cruciale de la dépendance technologique dans un monde marqué par des tensions géopolitiques croissantes. Le numérique, autrefois perçu comme une innovation stimulant le consumérisme et ouvrant de nouvelles perspectives de marché, est désormais considéré comme un élément vital pour assurer le développement d'un pays de manière autonome, sans dépendre de processus de soumission à des acteurs étrangers. Ainsi, concept datant pourtant du début des années 2000, la "souveraineté numérique" refait surface.

En effet, la législation américaine avec le trio Patriot Act, FISA section 702, Cloud Act, présente des implications significatives pour la protection des données[35] pour les entreprises européennes ayant des activités, des données aux États-Unis ou utilisant des services américains. Cela concerne donc "presque" toutes les organisations publiques et privées européennes.

Patriot Act (2001)

Permet au FBI d'accéder sans mandat judiciaire aux données détenues par ces entreprises ou leurs prestataires, même si leur siège social est situé en Europe.

FISA (Foreign Intelligence Surveillance Act) section 702 (2008)

Autorise la collecte de renseignements sur les communications électroniques de personnes étrangères situées à l'extérieur des États-Unis, dans le but de recueillir des renseignements en matière de sécurité nationale. Cette disposition a été promulguée et prolongée en avril 2024

[32] Insight, novembre 2022
[33] France Info, janvier 2022
[34] Ecole de la guerre Économique, mars 2023
[35] Cyber Management School, avril 2024

pour permettre aux agences de renseignement, (NSA, CIA, FBI entre autres), de collecter des données sans avoir besoin d'un mandat spécifique pour chaque cible.

Cloud Act (2018)

Modernise les lois sur la surveillance et le stockage des données à l'ère du cloud computing. Il autorise les agences gouvernementales américaines à accéder aux données stockées sur des serveurs cloud partout dans le monde.

Cette confrontation entre ces dispositions légales américaines et les réglementations européenne et nationales, (ex : RGPD), soulève des défis pour les entreprises opérant en Europe. Elles doivent non seulement naviguer entre le risque d'utilisation effective et non visible de ces textes, mais aussi être en conformité vis-à-vis des normes européennes en matière de protection des données. Cela nécessite souvent des adaptations et une nouvelle forme de complexité : évaluation des zones de conflits entre les législations, choix entre logiciels souverains et non-souverains (en fonction de la criticité des données), échanges de conformité versus enjeux de productivité entre DSI (Directeur des Systèmes d'Information), RSSI (Responsable de la Sécurité des Systèmes d'Information), DPO (Data Protection Officer), départements juridiques, directions générales, et directions métiers.

La souveraineté numérique émerge comme une réponse stratégique face aux menaces posées par ces législations. Les États européens cherchent à garantir un contrôle accru sur leurs données sensibles et à réduire leur dépendance vis-à-vis des fournisseurs de services numériques basés aux États-Unis. Les français sont d'ailleurs à 86% pour des mesures d'achat de souveraineté numérique, d'après l'étude WIMI-IPSOS (2021).[36] Cela implique de promouvoir le développement de solutions technologiques et de services numériques français et européens avec une coloration forte en cybersécurité (ex : SecNumCloud, EUCS..). Cela permettrait aux organisations européennes de mieux se protéger des fuites de données, tout en préservant leur autonomie et leur compétitivité sur la scène mondiale. De plus, en favorisant la coopération entre les acteurs publics et privés au niveau national et européen, les démarches de souveraineté numérique permettent de partager les informations en circuit court, et ainsi avoir une meilleure efficacité dans les réponses aux menaces cyber.

Conclusion

Avec près de 450 millions de tentatives de cyberattaques tentés sur l'infrastructure des Jeux Olympiques (JO) 2020 à Tokyo, les JO sont devenus une cible privilégiée par les cybercriminels (x 2.5 par rapport à l'édition de 2012 à Londres).

Dans le contexte géopolitique et technologique actuel (guerre en Ukraine, arrivée de l'IA, informatisation croissante des systèmes...) les JO 2024 à Paris constituent donc un événement d'envergure susceptible d'attirer encore plus d'attaques ; environ "huit à dix fois plus" d'après le directeur de la technologie de Paris 2024, Bruno Marie-Rose. De surcroît, l'inquiétude est d'autant plus forte que les autorités craignent un passage cyberattaque "avec des dégâts matériels à une cyberattaque qui entraînerait des morts ou des blessés" selon Johanna Brousse, cheffe de la section

[36] WIMI, décembre 2021

spécialisée dans la lutte contre la cybercriminalité au parquet de Paris.

Les autorités françaises, l'ANSSI au premier rang, sont sur le qui-vive pour protéger les systèmes informatiques essentiels qui gèrent les transports, l'énergie, la sécurité, et les communications, cruciaux pour le déroulement de l'événement.[37] 350 entités sont pilotés par l'ANSSI, dont 80 critiques[38]. La sécurisation des données personnelles des milliers de visiteurs est également capitale pour prévenir les risques de fraude et d'usurpation d'identité dans le cas de tentatives d'attaques terroristes. Par ailleurs, les plateformes de diffusion des jeux sont des cibles potentielles pour des attaques par dénis de service (DdoS, voir définition plus haut), qui pourraient perturber la transmission des compétitions (ex : le chrono qui s'arrête en finale du 100m, une piscine olympique plongée dans le noir, des accès aux enceintes perturbés...) et donc la réputation de la France à l'international.

"On s'attend à ce que ce soit considérable", déclarait à l'AFP le général Christophe HUSSON, à la tête du ComCyber-MI (Gendarmerie, poussant par exemple l'ANSSI à lancer un kit d'exercice prêt à l'emploi pour les entreprises, pour se préparer à une crise cyber.[39]

Nous espérons que cet article, qui a eu comme objectif de synthétiser les menaces, les parades et les enjeux de cybersécurité actuels, aura éclairé et contribuera à passer le cap pour préparer le changement d'échelle du champ de bataille qui s'ouvre devant nous.

[37] Le Figaro, mars 2024
[38] Strategies, janvier 2024
[39] Le Monde Informatique, décembre 20

Antoine Duboscq et **Timothée Demoures**, sont respectivement Président et Chief Of Staff de Wimi, suite collaborative **sécurisée** et **souveraine**.



La mission de Wimi est de constituer l'**alternative** souveraine pour la collaboration numérique autour de projets sensibles. Fondée il y a 12 ans, l'entreprise française est notamment **lauréate French Tech 2030**, et **sélectionnée dans le plan de relance France 2030**.

Wimi offre une couverture fonctionnelle large : *espaces de travail, documents & drive, réseau social interne, emails, chat & channels, tâches & Gantt, agendas & réunions, appels vidéos, signature électronique, reporting & activités, chiffrement de bout-en-bout, tatouage numérique, MFA.* La suite Wimi est déployée auprès de **milliers d'organisations** : ministères, collectivités, entreprises, ONG. Parmi ceux-ci, l'Assemblée Nationale, le SIG (Service d'Information du Gouvernement), Vinci Construction, la Fédération Française de Rugby, des laboratoires CNRS...



La plateforme Wimi dispose de sa propre infrastructure, sécurisée en suivant les recommandations de l'**ANSSI** et d'experts en cybersécurité. Wimi vise une qualification SecNumCloud ANSSI en 2024, et propose en **partenariat avec Thalès** une offre DR ('Diffusion Restreinte').

POUR EN SAVOIR PLUS SUR WIMI

L'ÉTAT FACE À LA CYBERCRIMINALITÉ

Il y a 15 ans la cybercriminalité était réservée à des personnes connaissant l'informatique et aux initiés. Les actes de cybercriminalité se limitaient principalement à des défigurations de site internet, des attaques par déni de service et des vols de données. L'arrivée des smartphones, la numérisation des services et la popularisation d'internet ont fortement contribué à la prolifération de nouvelles formes de cybercriminalité. L'État a dû réagir et s'organiser pour lutter contre toute menace.

Contributeur anonymisé à sa demande. Il est investigateur cybercriminalité.

La cybercriminalité, nouvel enjeux national

Un cybercrime est une activité illégale menée à l'aide d'appareils ou de réseaux informatiques. Ces activités impliquent l'utilisation de la technologie pour commettre des fraudes, des vols d'identité, des vols de données, des escroqueries, des extorsions, diffuser des virus, etc.

L'arrivée des smartphones, la numérisation des services et l'internet pour tous ont été un tournant dans l'augmentation de la cybercriminalité offrant des possibilités infinies en termes d'attaque et des nouvelles formes de cybercriminalité (HackTivisime, BotNet, Rançongiciel, phishing sophistiqué, smishing, etc.).

Déployer un site internet est à la portée de n'importe qui. Les hébergeurs web encore peu nombreux il y a 15-20 ans sont une infinité aujourd'hui. N'importe qui peut devenir hébergeur web moyennant un petit investissement.
La cybercriminalité qui n'était qu'une délinquance de niche est devenue un enjeu majeur pour les États.

En France, on dénombre près de 330 000 attaques réussies en 2022 sur des PME et 17 000 contre les grands groupes et ETI.

Les acteurs de la lutte contre la cybercriminalité en France

Depuis 15 ans, plusieurs séries de mesures ont permis la création de structures d'État spécialisées dans la lutte contre la cybercriminalité (ANSSI, COM CYBER, OFAC, etc.).

Les tribunaux judiciaires

Chaque parquet est indépendant, mais pour répondre efficacement à la cybercriminalité, un parquet spécialisé et ayant une compétence nationale a été créé au Tribunal de Paris : J3, anciennement F1.
Cette section cybercriminalité est intégrée à la troisième section, celle qui traite les affaires relevant de la juridiction interrégionale spécialisée (JIRS) ou de la juridiction nationale de lutte contre la criminalité organisée (Junalco). Cela concerne les affaires d'une grande complexité dans les domaines de la criminalité organisée et financière.

Grâce à sa compétence nationale, la section J3 est habilitée à traiter les affaires de cybercriminalité complexes, quelle que soit leur localisation sur le territoire national. Les parquets locaux, quant à eux, conservent leur compétence pour le reste des affaires de cybercriminalité. La section J3 est seule compétente pour les infractions commises dans le ressort du tribunal judiciaire de Paris.
En pratique, la section J3 exerce sa compétence nationale dans les quatre cas suivants :

- Pluralité d'auteurs ou de victimes sur le territoire : afin d'éviter la multiplication d'enquêtes parallèles par plusieurs parquets locaux.
- Dimension internationale importante de l'affaire : la section J3 dispose d'une expertise avérée en matière de procédures de coopération judiciaire européenne et internationale.
- Technicité ou complexité du mode opératoire : l'affaire requiert des compétences spécialisées que la section J3 est en mesure de mobiliser.
- Qualité de la victime : lorsqu'il s'agit d'un opérateur d'importance vitale, d'un ministère ou d'un sous-traitant de l'armement, par exemple.

Néanmoins, pour répondre à la technicité et à la complexité croissantes des dossiers cyber, chaque parquet s'équipe de plus en plus de magistrats référents cyber et d'assistants spécialisés en cybercriminalité.

L'office anti-cybercriminalité (OFAC)

Créé en 2023 et implanté à Nanterre, cet office est chargé, d'une part, du traitement des attaques cyber à l'encontre des systèmes informatiques et des activités illicites sur le darkweb sur l'ensemble du territoire national. D'autre part, il assure le pilotage et l'animation du plan national cyber, impliquant l'ensemble des acteurs concernés (police, gendarmerie...).

Sont rattachées à cet office la plateforme Pharos, dédiée au signalement des contenus illicites sur internet, et la plateforme Thésée, permettant le recueil de plaintes en ligne pour certaines escroqueries commises sur internet.

La police (Paris et petite couronne)

La préfecture de police de Paris dispose de plusieurs services spécialisés dans la lutte contre la cybercriminalité, compétents pour les infractions commises sur le territoire de Paris et de la petite couronne (Hauts-de-Seine, Seine-Saint-Denis et Val-de-Marne).

Voici les principaux services compétents :

- La Brigade de lutte contre la cybercriminalité (BL2C) est chargée d'enquêter sur les infractions liées aux STAD (Système de traitement automatisé de données) , telles que les vols de données informatiques, les intrusions dans des systèmes informatiques et les attaques par déni de service. Elle dispose en son sein de plusieurs groupes :
    - Deux groupes généralistes dédiés aux différentes formes de piratage (vol de données, piratage avec par la suite une escroquerie/extorsion...)
    - Un groupe dédié au rançongiciel
    - Un groupe de Cyberpatrouilleurs

- Un LION (Laboratoire d'investigation opérationnelle du numérique)

- Brigade de protection des mineurs (groupe internet) : Ce groupe est spécialisé dans la lutte contre les infractions à caractère sexuel commises sur internet, telles que la diffusion d'images et de vidéos à caractère pédopornographique, le proxénétisme d'enfants et la sollicitation d'enfants à des fins sexuelles.
- Moyens de paiement : La brigade des fraudes aux moyens de paiement est chargée d'enquêter sur les infractions liées aux moyens de paiement, telles que l'utilisation frauduleuse de cartes bancaires, les piratages de comptes bancaires et les escroqueries en ligne.

En province

La France compte environ 430 investigateurs spécialisés en cybercriminalité (ICC), répartis sur l'ensemble du territoire national. En plus de ces ICC, les forces de l'ordre disposent également d'enquêteurs généralistes formés aux techniques d'investigation cyber.

Ces investigateurs bénéficient du soutien d'un réseau d'antennes de l'Office anti-cybercriminalité (OFAC) disséminées dans toute la France. Ces antennes apportent une assistance technique et opérationnelle aux enquêteurs locaux lorsqu'elle s'avère nécessaire.

La gendarmerie

Le pôle spécialisé Enquête judiciaires nationales : centre de lutte contre les criminalités numériques (C3N). Le C3N est l'autorité centrale de la gendarmerie en matière de cybercriminalité. Il est chargé d'enquêter sur les affaires de grande envergure et complexes qui requièrent des compétences techniques pointues.

Et au niveau local, 260 enquêteurs NTECH en France et des enquêteurs spécialisés.

La DGSI

La lutte contre le terrorisme, l'ingérence étrangère et les menaces radicales est confiée à la Direction générale de la sécurité intérieure (DGSI).

En plus de cette mission principale, la DGSI est également chargée des enquêtes judiciaires dont sont victimes l'État, les opérateurs d'importance vitale et certaines entreprises.

D'autres acteurs

Il existe également plusieurs services en charge de la cybercriminalité mais attaché au ministère de l'Économie :

1. DOUANE (DNRED)
2. TRACFIN
3. DGCCRF (SNE)

En Europe : EUROPOL

Europol est une agence européenne de police criminelle qui facilite l'échange de renseignements entre polices nationales en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédocriminalité au sein de l'Union européenne.

Face au développement des nouvelles menaces Europol est également devenu un acteur de la lutte contre la cybercriminalité à travers le **Centre européen de lutte contre la cybercriminalité européenne**.

L'auteur est investigateur cybercriminalité depuis cinq ans.



Sources :
Cert.ssi
Panorama de la cybermenace
Diplomatie.gouv
Hostadvice
Incyber
Flare
Police Nationale
Sénat

LA CYBERSÉCURITÉ DANS LA STRATÉGIE MILITAIRE FRANÇAISE

La cybersécurité s'ancre dans une myriade de concepts liés au cyberespace (l'espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'internet, et par les données qui y sont traitées). La cybersécurité comprend les usages défensifs et offensifs des systèmes d'information. On prend en compte les moyens techniques utilisés pour l'échange de données (réseaux informatiques, téléphoniques, satellitaires...) ainsi que l'ensemble des informations stockées ou circulant sur des supports numériques (sites Internet, bases de données, messageries et communications électroniques, transaction dématérialisées, etc).

Par Paul Laurent, étudiant en droit public à l'université Paris-Panthéon-Assas.

Le cybersécurité est constituée de 3 axes fondamentaux :

- La cyberdéfense
- La cyberrésilience
- La cyberprotection

1/ La cyberstratégie militaire française, perspective historique

Le **livre blanc sur la Défense et la Sécurité nationale** en 2008, en positionnant les attaques informatiques comme deuxième menaces la plus importante pour la sécurité antaionle, affirme la prise de conscience des enjeux "cyber".

Le livre blanc de 2013 va plus loin en affirmant que la "capacité à se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs, est devenue un des éléments de la souveraineté nationale".

La stratégie cyber française est développée en profondeur dans la revue stratégique de cyberdéfense de 2018.

La cybersécurité française est mise à l'épreuve annuellement sur l'exercice **DEFNET**.

2/ Le éléments de la doctrine militaire française

Taillée pour répondre à 6 missions principales (prévenir, anticiper, protéger, détecter, réagir, attribuer), la doctrine française s'organise en 3 axes de lutte informatique :

La Lutte Informatique Défensive (LID).

C'est la composante traditionnelle de la posture stratégique française dans le domaine "cyber". Elle met en œuvre le travail de plusieurs acteurs (principalement COMCYBER, ANSSI et services de renseignement) pour répondre principalement aux missions de prévention, de protection et d'attribution.

La LID, par la vigilance continue imposée par le cyberespace, nécessite la mise en place d'une posture permanente de cyberdéfense (PCC), qui doit permettre de répondre à quatres niveaux de menaces :

1. Jaune : risques potentiels plus ou moins importants.
2. Orange : risques potentiels plus ou moins importants.
3. Rouge : risques hostiles jugés plausibles.
4. Écarlate : risques majeurs et simultanés.

La Lutte Informatique Offensive (LIO)

Le volet offensif de la lutte informatique n'apparaît publiquement qu'en janvier 2019 dans le corpus doctrinal français.

C'est dans une volonté d'affirmation face à des concurrents étatiques et infra-étatiques de plus en plus agressifs que les autorités ont décidé de rompre (légèrement) avec la posture uniquement défensive qui prévalait.

Cet aspect offensif reste très encadré par le droit national et international, et la France affirme n'y recourir que dans le cadre de la légitime défense.

La mise en place d'une action offensive peut être réalisée de manière autonome ou en combinaison avec des moyens militaires conventionnels pour "produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données".

La Lutte Informatique d'Influence (L2I)

Ce dernier élément est probablement le plus dense, puisqu'il nécessite une posture permanente offensive et défensive, et comprend un aspect tri temporel, avec une utilisation en amont, durant et en aval d'un conflit.

Cet aspect met potentiellement en concurrence l'Etat français et les forces armées avec n'importe quel acteur dans un conflit asymétrique déterritorialisé, en jouant sur des leviers parfois exclusivement irrationnels (la stimulation émotionnelle des utilisateurs notamment). La guerre, mais aussi les relations internationales, pouvant se définir comme une dialectique des volontés, la lutte d'influence au sein de la "couche informationnelle du cyberespace" joue un rôle éminemment stratégique.

Les missions du COMCYBER consistent "à détecter les attaques informationnelles susceptibles de nuire à la réputation des armées ou d'entraver leur action, à les caractériser, à les contrer et à promouvoir l'action de nos forces" (renseigner, défendre et agir).

3/ La structure militaire française

Le **COMCYBER** : Le commandement de la cyberdéfense, créé en 2017, rassemble l'ensemble des forces de cyberdéfense du ministère des armées. Il est placé sous l'autorité du chef d'état-major des armées.

Il dispose d'un état-major de la cyberdéfense (EM-CYBER) intégré dans la structure de l'état-major des armées, ainsi que d'un groupement de la cyberdéfense des armées (GCA) qui regroupe les centres spécialisés en cyberdéfense (notamment le Centre d'Analyse en Lutte Informatique Défensive – CALID).

L'ANSSI : L'Agence nationale de la sécurité des systèmes d'information, créée en 2009, est placée sous l'autorité du Premier ministre par le biais du secrétariat général de la Défense et de la Sécurité nationale (SGDSN). Entité non-militaire, elle est chargée de la mission

d'autorité nationale de défense des systèmes d'information de l'Etat et du soutien à ses opérateurs. L'ANSSI travaille en étroite collaboration avec les acteurs militaires de la cybersécurité.

Le CIAE : Le Centre interarmées des actions sur l'environnement, sous la tutelle du commandement du renseignement (COM-RENS) regroupe des acteurs français de l'influence militaire dans une perspective de mise en œuvre de la L2I.

Les autres organes : Un certain nombre d'autres structures sont dotés de compétences pour répondre aux enjeux de LID, LIO et L2I. On soulignera notamment VIGINUM (sous l'autorité du SGDSN), la DGSE, la DGSI, le Conseil de défense et de sécurité nationale (CDSN, le Comité de direction cyber (CODIR), le Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), etc.

Depuis 2021, la gendarmerie nationale s'est dotée d'un "commandement de la gendarmerie dans le cyberespace" (ComCyberGend) regroupant l'institut de recherche criminelle (IRCGN) et le centre de lutte contre les criminalités numériques (C3N). Il est chargé de piloter, conduire et animer le dispositif de la gendarmerie nationale dans la lutte contre les cybermenaces.

4/ Le cadre juridique internationale des actions de cyberdéfense

Les actions de lutte informatique défensive et offensive s'ancrent dans le principe de légitime défense, et dans la doctrine française du droit international sur le cyberespace.

Les actions de lutte informatique d'influence répondent à deux systèmes normatifs en fonction du contexte d'action. En temps de paix, c'est la Charte des Nations unies qui est la norme internationale de référence. En cas de conflit armé, la France s'engage à respecter les règles du Droit international humanitaire (nécessité militaire, précaution et proportionnalité dans l'attaque).

Les articles L. 2321-1 à L. 2321-4 du Code de la défense contiennent les dispositions juridiques nationales principales en ce qui concerne la mise en œuvre des actions de l'Etat sur le cyberespace.

5/ Les acteurs industriels français

On note le déploiement de certains des grands acteurs industriels de Défense et de Sécurité français sur le segment de la cybersécurité (Thalès, Aribus Defence & Space, etc) mais aussi d'acteurs civils comme Capgemini, Atos, Orange Cyberdéfense ou encore SFR Cybersécurité.

La France représente 4% d'un marché mondial de la cybersécurité écrasé par les Etats-Unis (39%).

La question d'un marché européen face aux filières nationales chinoise, états-unienne ou israélienne se pose. Le règlement EIDAS (harmonisation des normes sur l'identification électronique) ou la directive Network and Information Security de 2016 concrétisent une démarche timide en ce sens, malgré l'absence de vision commune dans le domaine.

6/ L'évolution des menaces

La particularité du risque cyber réside dans l'absence totale de barrières géographiques combinée à l'accès à une capacité de nuisance de la part d'individus isolés. Plus globalement, la menace se découpe en deux catégories : l'action militante et l'action mercantile.

Ce péril joue un rôle majeur dans le rééquilibrage du rapport de force mondial au profit des pays émergents, dans l'émergence des mouvements terroristes et dans la redistribution des sphères d'influence régionales.

A l'échelle nationale, la menace cyber est sur une courbe largement ascendante, en raison d'une part de l'augmentation des menaces mondiales, mais aussi plus simplement de l'intensification de la cybernétisation qui étend mécaniquement la surface menacée.

Quelques chiffres :

- **Augmentation de 50% des cyberattaques** visant les collectivités territoriales (depuis 2019).
- Plus de la moitié des entreprises françaises ont déjà subi une cyberattaque.
- **2 milliards d'euros de dégâts** pour l'économie française (2023). Augmentation de 300% des cyberattaques russes contre les pays de l'OTAN (de 2020 à 2022).

7/ Les enjeux à venir

Outre l'augmentation des menaces et la difficulté de mise en œuvre commune à l'échelle européenne (absence de conception commune des menaces, méthodes de traitement et normes industrielles), la France est confrontée à plusieurs enjeux. Voici les principaux :

- La proposition, conformément au droit international, d'une définition exacte de l'étendue de la souveraineté des Etats sur les différentes couches du cyberespace et des actes considérés comme illicites.
- Les difficultés de recrutement (1 100 postes non pourvus au ministère des Armées) malgré l'ambition de créer 953 nouveaux postes d'ici 2030.
- L'importance de la formation continue dans ce secteur, donc la perte de temps de travail effectif.
- La complexité de la mise en place d'un cloud de confiance souverain.
- Le cas d'Atos, et du maintien de ses activités cyber dans le giron d'un groupe français.
- La "dette technique" à rattraper pour adapter les forces françaises aux enjeux technologiques (près d'un milliard d'euros).
- La sécurisation des Jeux Olympiques (3 milliards d'attaques cyber attendues, 10 fois plus qu'à Tokyo en 2020.

Paul Laurent est étudiant en 3ème année de droit public à l'université Paris-Panthéon-Assas, Président de l'Institut Minerve et réserviste opérationnel au sein du 24ème Régiment d'Infanterie.



INTELLIGENCE ARTIFICIELLE ET CYBER-CONFLICTUALITÉ

Depuis novembre 2022 et la sortie de ChatGPT 3, l'IA suscite un intérêt passionné - mais aussi teinté d'inquiétude - dans les médias, le grand public et le monde économique. Jamais une innovation ne s'était diffusée aussi vite : le million d'utilisateurs était atteint en cinq jours, les cent millions en moins de deux mois. Un débat mondial s'engageait à son égard.

Par Colomban Lebas, agrégé d'histoire et géographie, docteur en science politique.

Quelques mois après le lancement public de ChatGPT 3,5, apparaissait une version augmentée, ChatGPT 4, ce qui semblait impliquer une dynamique de progression très ascendante – à rapprocher de la loi de Moore, ininterrompue depuis les années 50, et prévoyant le doublement des capacités de calcul des circuits intégrés à base de transistors tous les 18 mois environ. Bientôt des entrepreneurs et des chercheurs de haut niveau s'inquiétaient d'une possible perte de contrôle du destin de l'humanité, au cas où les IA atteindraient trop vite et sans précaution un niveau d'intelligence apparente dépassant celui d'un humain convenablement éduqué (La fameuse AGI)...
Une telle rupture technologique n'aurait-elle pas inévitablement un impact significatif sur les équilibres régnant au sein du cyberespace en particulier matière de rapport offensive-défensive ?

Après un bref commentaire des performances actuelles des grands modèles de langage de type GPT, Gemini ou Claude, nous tenterons de mettre en évidence la manière dont ces IA pourraient transformer les pratiques ayant cours dans le champ de la cyberconflictualité.

Si à moyen/long terme, l'apparition d'IA à aux performances décuplées, capables de dépasser l'humanité dans nombre de tâches quotidiennes, constitue sans nul doute une rupture anthropologique profonde – car facteur d'accélération du progrès techno-scientifique et porteuse de mutations qui affecteront l'ensemble des domaines d'activité – il convient néanmoins de resituer à sa place exacte la percée technologique en cours.

Les IA comme ChatGPT fonctionnent sur la base de grands modèles de langage (LLM), capables de sélectionner à partir d'une amorce textuelle les contenus les plus plausibles, sur la base d'un entraînement préalable supervisé portant sur un gigantesque corpus de données issues de la sphère numérique et tirant parti d'algorithmes probabilistes sophistiqués. La performance du système repose sur la capacité à effectuer massivement des calculs dans des délais de plus en plus brefs. Ce qui, incidemment, posera à terme d'importants problèmes énergétiques. Notons qu'en aucun cas les LLM (Large Language Models) ne comprennent ce qu'ils font. Il s'agit de simples programmes informatiques, agissant de manière purement mécanique.
A noter également que ces dispositifs ne constituent que l'une des manières de progresser en matière de simulation des intelligences humaines. Des voies alternatives sont possibles, et il est tout à fait plausible qu'à moyen/long terme, le progrès en IA emprunte

d'autres chemins que celui des LLM. Toujours est-il que ce sont ces IA à base de LLM qui sont aujourd'hui à la disposition du grand public. D'utilisation assez simple, elles sont intrinsèquement reliées – par leurs modalités d'entraînement et de fonctionnement – au cyberespace, milieu en proie à une intense conflictualité dont l'origine et les modalités sont très diverses : rançonnage, intrusions, prises de contrôle hostile, acquisition de renseignement, opérations d'influence, déstabilisation du système de défense de l'adversaire…

Examinons désormais en quoi les IA contemporaines, fondées sur l'apprentissage supervisé et /ou automatique, type ChatGPT et concurrents, sont-elles susceptibles, aujourd'hui et dans l'avenir proche, de modifier les termes de la conflictualité dans le cyberespace ?

La sphère numérique se caractérise par sa très forte évolutivité. Le cycle de vie des outils qui y permettent l'action est en effet extrêmement court. Dans ce monde opaque et changeant, l'agilité des postures est le maître-mot. D'où l'avantage donné à l'offensive sur la défensive. D'où également la supériorité de principe des défenses mobiles sur les défenses statiques ou périmétriques. Dans ce cadre, l'usage d'outils d'attaque ou de défense fondés sur l'IA y apparaît a priori fort utile. Cette sphère est par ailleurs transversale à tous les autres milieux physiques d'action : terre, air, mer, espace,…. d'où un important potentiel, hors-cyber (actions parfois qualifiées de "cinétiques").
Le coût d'accès à la sphère cyber est par ailleurs très faible, tandis que se développent des outils d'IA généralistes quasi-gratuits. Alors qu'à l'inverse, les effets d'une attaque cybernétique peuvent procurer des gains considérables, comme par exemple la création d'une nouvelle configuration du champ de bataille, structurellement favorable, sans même avoir physiquement combattu,… ce qui, dans la perspective de penseurs comme Sun Tzu, établirait une situation stratégique "idéale".
Cette sphère numérique est enfin le milieu où il est aujourd'hui le plus aisé aux IA de type LLM d'opérer,… en attendant la généralisation de leur appariement avec des agents physiques artificiels qui permettront de disposer de robots pleinement insérés dans la sphère matérielle, et pourtant dotés de la même quantité d'intelligence que ChatGPT 4 , 5 ou ses successeurs…

Il faut donc s'attendre dans les années qui viennent à un recours massif aux techniques d'IA dans **la cyberconflictualité**, qu'il s'agisse d'actions sur la couche sémantique, sur la couche logicielle, ou bien même sur la couche physique.

Il en sera ainsi, par exemple, des opérations de cyber-influence, qui seront de plus en plus friandes en outils à base d'IA.

- Dans le cadre d'une opération d'influence, intervenant sur la couche sémantique, L'IA permettra de créer très vite des agents conversationnels de propagande diffusant des contenus biaisés, ou bien comportant des informations volontairement erronées. L'automatisation par l'IA permet de créer massivement de tels agents, entraînant un effet de masse et saturation du "marché idéologique" susceptible de susciter massivement de fausses perceptions : théories complotistes, ou bien, au cours d'un conflit, impression que l'on perd alors que dans la réalité on progresse, etc.

- Le recours à des IA à des fins de persuasion peut s'avérer très productif car les LLM les plus performants s'avèrent dès aujourd'hui plus convaincants qu'un humain réel. Les IA

récentes sont par ailleurs plus empathiques que ces derniers.

- De plus en plus, L'IA permettra de diffuser massivement et de manière toujours plus crédibles, des fausses images, de faux fichiers vocaux, de fausses vidéos, de fausses interviews, même si certaines IA pourraient inversement s'avérer performantes dans le repérage des "fakes".

- L'IA permettra d'aller toujours plus loin dans l'hyper-personnalisation des contenus, affinant d'autant les techniques de manipulation de masse.

- Le recours à des agents conversationnels à base d'IA performantes peut être utile pour effectuer des tâches de renseignement comme le repérage et la priorisation de cibles en vue d'opérations ultérieures, y compris dans la sphère physique. Dans tous les cas, l'IA pourra être mobilisée pour repérer le plus rapidement et le plus exhaustivement possible l'ensemble optimal des cibles à soumettre à une attaque cyber donnée, par exemple dans le cadre d'une opération d'intrusion et de vol de données ou bien d'influence. Des techniques comme l'eye tracking, la reconnaissance des émotions, le neurohacking ou bien la détermination de patterns de comportement à travers l'exploitation d'objets connectés à diffusion aujourd'hui exponentielle, peuvent être mobilisées pour affiner la connaissance de la cible. Elles faciliteront sa manipulation ultérieure : captation d'attention, exploitation rationnelle des circuits de la récompense… les leviers à disposition sont nombreux et variés !

Hors de la couche sémantique ensuite, l'IA va également être déterminante : au plan logiciel, elle change la donne. Elle met en effet - et elle mettra toujours plus – de capacités de programmation automatisées à la disposition de ses utilisateurs.
Autrement dit, il deviendra de plus en plus facile à des pirates, même peu avancés en programmation, de réaliser des outils relativement sophistiqués, et en un temps très bref puisque l'IA code extrêmement rapidement. Le consensus des experts s'attend d'ailleurs à une poursuite de la progression exponentielle des performances des LLM dans les tâches de programmation.

Enfin, au plan des actions offensives matérielles à des fins de perturbation de la couche physique, il est clair que le développement de drones ou de robots d'attaque, dont la part d'autonomie ira croissant en particulier grâce à l'IA, ouvre d'importantes perspectives : des drones, toujours plus denses en outils fondés sur l'IA, pourraient apprendre à perturber le fonctionnement d'infrastructures-clés des réseaux. Par exemple des drones ou robots sous-marins, dopés à l'IA - particulièrement utile ici pour pallier l'opacité du milieu sous-marin vis-à-vis des ondes électromagnétiques, qui rend quasi-impossible leur téléopération sans fil. Ces drones pourraient perturber efficacement et en toute discrétion le fonctionnement de câbles sous-marins.

Inversement, n'oublions pas que l'IA ouvre également d'importantes perspectives en matière de défense cyber : mise au point plus rapide de parades logicielles (antivirus par exemple, patchs correctifs de failles logicielles) en utilisant les capacités de codage rapide de l'IA. L'analyse de la stratégie des attaquants pourra également être facilitée par le recours à l'IA en matière d'observation du comportement de l'adversaire, de détection des intrusions et des manipulations, d'identification des dégradations commises et

compréhension générale de la manœuvre et du dispositif d'attaque auxquels on fait face. En cas d'attaque portant sur le capital réputationnel d'un acteur, l'IA rendra la détection des signaux faibles plus aisée et permettra d'engager au plus vite des actions correctives.

En conclusion, les technologies relevant de l'IA modifient considérablement les outils à disposition pour agir dans le cyberespace autant au plan offensif que défensif, et ce, pour les couches tant sémantiques que logicielles ou physiques. La plus ou moins grande maîtrise de ces techniques sera l'un des paramètres décisifs du rapport de force et de la relation offensive/défensive lors des conflits à venir. L'irruption de l'IA grand public accentuera encore la porosité entre sphère civile et sphère militaire dans le cyberespace, fragilisera de nombreux États et démocratisera toujours plus l'usage de techniques d'attaques qui autrefois étaient l'apanage d'acteurs chevronnés. Sans une réelle volonté politique régulatrice, dotée de moyens convenablement dimensionnés, il pourrait en résulter une explosion des récits divergents, une prolifération des théories complotistes et une dangereuse relativisation du concept même de Vérité. La maîtrise des technologies fondamentales de l'IA ainsi que la capacité à les appliquer à la sphère militaire et sécuritaire apparaissent donc incontournables pour une puissance comme la France, membre permanent du Conseil de Sécurité de l'ONU : il en va de sa crédibilité future et de sa liberté de manœuvre dans le monde complexe et instable du XXIe siècle, qui, sous nos yeux, s'esquisse.

Colomban Lebas, ingénieur en télécommunication et traitement du signal, est diplômé de Sciences-po Paris et du master de géopolitique ENS-Ulm/Paris-I Sorbonne. Il est également agrégé d'histoire et géographie ainsi que docteur en science politique de l'Université Paris-II Panthéon-Assas. Il a été directeur d'Études au CEREM (Centre de recherche de l'Ecole Militaire qui a précédé l'actuel IRSEM), chef de la section académique du Centre d'Études Stratégiques de la Marine), et maître de conférences (hors corps universitaire) à Sciences-Po Paris. Ancien officier supérieur, il se consacre aujourd'hui à l'enseignement et à la recherche. Colomban Lebas est également Chevalier de la Légion d'Honneur (2016).



LES ENTREPRISES ET PROFESSIONS LIBÉRALES FACE À LA CYBERCRIMINALITÉ

Le risque cyber constitue désormais un territoire de délinquance de masse. Il impose aux entreprises d'opérer un changement de paradigme sur le sujet pour se protéger face à cette insécurité de type numérique.

Par Benoît Fayet, membre du comité stratégique du CRSI.

Les petites entreprises et les professions libérales, au même titre que les grandes entreprises ou organismes publics détenteurs de données personnelles, sont particulièrement exposées aux risques numériques et doivent en conséquence s'adapter et trouver des solutions pour se protéger de la cybercriminalité. Il s'agit de systématiser la prise en compte de cette menace. Penser son activité professionnelle sans intégrer le risque cyber est désormais l'assurance de conséquences potentiellement dramatiques sur le long terme.

Plus de 6 000 PME françaises victimes de cybercriminalité en 2023

Les entreprises françaises, ETI, PME ou grands groupes, au même titre que des structures publiques (hôpitaux, écoles, …) sont aujourd'hui massivement victimes d'incidents de sécurité informatique.

Plus de 6 000 PME françaises ont été attaquées sur les 12 derniers mois.

Des données sans doute minorées, pour 1 cyberattaque déclarée auprès des services de police, il y aurait plus de 50 cyberattaques en réalité, tentées ou réussies.

Les conséquences sont désastreuses puisque 60% des entreprises victimes de cybercriminalité déposent le bilan dans les 6 mois. Il est donc nécessaire que les entreprises prennent conscience du risque cyber, sans attendre de se faire attaquer pour réagir.

La cybercriminalité, un "marché" structuré et organisé

Le "marché" de la cybercriminalité s'est en effet considérablement transformé et structuré depuis quelques années. **70% des infractions "cyber" sont liées à des escroqueries**, **25% sont liées à l'image et à la vie privée** (cyber harcèlement, pédopornographie, etc.) et **5% sont véritablement du hacking**, émanant de professionnels généralement liées à des attaques organisées par des groupes, voire des États dans un marché ou le caractère international des attaques est de plus en plus prégnant.

Désormais en effet, des groupes de cybercriminels sont constitués en véritables

entreprises avec des stratégies et des objectifs pour réaliser un chiffre d'affaires et faire fructifier leurs activités. Aussi, ces cybercriminels visent ils en priorité les entreprises de taille moyenne du fait de leurs vulnérabilités avec de la donnée sensible qu'il est possible de faire "fuiter" et essentielle au bon déroulement des activités de ces entreprises sans laquelle elles pourraient être paralysées et qui sont donc des leviers pour les faire "chanter". Les données médicales sont par exemple les données les plus lucratives pour les cybercriminels avec le coût d'un dossier médical pouvant atteindre **350 dollars sur le darkweb**.

De plus, le risque cyber a été particulièrement renforcé avec la crise sanitaire. Le confinement a contraint les entreprises à laisser leurs salariés accéder aux réseaux internes depuis des appareils personnels, sans que ces réseaux n'aient été durcis en conséquence. Plus généralement, les entreprises payent aujourd'hui le prix d'une accélération de la digitalisation de la société alors même que leurs environnements informatiques se sécurisent peu à peu.

Cette situation est d'autant plus préoccupante que ces environnements sont de plus en plus interconnectés, générant des quantités de données qui sont autant de cibles. Les cybercriminels surfent aussi sur les nouvelles technologies qui leur offrent des opportunités comme le cloud qui a vu le nombre d'attaques contre ces serveurs doubler en 2023. L'intelligence artificielle est aussi un facteur de risque avec des technologies facilitant la tromperie des entreprises sur des périmètres de plus en plus large (clonage vocal, pretexting, …).

Des réponses possibles face à la cybercriminalité

1. Un enjeu clé de souveraineté qui engage une réponse étatique

En France, la cybercriminalité est prise en compte depuis la **loi informatique et libertés** (1978) et encadrée par un dispositif juridique prévoyant des peines allant jusqu'à **cinq ans d'emprisonnement** et **75 000 euros d'amende**.

La France dispose de plusieurs structures dédiées à la répression de la cybercriminalité au sein d'un dispositif de défense de qualité mais morcelé et complexe. Il y a l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) au sein de la Police judiciaire, le Centre de lutte contre les criminalités numériques (C3N) au sein de la Gendarmerie nationale ou encore la Brigade d'enquête sur les fraudes liées aux technologies de l'information (BEFTI) au sein de la préfecture de police de Paris auquel s'ajoute l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui pilote la stratégie de défense et de sécurité des systèmes d'information de la France. Un dispositif national d'assistance aux victimes de cybercriminels existe également (cybermalveillance.gouv.fr) permettant de les aider dans leurs démarches et proposant des programmes de formation (SensCyber).

2. Un enjeu clé pour les entreprises qui disposent de solutions pour se protéger

Les entreprises et professions libérales hébergent des données particulièrement recherchées par des cybercriminels qu'ils pourront revendre. Il s'agit de données dites sensibles, au sens du RGPD. Dans le cas d'un cabinet d'avocats, ces données peuvent être celles d'entreprises clientes couvertes par le secret des affaires (savoir-faire industriel, technique ou technologique, brevet ou marque, fichiers clients, activités commerciales, …). Il peut s'agir aussi de données personnelles confiées en vue d'une action en justice (données médicales, données d'identité, données financières, données liées à des activités professionnelles, …) qui sont des informations recherchées pour servir ensuite à des infractions liées à des usurpations d'identité.

Les actions de prévention ou de limitation des impacts

La plupart des infractions cyber peuvent être évitées, en mettant en place des systèmes de prévention. La cybersécurité d'une entreprise doit reposer sur les axes suivants :

Mettre en place des dispositifs amont de sécurité informatique

- Réaliser un audit de sécurité et une analyse des risques par un prestataire de service spécialis
- Identifier si sa structure dispose d'informations sensibles, s'interroger sur l'endroit où sont stockées les données, …
- Identifier les données sur lesquelles la structure a des obligations de protection et de gestion aux termes du RGPD,
- Evaluer la sécurité informatique des données utilisées et des équipements informatiques (stockage, propriété des informations, outils type messageries, etc.).

S'appuyer sur l'audit pour mettre en place un dispositif de protection

- Mettre en place des outils numériques sécurisés garantissant la sécurité des données et des échanges au sein de sa structure et vers l'extérieur,
- Mettre en place des dispositifs de protection qui permettent en cas d'attaque de revenir rapidement à une situation acceptable (sauvegarde et back-up de ses données essentielles, plan de continuité de l'activité informatique, …).
- Mettre en place au sein de son organisation des actions de sensibilisation et de formation des collaborateurs sur des règles d'hygiène numérique (parcours proposés par l'ANSSI, la CNIL, …).
- Intégrer le risque cyber dans les budgets pour l'achat de logiciels de protection, de matériel, mais aussi pour les moyens humains ou de formations pour mener les actions évoquées de formations ou les plans de prévention.

Les actions en réaction à une attaque

En réponse à une attaque, plusieurs points clés sont à retenir, autour des actions suivantes :

- Signaler rapidement les faits auprès des services de police et systématiquement porter plainte.
- Communiquer en transparence et rapidement aux enquêteurs toute trace ou preuve numérique que le cybercriminel aurait pu laisser comme sur une scène "physique" de crime
- Solliciter le dispositif cybermalveillance.gouv.fr et se faire aider par des prestataires spécialisés pour mettre en place les actions de relance de l'activité.
- S'appuyer sur les liens existants à un niveau interprofessionnel (CGPME ou MEDEF, CNB,…) avec les structures type ANSSI afin de remonter les incidents.

En conclusion, les cyberattaques spectaculaires et médiatisées contre les infrastructures sont les prémices de difficultés voire de catastrophes qui peuvent désormais frapper tous les acteurs économiques privés. Compte tenu des enjeux attachés à leur secteur d'activité, les entreprises et professions libérales sont autant exposées que les autres. Il incombe donc à chacun de s'organiser en conséquence et de s'y préparer, avec l'aide de spécialistes, via des plans de prévention de hauts niveaux et surtout en éduquant chacun des collaborateurs des entreprises concernées. La première faille est humaine, et chacun doit être responsabilisé.

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. Il est membre du comité stratégique du CRSI.



DES MÉTIERS DE LA CYBERSÉCURITÉ EN PLEINE MUTATION

En 2021, la cybercriminalité a coûté plus de 6000 milliards de US$ en termes de dommages. Si le cybercrime était comparé à un pays, il serait situé au 3ème rang de l'économie mondiale selon l'EPRS (European Parliamentary Research Service). Avec plus de 20 milliards d'objets connectés, les métiers de la cybersécurité sont en plein boom. Explications.

Par Valérie Doye, spécialiste de la cybersécurité.

La montée en puissance du web, les réseaux sociaux, les objets connectés, les malwares, l'intelligence artificielle, les hackers, les cybercriminels et les robots, tels sont les éléments et les acteurs du cyberespace.

On compte déjà plus de 20 milliards d'objets connectés.

La surface d'attaque devient de plus en plus étendue et complexe. Les professionnels de la cybersécurité deviennent très recherchés, les personnes expérimentées se font rares… Et parmi les personnes travaillant dans les métiers de la cybersécurité à l'échelle nationale, on trouve encore trop peu de représentations féminines.

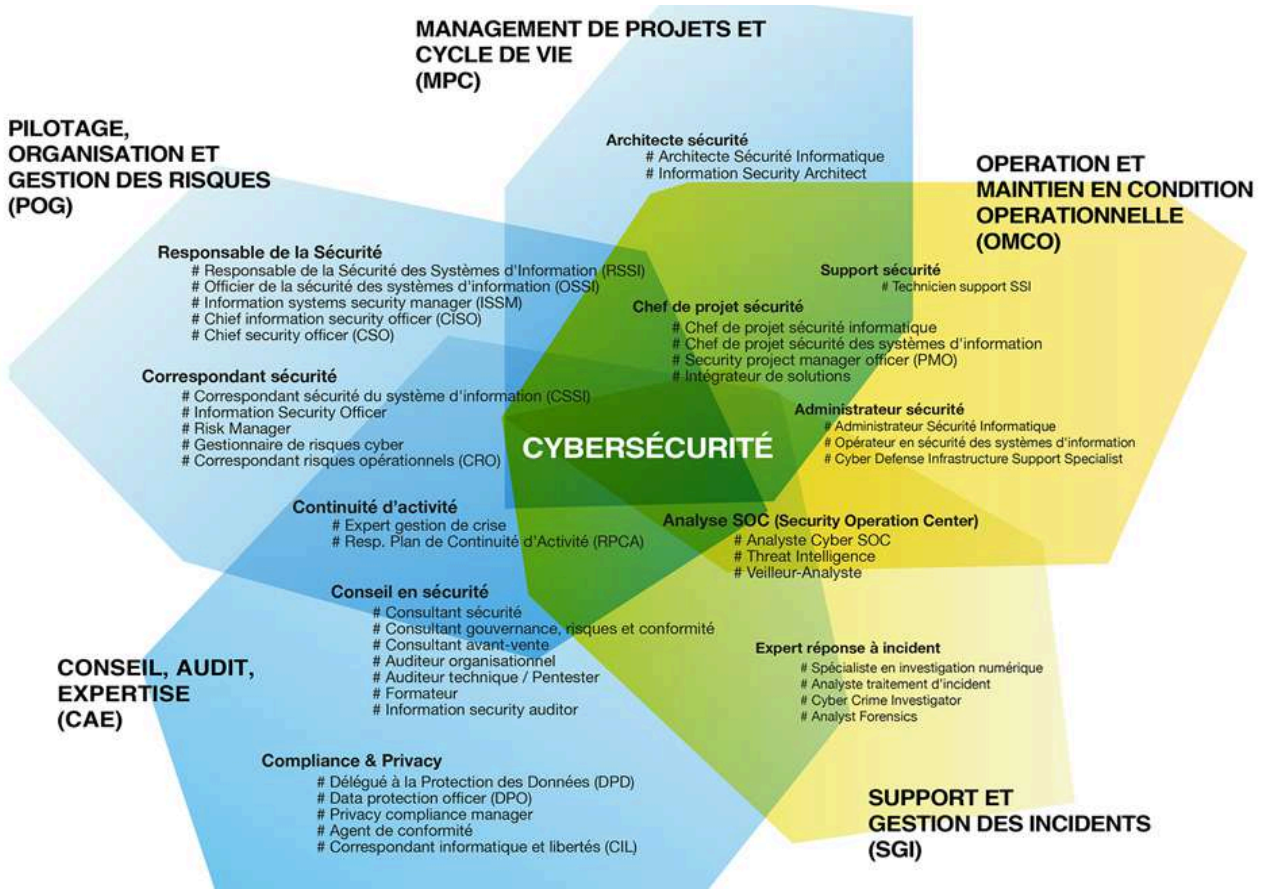
Pourtant, le domaine est passionnant, exaltant, il nécessite une multiplicité de compétences, de l'analyse, de la recherche, du développement, du déploiement, du conseil, de la mise en conformité, demandant d'interagir avec de nombreux métiers et de la géopolitique pour comprendre les enjeux des cyberguerres. Ce domaine est aussi exigeant, basé sur un apprentissage permanent, accompagné d'une veille active, réalisée grâce à un suivi de la presse spécialisée dans le domaine technologique et des avancées de la recherche, pouvant être complété par des investigations sur le dark web non référencé par les moteurs de recherche classiques. Il nécessite de plus une compréhension et une connaissance fine des environnements culturels et géopolitiques pour déceler au plus tôt les prémices de cyberattaques et investiguer post-incident.

En général, la cybersécurité est souvent perçue comme un domaine complexe et opaque réservé à des spécialistes de l'informatique, ce qui est loin de la réalité. Revenons tout d'abord à la définition de la cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements issus du Cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. On devine alors que les métiers contribuant à garantir la cybersécurité sont nombreux.

Pour illustrer la diversité des métiers, l'Ecole de Guerre Economique (EGE) a publié en 2020 une cartographie des métiers de la cybersécurité, cf. figure n°1. On y trouve deux familles de métiers cyber, l'une de type fonctionnel figurant dans les pétales bleues tels que les métiers de RSSI (CISO en anglais),

Correspondant Sécurité, Expert en gestion de Crise ou Expert en Plan de Continuité ou de Reprise d'Activités, Consultant en sécurité. L'autre de type opérationnel figure dans les pétales jaunes avec des Administrateurs en Sécurité, des Analystes SOC (Security Operation Center), des Experts en réponse à incident, des Supports en Sécurité, avec à la croisée des chemins, des Chefs de Projets Sécurité et des Architectes Sécurité. Avec la montée en puissance de l'informatique quantique, il y aussi un grand besoin de chercheurs en cryptologie, science englobant la cryptographie (l'écriture secrète) et la cryptanalyse (l'analyse de cette dernière).

Sur le plan technique, ce serait une erreur de penser que ce domaine n'est restreint qu'à l'informatique. Par le préfix cyber, on désigne tout ce qui est relatif à l'utilisation du réseau Internet. Autrement dit, l'architecte expérimenté en réseaux télécoms et informatiques est doté d'un énorme avantage pour travailler dans le domaine de la cybersécurité. Celle-ci se décline en effet dans toutes les couches des réseaux de transport et des systèmes d'information.



Cartographie des métiers de la cybersécurité en 2020, Source EGE 2020.

Dans les métiers à dominante fonctionnelle, on y trouve aussi les métiers du conseil en Gouvernance, Risques et Conformité, les Délégués à la Protection des Données (DPD ou DPO en anglais). Parmi les métiers connexes contribuant à la démarche de cybersécurité, on y trouve des juristes d'entreprises, des avocats, des managers de risques, des directeurs de la sûreté, le responsable des assurances, le responsable du contrôle interne, le chargé de communication spécialisé en cybersécurité et nécessairement des spécialistes des relations internationales ou géopolitiques, cf. le panorama des métiers de la cybersécurité publié en 2020 par **l'Agence Nationale de la Sécurité des Systèmes d'Information** (ANSSI).

La cybersécurité est une filière d'avenir. Selon une étude menée par l'APEC (l'Association Pour l'Emploi des Cadres), les besoins de cadres dans le domaine de la cybersécurité n'ont jamais été aussi élevés, ils ont doublé en l'espace de quatre ans. L'augmentation de la numérisation des échanges et des transactions ainsi que l'accroissement de la menace cyber renforce le besoin de professionnels qualifiés au sein des entreprises et des administrations.

Par ailleurs, une enquête a été menée par l'observatoire des métiers de l'ANSSI auprès des étudiants d'écoles d'ingénieurs, des professionnels en formation initiale (etc.) inscrits en filière cybersécurité, informatique hors cybersécurité ainsi que les filières hors informatique (scientifique, commerce, communication, droit, autres). L'objectif de cette étude est de comprendre la représentation que se font les étudiants en fonction de leur cursus. Le taux de féminisation des formations en cybersécurité (14%) et en informatique est relativement faible (18%).

Interrogés sur les secteurs d'activités les plus attractifs en termes de carrière et d'emploi, les répondants des cursus cybersécurité et informatique établissent un classement identique : le secteur le plus attractif leur paraît être le secteur de l'informatique/numérique, suivi du secteur de l'industrie aéronautique/spatiale/défense et du secteur des prestations et solutions spécialisées en cybersécurité. Les étudiants désignent le secteur du e-commerce comme étant le secteur le moins attractif. Les secteurs de la santé, des télécoms et de l'enseignement sont également ressentis comme moins attractifs, pourtant les besoins en cybersécurité sont actuellement préoccupants.

Parmi les menaces qui défient la paix et la sécurité en Europe, on relève :

- Les conflits violents,
- La prolifération des armes de destruction massive,
- Le changement climatique,
- Le terrorisme,
- Les cyberattaques,
- La désinformation.

La cybersécurité est devenue un enjeu essentiel pour les Européens (88% sont connectés à l'Internet) en vue de garantir leur souveraineté numérique et autonomie stratégique.

En 2021, la cybercriminalité a coûté en termes de dommages plus de 6000 milliards de US$.

Si le cybercrime était comparé à un pays, il serait situé au 3ème rang de l'économie mondiale selon l'EPRS (European Parliamentary Research Service).

En 2021, 150 personnes ont été arrêtées lors d'une opération historique d'Europol pour des faits de revente de drogues, d'armes ou des propositions de services illégaux sur le dark web. En avril 2022, la marketplace russophone Hydra du dark web a été fermée après une enquête de plusieurs mois diligentée par la police allemande. Elle permettait d'échanger des NFT et des crypto en dehors des plateformes légales.

Dans son rapport TE-SAT publié en 2023, EUROPOL (European Union Agency for Law Enforcement Cooperation, Centre de lutte contre la cybercriminalité) indique que "l'Internet et la technologie sont restés des vecteurs majeurs de propagande, ainsi que de radicalisation et de recrutement de personnes vulnérables au service du terrorisme et de l'extrémisme violent".

Beaucoup d'experts en cybersécurité s'attendaient à ce que l'Ukraine subisse une paralysie informatique totale après quelques mois de conflits avec la Russie. Harcelée pendant des années par les cyberattaques russes, l'Ukraine s'est forgé une solide défense numérique. Le 27 juin 2017, à la veille de célébrer la constitution de l'Ukraine, le pays a subi une nouvelle vague de cyberattaques d'une puissance inédite dans le monde entier avec la propagation du virus NotPetya, un ransomware qui s'est avéré en réalité être un logiciel de sabotage détruisant toutes les données sur son passage.

Tout en consolidant sa défense numérique, l'Ukraine a aussi accordé une très grande importance à la coopération entre entreprises et gouvernements. Elle a reçu beaucoup de soutien sur le plan numérique de l'Estonie, de la Roumanie et de l'OTAN.
La mise en œuvre d'un plan de continuité numérique basé sur une sauvegarde de toutes les données dans le cloud Amazon Web Services (AWS) facilité par le déploiement ultra-rapide des connexions internet via le réseau satellite de SpaceX a permis de secourir l'Ukraine sur le plan numérique en un temps record.

Si la force économique du continent Européen est à l'Ouest, les centres d'expertises en cybersécurité sont à l'Est, pour des raisons historiques. L'Estonie, pays pionnier européen en matière d'utilisation d'Internet, a vécu une cyberguerre dès 2007. Pour diminuer l'emprise de la sphère d'influence russe, les experts de l'OTAN ont développé à Tallinn dès 2008 un centre d'analyse et de surveillance pour défendre le cyberespace des Etats membres.

Le 28 juin 2021, le règlement établissant le Centre de Compétences Européen en matière de Cybersécurité (CECC) est entré en vigueur. Le CECC est basé en Roumanie à Bucarest. Il réunit également les principales parties prenantes européennes, notamment des entreprises, des organisations universitaires et de recherche et d'autres associations de la société civile concernées, afin de constituer une communauté de compétences en matière de cybersécurité destinée à renforcer et diffuser l'expertise en matière de cybersécurité dans toute l'Union Européenne.

L'Union Européenne entend renforcer la sécurité de l'internet ainsi que d'autres réseaux et systèmes d'information critiques par la mise en place d'un centre de compétences en matière de cybersécurité. L'objectif est de mettre en commun les investissements dans la recherche, les technologies et le développement industriel en la présence de leaders industriels européens tels que BitDefender en Roumanie et ESET en Slovaquie.

Lorsque l'Ukraine a dû se défendre face à l'invasion russe, c'est l'Estonie qui a dirigé le programme de l'Union européenne visant à fournir au pays attaqué les services de protection des données. Quant à la Roumanie, elle s'est associée avec le géant de la cybersécurité Bitdefender pour apporter une assistance professionnelle à l'Ukraine et offrir un accès gratuit aux logiciels du groupe.

Sources :

"Cartographie des métiers de la cybersécurité" EGE 2020.
"Panorama des métiers de la cybersécurité", ANSSI 2020.
"Rapport TE-SAT", sur la situation et les tendances du terrorisme dans l'Union européenne, EUROPOL 2023.
"Cyberguerres et cyberattaques, les défis de la cybersécurité", Autrice Valérie DOYE, ouvrage à paraître en 2024.



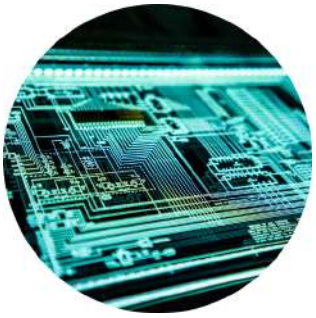
Ingénieure de Telecom Paris Tech, **Valérie Doye** a commencé sa carrière professionnelle dans la cybersécurité en 1998 avant de se spécialiser en architecture réseaux et sécurité dans le domaine des télécoms. Passionnée par le domaine de la cybersécurité, elle a suivi en 2021 une formation certifiante en Sécurité des Systèmes d'Information (SSI) à l'école Polytechnique Executive Education.

Fondatrice de la société Keystone Cybersecurity, elle donne des cours de cybersécurité à des écoles d'ingénieur et de management. RSSI Adjointe, à l'ACMOSS sous la tutelle du Ministère de l'Intérieur et des Outre-mer, également membre du CEFCYS, elle fait partie des 65 rôles modèles féminins dont le portrait est décrit dans le livre publié en août 2023 "Je suis une femme, et je travaille dans la cybersécurité".

Valérie Doye est aussi autrice, elle travaille sur un ouvrage "Cyberguerre et Cyberattaques, les défis de la cybersécurité", à paraître en 2024.

TRIBUNE

LA CYBERCRIMINALITÉ,
Fraude, pédopornographie, et cyberguerre



L'auteur de cette tribune est fonctionnaire de police. Il a été anonymisé à sa demande. Depuis ses débuts dans les forces de l'ordre en 2005, il a été témoin d'une évolution sans précédent dans le cyberespace.
En tant qu'officier de police judiciaire et investigateur en cybercriminalité, il a été confronté à des défis complexes et changeants, allant de la lutte contre le terrorisme à la protection des enfants contre l'exploitation en ligne.

Dans cet état numérique, les menaces évoluent à une vitesse fulgurante. Les cybercriminels exploitent habilement les technologies émergentes pour mener des attaques sophistiquées, mettant en péril la sécurité de nos données personnelles, de nos infrastructures critiques et de nos institutions.
Les cyberattaques ne se limitent pas au monde virtuel. Elles ont un impact direct sur la sécurité publique, que ce soit par le biais de la criminalité en ligne, de la propagande extrémiste ou de la manipulation de l'information. Les forces de l'ordre doivent s'adapter à cette nouvelle réalité pour protéger efficacement les citoyens et maintenir l'ordre public.

Les réseaux sociaux et les plateformes en ligne sont devenus des outils de choix pour les organisations terroristes, qui les utilisent pour recruter de nouveaux membres, propager leur idéologie et planifier des attaques. En tant qu'enquêteur cyber, il a été impliqué dans des opérations visant à démanteler des réseaux terroristes en ligne et à identifier leurs propagandistes.

La cybercriminalité prend de nombreuses formes, allant de la fraude financière au vol d'identité en passant par le cyberharcèlement. En travaillant en étroite collaboration avec des partenaires nationaux et internationaux, il a été possible de traquer et d'arrêter des cybercriminels de haut niveau et de démanteler des réseaux criminels opérant dans le cyberespace.

La protection des enfants contre l'exploitation en ligne est une priorité absolue. En tant qu'enquêteur cyber, j'ai travaillé sur des affaires de pédopornographie en ligne, traquant les prédateurs et sauvant des victimes innocentes de situations horribles. Nous devons redoubler d'efforts pour sensibiliser le public aux dangers de la pédopornographie en ligne et pour renforcer la coopération internationale dans la lutte contre ce fléau.

La sensibilisation du public aux risques potentiels en ligne est essentielle pour renforcer la résilience de nos communautés face aux menaces numériques. En animant des tables rondes et des conférences sur les dangers de l'internet et des réseaux sociaux, j'ai pu

partager mon expertise et mes connaissances avec un large public, contribuant ainsi à créer une culture de sécurité en ligne.

Face à des adversaires aussi agiles et sophistiqués que les cybercriminels, la collaboration entre les forces de l'ordre, les entreprises, les organisations de la société civile et les citoyens eux-mêmes est indispensable. Ensemble, nous pouvons partager des informations, développer des solutions innovantes et coordonner nos efforts pour lutter efficacement contre les menaces numériques.

Dans notre lutte contre la cybercriminalité, l'innovation est notre meilleur atout. Nous devons constamment repousser les limites de la technologie pour développer de nouvelles techniques d'investigation, des outils de détection avancés et des stratégies de prévention efficaces. En investissant dans la recherche et le développement, nous pouvons rester un pas en avant des cybercriminels et protéger efficacement nos communautés dans le cyberespace.

En conclusion, la cybersécurité est l'un des défis les plus pressants de notre époque. En tant que policier engagé dans la protection des concitoyens, je reste déterminé à relever ce défi avec efficacité et détermination. En partageant nos expériences, en renforçant nos compétences et en travaillant ensemble, nous pouvons construire un cyberespace plus sûr et plus résilient pour tous.

Pour ne rien manquer de notre actualité,
vous pouvez nous suivre sur les réseaux sociaux

TÉMOIGNAGE

RÉSILIENCE,LA FONDATION AU SERVICE DES BLESSÉS DE LA VIE

En 2021, 215 000 condamnations définitives ont été prononcées en France à l'encontre de jeunes de 10 à 24 ans (*). Malgré cet état de fait, un ensemble de personnes refuse de croire en la défaite et la défaillance absolue de cette jeunesse en difficulté. Des hommes et des femmes, issus des métiers de l'uniforme, blessés en service s'engagent pour une nouvelle mission. Celle de venir en aide à ces adolescents désœuvrés.

Texte et photos : Jean-Marie Leclère / Collectif DR.

Depuis 2022, dans l'Ain, la Fondation Résilience aide les blessés des métiers de l'uniforme à surmonter leurs épreuves physiques et mentales du quotidien. Geoffrey Hodicq en est le président. La structure organise, en France et à l'étranger, des stages pédagogiques et sportifs au profit d'une jeunesse désœuvrée en manque de repères souvent rebelles à l'autorité.

En 2023, près de mille cinq cents stagiaires (tous publics, tous âges) ont été pris en charge par la fondation Résilience. Ainsi, le président Hodicq a développé, entre autres, un partenariat avec les Établissements pour l'insertion dans l'emploi (Épide). Lors de la session hivernale 2024, un stage de rupture est organisé à Boulogne sur Mer. L'équipe d'instructeurs vétérans a pour mission d'accompagner dix jeunes de l'Épide de Doullens dont la volonté est de rebondir vers l'insertion.

Geoffrey Hodicq, l'engagement et le service chevillé au corps

À dix-neuf ans, Geoffrey devient jeune chasseur alpin "au 7" (7ème B.C.A.). Alors qu'il vient du plat pays avec les terrils comme point culminants, il s'adapte rapidement aux montagnes de la Tarentaise où il se forge un mental de fer et d'acier. Après différentes missions Opex en Afrique, fin 2010 il s'envole pour la FOB (Base opérationnelle avancée) de Nijrab (province de Kapisa) en Afghanistan.



Il côtoie la menace des talibans. Le 19 février 2011, dans la vallée d'Alasay, sa vie bascule. Alors en mission de reconnaissance au sein d'une patrouille motorisée, son VAB (véhicule de l'avant blindé), subit une attaque de roquettes. Malgré l'effet du souffle de l'explosion, les gestes, les comptes-rendus, et les ordres sont opérants pour extirper son groupe de l'impasse. Le bilan est lourd. Clément, un de ses camarades est mort. Benjamin a une jambe arrachée.

Après six mois de soins en France et au titre de sa thérapie, Geoffrey demande à repartir en Opex au Mali. Après d'autres affectations métropolitaines, il quitte définitivement les effectifs en 2021. Il a la conviction de pouvoir servir son pays autrement.

Demeurer actif pour continuer à vivre

Pour les blessés physiques et psychiques et leurs familles, le retour à la vie civile comporte son lot de difficultés ; mutisme, isolement, désocialisation et parfois couplées aux addictions de toutes sortes. Geoffrey connaît ces démons. Ne plus se sentir utile l'affecte et pourtant, servir est dans ses gênes. Par les compétitions sportives civiles et militaires, il se dope à l'adrénaline et réussit à refaire surface. Vies sociale et privée s'apaisent.

Parce qu'ils ont tout donné, notre devoir est de les aider

À Brénod dans l'Ain, La maison des blessés offre l'entraide et l'écoute dont les blessés ont besoin. C'est ici que l'ancien chasseur alpin crée le futur camp de base de la fondation. Mais il veut aller encore plus loin. *"Les Résilients sont ces blessés de guerre que nous souhaitons voir réintégrer une nouvelle vie"*, explique le Président. *"Je veux épauler nos vétérans à continuer de servir leur pays. Ils savent encadrer et maitrisent la vie en pleine nature"*, poursuit-il. Cet objectif devient un leitmotiv. Il structure sa stratégie en participant au parcours défense entrepreneur (partenariat entre le ministère de la Défense et le Mouvement des entreprises de France). L'ex-militaire est accompagné par un chef d'entreprise du Medef, Geoffrey professionnalise son projet.

En 2022 au terme de ce tutorat, le nouvel entrepreneur est rejoint par trois cadres supérieurs d'entreprises nationales. Ils créent ensemble la fondation Résilience. Ce statut juridique leur permet de lever des fonds publics et privés à destination de leurs actions d'aide aux blessés.

"Parce que nous souhaitons toujours servir notre pays, nous décidons de le faire autrement envers des publics qui en ont besoin,
la Fondation a cette ambition."

Geoffrey Hodicq, co-fondateur

Restructuration et partage de valeurs



Après leur santé recouvrée, les blessés résilients se forment aux métiers de l'éducation sportive. Ainsi, ils encadrent des stages de restructuration personnelle. Ces sessions de cohésion, d'aguerrissement et de rupture visent à renforcer l'estime de soi et des autres par la reconnaissance de valeurs partagées, celles du respect, de la loyauté, de l'entraide et de l'autonomie. La fondation Résilience propose ainsi une boucle vertueuse de la guérison à double effet à l'image d'une organisation symbiotique où chacun tire bénéfice de l'autre.

Accompagner la jeunesse des centres Épide

Les Épide ont été créés à la suite de la fin de la conscription en 2002. En France, vingt centres accueillent des jeunes de 17 à 25 ans pour une durée de huit mois renouvelables. Face à un public le plus souvent en perte de valeurs et notions républicaines, le respect des Droits et Devoirs côtoient l'élaboration de leur projet professionnel.

"Ces jeunes sont habitués à l'affrontement, ils ont besoin de cadre et d'exemplarité."

Jean-Michel, coordinateur de la zone Nord

Au cours d'une séance de cohésion sur la plage de Boulogne-sur-Mer, un jeune se confie, *"c'est dur, je suis à saturation, j'ai les jambes qui tremblent"*, annonce-t-il groggy dans sa tenue trempée. Par le jeu, le dépassement de soi, l'esprit collectif aide à résoudre les difficultés rencontrées pour atteindre l'objectif assigné ou encore monter le bivouac dans la nuit noire.



"Je me suis découvert des capacités physiques que je ne soupçonnais pas. Pour continuer et les développer encore, je dois gérer mon addiction aux stupéfiants,...", annonce l'un d'eux.

En fin de stage, les jeunes sont reçus pour un bilan individuel. Certaines prises de conscience se révèlent. Un des stagiaires confie à un instructeur, *"Je peux suivre physiquement, mais je dois gérer mes émotions. Si je ne les maîtrise pas, je deviens violent. En me contrôlant je vais pouvoir continuer mon projet vers un métier de l'uniforme"*. Bailem, conseiller éducation citoyenneté au centre Épide de Doullens, confie que les stages doivent perdurer dans le temps. *"Leurs travers réapparaissent dans les semaines suivantes. Avec la direction, on propose aux jeunes un deuxième séjour de rupture avec des entretiens de suivi en Épide plus réguliers afin de mieux les aider"*, complète-t-il. Pour les conseillers éducatifs de l'Épide commence le long travail d'accompagnement dans la mise en place des mesures correctives évoquées par les stagiaires.

Dix candidats ont participé à ce stage de rupture. Un a abandonné pour raison sanitaire. six sur les neufs autres sont volontaires pour refaire un stage afin de progresser dans leur vie. La jeune femme, Delphine, qui avait le projet d'intégrer un régiment d'élite, n'a pas réussi sa sélection. Elle pourra à l'avenir re-postuler. En attendant, elle a fait sa demande de Volontaire découverte de l'armée de terre (VDAT). Elle sera admise en formation dès la fin mai 2024.



"Vous avez des parcours de vie compliqués. Sachez que vous n'êtes pas les seuls. Nous sommes passés par là aussi. Mais cela ne nous empêche pas de croire en nos valeurs et en l'avenir. Vous pouvez réaliser vos projets professionnels", expose Geoffrey lors de la clôture du séjour de rupture de Boulogne.

Une action en symbiose

En 2023, dix instructeurs sont certifiés par l'obtention d'un brevet professionnel de la jeunesse de l'éducation populaire et du sport et/ou d'activités de randonnée de proximité et d'orientation. Ils encadrent cinq cent quatre-vingts jeunes. Des partenariats sont également noués avec des institutions telles que les Associations départementales des amis et parents d'enfants inadaptés (Adapei), afin d'élargir le public bénéficiaire des stages et pouvoir augmenter ainsi le nombre de blessés à devenir Résilients. La fondation relie également les résilients au monde du travail civil. Il noue

des partenariats avec le Mouvement des entrepreneurs de France (Medef). Les séjours ainsi proposés sont pour les instructeurs des occasions de transmettre leurs valeurs telles que l'autonomie, dignité, respect et cadre de vie.

Ainsi au travers de l'ensemble de ses actions la fondation Résilience assure la reconnaissance et le bien être d'hommes et femmes meurtris dans leurs parcours. Par leur travail les résilients exigeants mais justes réveille les consciences de cette jeunesse, elle aussi blessée par une désocialisation ou un handicap.

"Les militaires, forces de l'ordre et pompiers mettent souvent leurs vies en danger pour protéger les nôtres. Il est normal de leur rendre de l'espoir dans les situations difficiles."

Richard Zirmi, co-fondateur

Une ambition budgétaire basée sur le partenariat.

À 2027, quatorze millions d'euros sont prévus pour financer structurer l'organisation des stages sur l'ensemble du territoire national. Pour assurer ce budget, une cinquantaine de personnes et institutions soutiennent la fondation. Des entreprises privées (STID, QPARK, SAFRAN et Netceler) participent aussi au développement de la fondation. La recherche de partenariats est une nécessité pour l'équilibre du budget. Elle est le travail quotidien des membres de la fondation.

(*) **Champ** : France entière, auteurs condamnés en 2021.
Sources : Ministère de la justice, SG-SDSE, exploitation statistique du casier judiciaire national
Note : Les condamnations définitives ont pu être prononcées en 1ère instance ou en appel. Du fait des délais de procédure, le nombre de condamnations prononcées en 2021 ne correspond pas au nombre d'auteurs présumés poursuivis la même année.

EN BREF

PAROLE AUX JEUNES DU CRSI



"Étudiante en dernière année de Bachelor Relations Internationales, je me suis orientée vers le CRSI pour exercer mon stage de fin de diplôme. Mon intérêt croissant pour les questions de sécurité intérieure, particulièrement d'actualité en ces temps troublés, m'a naturellement conduite vers ce think thank de référence. Je suis convaincue que la compréhension approfondie de ces enjeux est essentielle pour construire un avenir plus sûr et plus serein."

Charline, nouvelle stagiaire au CRSI

"J'ai rejoint le CRSI car il est un lieu de convergence essentiel pour les individus impliqués et engagés dans les questions régaliennes et sécuritaires. Le CRSI offre en effet un espace distinctif dédié à la réflexion et à l'échange, ce qui contribue de manière significative au domaine de la sécurité intérieure. De plus, son approche inclusive rassemblant forces de l'ordre, militaires, juges, chercheurs et d'autres acteurs de la sécurité, permet une réflexion approfondie dépassant les cadres émotionnels, et d'adopter un regard plus objectif sur la situation. Cette approche donne une vision sur le long terme en reconnaissant les racines profondes des défis actuels."



Alichane, Master en relations internationales à l'IRIS Sup'



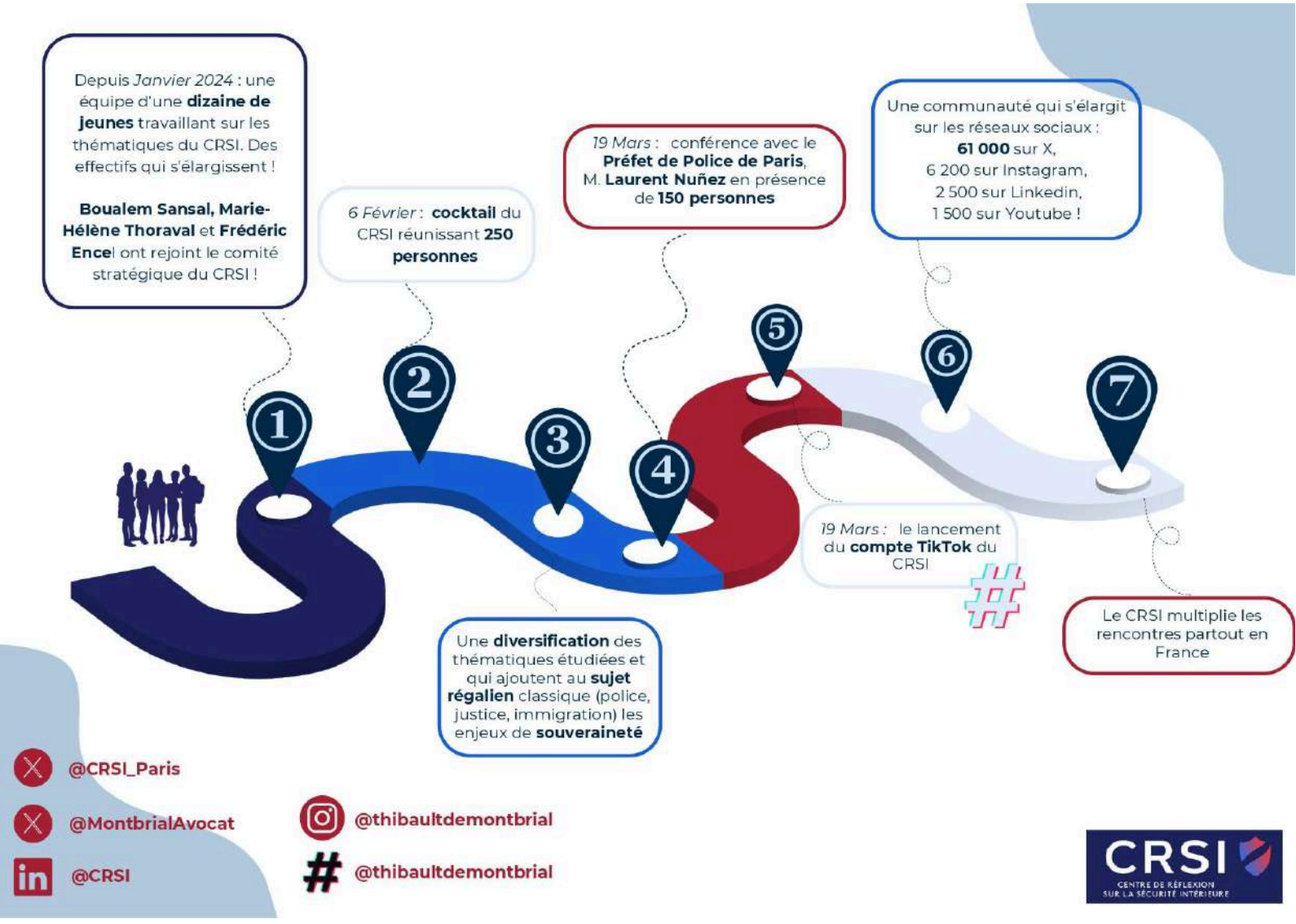
"À la suite d'une intervention de Thibault de Montbrial sur le thème : "La violence urbaine, un mal occidental ?" j'ai voulu en savoir plus sur le Think-Tank du CRSI. Sa vocation qui est de contribuer à la réflexion autour des enjeux relatifs à la sécurité intérieure m'a attiré, surtout dans le climat sécuritaire actuel particulièrement tendu à l'approche des JO de Paris 2024. Rejoindre cette communauté de pensée est pour moi l'occasion d'apporter ma pierre à l'édifice."

Blandine, Licence en science politique à l'ICES

DÉVELOPPEMENT DU CRSI

Le CRSI poursuit son développement. Depuis janvier dernier, une quinzaine de jeunes ont rejoint les équipes opérationnelles du Centre. Ils participent activement à son travail de veille et de production de notes en se réunissant régulièrement. Le CRSI densifie également sa présence sur les réseaux sociaux grâce à une équipe nouvellement constituée et qui ne compte pas son temps.

Vous êtes étudiant et vous souhaitez consacrer du temps au service de votre pays : **contactez-nous**.



DERNIÈRES PUBLICATIONS

Le CRSI se dote de nouveaux moyens et augmente son travail de production. Depuis le mois de mars, nous avons pu aborder de nombreux sujets que nous vous proposons de retrouver sur notre site. Vous pouvez nous suivre sur les réseaux sociaux, en particulier X, LinkedIn et YouTube pour ne rien manquer.













ILS NOUS SOUTIENNENT





















DEVENEZ PARTENAIRE DU CRSI

Contactez-nous :

od@crsi-paris.fr

tdm@crsi-paris.fr

POUR ADHÉRER AU CRSI :

helloasso

MENTIONS LÉGALES

La Lettre de la Sécurité Intérieure - © Avril 2024 - Tous droits réservés

Directeur de publication : Thibault de Montbrial - Conception, rédaction et réalisation : Olivier Debeney, Charline Le Du

Crédit photos : Maud Koffler, Yaniv Bettane, Politeia

CRSI - Centre de Réflexion sur la Sécurité Intérieure

Association Loi 1901 - N° enregistrement W751227813 - 10 rue Cimarosa - 75116 PARIS - France

Contact : 01 43 80 15 25 - secretariat@crsi-paris.fr - www.crsi-paris.fr

