IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

OBSERVATOIRE
géopolitique du numérique et des technologies émergentes

RENSEIGNEMENT ET CYBERESPACE : LA RECONFIGURATION D'UNE FONCTION RÉGALIENNE À L'ÉPREUVE DE L'AUTONOMIE STRATÉGIQUE

Léa Samara / Contributrice au Programme Moyen-Orient / Afrique du Nord et à l'Observatoire numérique et technologies émergentes de l'IRIS

Novembre 2026



PRÉSENTATION DE L'AUTRICE

Léa Samara / Contributrice au Programme Moyen-Orient / Afrique du Nord et à l'Observatoire numérique et technologies émergentes de l'IRIS

Léa Samara est chargée de mission éditoriale à l'IRIS, où elle contribue au Programme Moyen-Orient/Afrique du Nord et à l'Observatoire géopolitique du numérique et des technologies émergentes. Diplômée de Sciences Po Paris en affaires publiques et arabophone, elle est spécialiste du Moyen-Orient. Ses recherches portent sur le milieu informationnel régional, et ses déclinaisons algorithmiques. Elle travaille également sur le confessionnalisme, la diplomatie transactionnelle, en particulier les accords d'Abraham et la diplomatie culturelle des États du Golfe. Elle suit en outre le dossier nucléaire iranien. Elle a mené des terrains à Beyrouth et au Caire et participe aux travaux de *La Revue internationale et stratégique*.

PRÉSENTATION DE L'OBSERVATOIRE

Sous la direction de **Camille Boulenguer**, chercheuse à l'IRIS, l'Observatoire géopolitique du numérique et des technologies émergentes propose un espace d'analyse et de réflexion dédié à l'étude de ces technologies et de leurs impacts multidimensionnels.

Il se donne pour objectif de centraliser et de produire une expertise indépendante sur les technologies émergentes, comme l'intelligence artificielle, les blockchains ou l'ordinateur quantique. Pour cela, l'Observatoire s'attache à analyser les implications géopolitiques, mais également économiques, sociales et éthiques des révolutions technologiques et se fixe pour objectif de favoriser le dialogue entre praticiens et chercheurs afin de se préparer aux évolutions à venir et accompagner les décideurs publics et privés.

iris-france.org

@InstitutIRIS

@InstitutIRIS

institut_iris

IRIS

IRIS - Institut de relations internationales et stratégiques

© IRIS - Tous droits réservés

En 2016, un collectif se présentant sous le nom de *Shadow Brokers* mit aux enchères une partie de l'arsenal d'intrusion (les exploits, codes d'accès et implants conçus pour pénétrer et surveiller à distance des systèmes ciblés) de la *National Security Agency*[1] (NSA). Que la première agence de renseignement technique du monde pût être percée à son tour[2] et voir ses outils offensifs circuler sur des forums clandestins en disait long sur la condition nouvelle du renseignement à l'âge numérique. Lorsque l'une de ces failles, *EternalBlue*, servit l'année suivante à propager les rançongiciels *WannaCry* puis *NotPetya* jusqu'à paralyser des hôpitaux britanniques et des multinationales (Maersk, Merck, FedEx, Saint-Gobain ou encore Mondelez), la démonstration se referma d'elle-même, puisque l'arme du renseigneur[3], une fois échappée, venait frapper l'ordre qu'il prétendait protéger[4]. De la même façon, en juillet 2019, SyTech, prestataire du Service fédéral de sécurité de la fédération de Russie (FSB), a été compromis par le collectif *0v1ru$*, qui a exfiltré environ 7,5 téraoctets de données exposant des projets secrets du service[5]. En investissant le cyberespace, le renseignement y a donc gagné une puissance de collecte et d'action sans précédent, mais y a contracté dans le même mouvement une fragilité qui lui était jusque-là étrangère.

Le renseignement recouvre l'ensemble des activités de recherche, d'exploitation et de diffusion d'informations utiles aux autorités responsables de la sécurité et de la défense. La tradition opposait les sources humaines aux sources techniques, et ces dernières ont connu, avec la généralisation des échanges numériques, une expansion telle qu'elles commandent aujourd'hui l'essentiel de la production. Héritier de l'interception des communications, le renseignement d'origine électromagnétique a étendu son domaine à l'exploitation des réseaux informatiques, au point que la pénétration des systèmes cyber constitue désormais le premier vecteur de la collecte[6]. En 2024, les accès aux données de connexion représentent à eux seuls plus de la moitié des demandes de techniques de renseignement formées par les services français, tandis que le recueil et la captation de données informatiques, c'est-à-dire l'intrusion directe dans les systèmes, progressent de 27,2 % en un an, signe d'une bascule vers les techniques les plus intrusives[7]. Cette prééminence engage davantage qu'une question de

[1] Scott Shane, Nicole Perlroth et David E. Sanger, « Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core », *The New York Times*, 12 novembre 2017.
[2] WikiLeaks, « Vault 7 reveals the staggering breadth of "CIA hacking" », *The Conversatio*n, 8 mars 2017
[3] L'acteur, service ou agent, qui conduit le renseignement, c'est-à-dire « l'ensemble des informations et faits révélés et analysés par le travail des services […] dans le but de prévenir les atteintes aux intérêts de la Nation. ». Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT), *La Stratégie nationale du renseignement*, Présidence de la République, 2019.
[4] Andy Greenberg, *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York :Doubleday, 2019).
[5] Zak Doffman, « Russia's Secret Intelligence Agency Hacked: "Largest Data Breach in Its History" », *Forbes*, 20 juillet 2019.
[6] Stéphane Taillat, Amaël Cattaruzza et Didier Danet (dir.), *La Cyberdéfense. Politique de l'espace numérique*, 2e éd., (Paris :Armand Colin, 2022).
[7] Commission nationale de contrôle des techniques de renseignement, *9e rapport d'activité 2024*, 2025.

volume, car elle inscrit l'État dans un espace qu'il ne possède pas en propre, dont les câbles, les protocoles et les logiciels relèvent d'acteurs privés et de puissances étrangères, et où son aptitude à voir dépend d'infrastructures qu'il ne maîtrise qu'en partie.

Dans quelle mesure le cyberespace reconfigure-t-il le renseignement en instrument de puissance, et que coûte cette transformation à l'autonomie stratégique française ? Deux dynamiques contraires se font face, le numérique accroissant la portée des services tout en les enserrant dans un tissu de dépendances techniques, d'alliances dont ils ne fixent pas les termes et d'incertitudes qui fragilisent leurs conclusions. Le renseignement cyber ne devient un véritable attribut de souveraineté qu'adossé à des moyens propres, à un encadrement juridique qui le légitime et à une aptitude autonome à désigner l'adversaire, faute de quoi il demeure une puissance empruntée.

LE RENSEIGNEMENT SAISI PAR LE CYBER : MUTATION D'UNE FONCTION RÉGALIENNE

Du renseignement électromagnétique au cyber

Le renseignement cyber prolonge une tradition ancienne, celle de l'interception des signaux, industrialisée au rythme où la radio puis les télécommunications ont multiplié les flux à capter. Entre écouter une conversation et pénétrer un système d'information, la différence de procédé ne doit pas masquer l'identité du geste, qui consiste dans les deux cas à accéder clandestinement au secret d'autrui. On comprend ainsi que les grandes agences techniques, la NSA américaine, le *Government Communications Headquarters* (GCHQ) britannique ou la Direction générale de la sécurité extérieure (DGSE) en France, se soient imposées comme les principaux opérateurs cyber de leurs États respectifs[8]. Les travaux de géopolitique du cyberespace conduits en France autour de Frédérick Douzet ont établi que la maîtrise de cet espace se joue sur la superposition de trois couches, matérielle, logique et sémantique, et que le contrôle des infrastructures physiques y conditionne celui des contenus qui y circulent[9].

L'ampleur et la concentration des points de captation marquent, en revanche, une transformation profonde. À partir des années 2000, la numérisation a ramené une part écrasante des communications mondiales vers un petit nombre de câbles sous-marins, de nœuds d'interconnexion et de centres de données, offrant au renseignement des accès d'une

[8] *Ibid.*
[9] Frédérick Douzet, « La géopolitique pour comprendre le cyberespace », Hérodote, no 152-153, 2014 :3-21 Frédérick Douzet (dir.), « Géopolitique de la datasphère », Hérodote, no 177-178, 2020.

densité inédite. Le coût d'une surveillance supplémentaire s'est effondré dans le même temps, puisque suivre une cible de plus ne réclame plus un dispositif humain dédié mais l'extension d'un traitement déjà en place. Une filature physique couverte revient à environ 275 dollars (USD) de l'heure par cible, contre 0,36 dollar (USD) de l'heure pour un suivi GPS sur vingt-huit jours (un rapport de l'ordre de 1 à 750)[10]. De cette bascule procèdent les grandes controverses contemporaines, depuis les révélations d'Edward Snowden en 2013 jusqu'aux législations nationales qui ont tenté d'encadrer l'analyse automatisée de données de masse[11]. La dualité propre aux opérations cyber achève de troubler les repères, car une même implantation dans un réseau adverse autorise l'écoute, le vol de données ou la destruction matérielle. L'attaque contre le réseau électrique ukrainien en décembre 2015 en offre l'illustration, la même intrusion, d'abord menée à des fins de reconnaissance, ayant ensuite servi à provoquer une coupure privant quelque 225 000 foyers d'électricité[12]. Parce que l'espionnage et le sabotage empruntent les mêmes voies d'accès et ne se séparent qu'au stade ultime, chaque intrusion découverte nourrit le soupçon du pire et alimente une défiance durable entre puissances[13].

Le renseigneur pris pour cible : la vulnérabilité au cœur de la puissance

Le trait le plus déroutant du renseignement cyber tient à ce que l'instrument de la puissance y forme également le point de faiblesse. Dans les domaines classiques, l'appareil qui observe demeure difficile à atteindre, tandis que dans le cyberespace les services comptent parmi les cibles les plus recherchées, et la compromission de leurs outils engendre des dommages en chaîne. L'affaire des *Shadow Brokers* en a administré la preuve la plus brutale, lorsque les capacités offensives soustraites à la NSA, conçues pour forcer des systèmes étrangers, ont nourri en 2017 deux campagnes destructrices planétaires. *WannaCry* désorganisa en quelques heures les systèmes hospitaliers du service public britannique, au point d'imposer la déprogrammation d'interventions, tandis que *NotPetya*, quelques semaines plus tard, se propagea depuis l'Ukraine jusqu'aux réseaux d'armateurs et d'industriels de premier rang, pour un coût que l'on a estimé à une dizaine de milliards de dollars[14]. L'épisode fit la démonstration qu'une arme de renseignement, une fois hors de portée de son détenteur,

[10] Kevin S. Bankston et Ashkan Soltani, « Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones* », *Yale Law Journal Forum* 123 (2014).
[11] Glenn Greenwald, *Nulle part où se cacher*, Paris, JC Lattès, 2014
Commission nationale de contrôle des techniques de renseignement, *6e rapport d'activité 2021*.
[12] Cybersecurity and Infrastructure Security Agency, « Cyber-Attack Against Ukrainian Critical Infrastructure », alerte IR-ALERT-H-16-056-01, 25 février 2016.
[13] Thomas Rid, *Cyber War Will Not Take Place*, Oxford, Oxford University Press, 2013.
[14] Andy Greenberg, « The Untold Story of NotPetya, the Most Devastating Cyberattack in History », *Wired*, 22 août 2018.
Dommages mondiaux estimés à 10 milliards de dollars par la Maison-Blanche ; pertes de 870 M$ (Merck), 400 millions de dollars (USD) (FedEx/TNT Express), 384 millions de dollars (USD) (Saint-Gobain), 300 millions de dollars (USD) (Maersk), 188 millions de dollars (USD) (Mondelez) et 129 millions de dollars (USD) (Reckitt Benckiser).

devient un bien commun de la malveillance et échappe à toute mesure de proportionnalité[15]. L'habitude de conserver des vulnérabilités inédites, pour s'en réserver l'usage offensif, se paie dès lors d'un affaiblissement de la sécurité collective, tension que Ben Buchanan a décrite comme la transposition numérique du dilemme de sécurité[16].

Cette exposition modifie la nature même de l'activité de renseignement, désormais soumise à une incertitude permanente sur la solidité de l'avantage acquis. Elle hausse surtout au rang d'enjeu stratégique une opération qui, hors du cyberespace, relevait de la police scientifique ou de l'analyse militaire, à savoir l'identification de l'auteur d'une intrusion. Reconnaître qui se dissimule derrière une attaque exige d'abord un travail de renseignement, technique autant qu'humain, avant d'engager une appréciation politique. Cette fonction d'attribution découle directement de la vulnérabilité partagée, l'anonymat offert à tout attaquant faisant de la capacité à nommer l'adversaire la condition de toute riposte.

LE RENSEIGNEMENT CYBER COMME INSTRUMENT DE PUISSANCE

Coopérer pour voir : l'autonomie française à l'épreuve des alliances

Comme les menaces et les flux se jouent des frontières, le renseignement cyber appelle une coopération étroite entre services, et il figure parmi les champs où celle-ci atteint son plus haut degré d'intégration. Cette coopération se révèle en même temps l'une des plus verrouillées qui soient, et c'est par là qu'elle éclaire la position de la France. Son noyau demeure l'alliance dite des *Five Eyes* qui, depuis l'accord UKUSA de 1946, associe les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans un partage approfondi du renseignement d'origine électromagnétique, sous la prééminence de Washington[17]. Le degré de confiance et d'interopérabilité qui lie ces cinq capitales anglophones ne trouve d'équivalent dans aucun cercle plus large. La France en reste absente. Elle participe à des configurations élargies et plus lâches, que la littérature désigne parfois comme les *Nine Eyes* ou les *Fourteen Eyes*, et entretient d'intenses échanges bilatéraux avec ses homologues, sans jamais accéder au cercle le plus resserré[18].

Pour une puissance qui aspire à l'autonomie stratégique, une telle mise à l'écart pèse un poids réel. Elle signifie qu'une part de la vision du monde dont dispose Paris procède d'un partage

[15] Greenberg, Sandworm, *op. cit.*
[16] Ben Buchanan, The Cybersecurity Dilemma. Hacking, Trust and Fear Between Nations, Oxford, Oxford University Press, 2017.
[17] « Five Eyes », Encyclopædia Britannica, consulté le 7 octobre 2026.
[18] Sébastien-Yves Laurent, Atlas du renseignement. Géopolitique du pouvoir (Paris : Presses de Sciences Po, 2014).

dont la France n'écrit pas les règles et dont elle peut être tenue éloignée au gré des circonstances. L'autonomie se mesure dès lors à la faculté de collecter et d'analyser par ses propres moyens, seule garantie contre la dépendance informationnelle. La France compte parmi les rares États européens à entretenir une capacité d'interception d'ampleur, adossée notamment à sa position sur plusieurs routes de câbles sous-marins et à l'implantation de ses services outre-mer, ce qui lui procure, dans ses échanges bilatéraux, une monnaie qui compense en partie son exclusion du cercle anglophone. Le niveau européen n'y supplée guère, le Centre de situation et du renseignement de l'Union mettant certes en commun des analyses nationales, mais demeurant un organe de synthèse dépourvu de moyens opératoires, l'Union n'ayant ni service ni capteurs intégrés[19]. La coopération européenne reste ainsi suspendue au bon vouloir des États et à la prééminence d'une architecture anglo-saxonne dont le centre de gravité se trouve outre-Atlantique. On touche là, à l'ambivalence des États-Unis, alliés indispensables des Européens et, par le poids de leurs agences comme de leurs grandes entreprises, facteur de dépendance pour ceux qu'ils protègent.

De l'espionnage économique à l'opération de destruction

La connaissance n'est pas le seul usage que les États font du renseignement cyber, car le même accès qui permet d'observer permet d'agir, et cette capacité d'intervention en fait un levier stratégique. Sa manifestation la plus massive, quoique la moins visible, reste l'espionnage économique et industriel. Peu onéreux, aisément déniable et déployable à grande échelle, le cyber s'est imposé comme le vecteur privilégié de la captation des secrets d'affaires. L'opération baptisée *Cloud Hopper* en fournit un exemple. Attribuée au groupe APT10, rattaché au ministère chinois de la Sécurité d'État par le truchement d'une société-écran, elle n'a pas pris les entreprises pour cibles directes, mais a compromis des prestataires d'infogérance afin d'atteindre par contagion l'ensemble de leurs clients à travers une douzaine de pays, dont la France, jusqu'à l'inculpation de deux ressortissants chinois par la justice américaine en décembre 2018[20]. Pour une économie française dont les fleurons, dans la défense, l'aéronautique, l'énergie ou la pharmacie, forment autant de cibles permanentes,

[19] Taillat, Cattaruzza et Danet (dir.), *La Cyberdéfense*, *op. cit.*

[20] U.S. Department of Justice, «Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information », Communiqué de presse, 20 décembre 2018
PwC UK and BAE Systems, *Operation Cloud Hopper, Exposing a systematic hacking operation with an unprecedented web of global victims* (April 2017).

l'enjeu justifie que la protection du patrimoine économique et scientifique ait été confiée à un service de renseignement intérieur, la Direction générale de la sécurité intérieure[21].

Une intervention cyber peut aussi produire un effet physique, et c'est alors que le renseignement rejoint la stratégie militaire la plus directe. L'opération *Olympic Games*, dont le ver *Stuxnet* fut le vecteur et que la découverte fortuite de 2010 porta à la connaissance du public, demeure à cet égard un cas d'école. Conduite conjointement par les services américains et l'unité israélienne 8200, elle visa l'usine d'enrichissement de Natanz, dont elle dérégla les automates de commande pour emballer puis briser les centrifugeuses, tout en renvoyant aux opérateurs iraniens des relevés faussement normaux qui retardèrent le diagnostic de la panne. La réussite supposait de marier l'expertise logicielle des uns au renseignement patiemment accumulé par les autres sur la configuration exacte des installations, ce qui confirme que l'arme cyber la plus sophistiquée reste d'abord une affaire de renseignement[22]. En frappant sans franchir le seuil de l'affrontement ouvert, l'opération offrit une solution de rechange à la frappe aérienne et inscrivit le sabotage informatique dans une stratégie assumée de contre-prolifération, dont Téhéran tira la leçon en se dotant à son tour de capacités offensives.

D'autres affaires déclinent le même registre selon des intensités variables. La campagne *SolarWinds*, mise au jour fin 2020, illustre l'espionnage par la chaîne d'approvisionnement, le service de renseignement extérieur russe ayant, par le groupe APT29, glissé un code malveillant dans une mise à jour d'un logiciel de supervision largement déployé, atteint près de dix-huit mille organisations et exploité activement une centaine d'entreprises et neuf agences fédérales américaines, avant que Washington n'impute l'opération à Moscou en avril 2021[23]. L'affaire *Pegasus*, révélée la même année, déplace le regard vers le marché commercial de l'intrusion, le logiciel espion de la société israélienne NSO Group, cédé à des États clients, ayant figuré au centre d'une fuite de plus de cinquante mille numéros sélectionnés, parmi lesquels ceux de chefs d'État et de responsables français[24]. Que des prestataires privés mettent à la disposition de gouvernements une capacité de surveillance jadis réservée aux plus grandes agences brouille le monopole régalien du contrôle informationnel et nourrit, jusque dans les enceintes onusiennes, l'inquiétude devant la

[21] Direction générale de la sécurité intérieure, « La DGSI au cœur de l'organisation française de cyberdéfense », 23 novembre 2023, consulté le 7 octobre 2026.
[22] David E. Sanger, *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*(New York : Crown, 2012).
« Operation Olympic Games and the Stuxnet Cyberweapon », synthèse dans GlobalSecurity.org, consultée le 9 octobre 2026.
[23] Cybersecurity and Infrastructure Security Agency, *Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally*, avis AA23-347A, 13 décembre 2023.
[24] Amnesty International, « Projet Pegasus : révélations sur un système mondial de surveillance », 17 juillet 2022.

prolifération de ces outils[25]. En effet, Le renseignement cyber n'est plus l'apanage des seuls États. Une véritable industrie privée de la surveillance s'est constituée, dont Google recense une quarantaine d'entreprises et auxquelles il attribue près de la moitié des failles de type *0-day*[26] exploitées contre ses produits entre 2014 et 2023[27].

LE NŒUD DE L'ATTRIBUTION

Attribuer sous incertitude : un travail de renseignement devenu geste diplomatique

L'anonymat relatif de l'attaquant, la facilité du déni et le relais possible par des territoires tiers font de l'identification de l'auteur une tâche techniquement ardue et politiquement périlleuse. Thomas Rid et Ben Buchanan en ont proposé une lecture graduée, articulant un niveau technique, un niveau opérationnel et un niveau stratégique, où la conviction se forme par recoupements successifs sans jamais atteindre la certitude de la preuve judiciaire. L'attribution n'est pas un constat mécanique mais relève d'un jugement de renseignement que prolonge une décision proprement politique, celle de rendre ou non l'accusation publique. Depuis le milieu des années 2010, les démocraties occidentales ont érigé cette dénonciation en doctrine, dans l'espoir qu'en nommant l'agresseur elles parviendraient à le dissuader. Néanmoins, l'effet escompté demeure limité, car la réprobation internationale pèse peu sur des régimes qui assument leurs opérations, et chaque attribution rendue publique consume des sources et des méthodes patiemment constituées, de sorte que la décision de parler engage un arbitrage délicat entre le bénéfice diplomatique et le coût opérationnel[28].

Les puissances du renseignement cyber accroissent la difficulté en cultivant des stratégies de brouillage. Beaucoup d'États s'appuient sur des relais, groupes criminels ou collectifs hacktivistes qu'ils tolèrent ou commanditent sans les avouer, afin de préserver un déni plausible et d'entretenir une zone grise où l'action étatique se dissimule derrière l'apparence

[25] Organisation des Nations unies, rapport final du Groupe de travail à composition non limitée sur la sécurité et l'usage des technologies de l'information et de la communication (2021-2025), A/80/257, entériné par la résolution A/RES/80/16 le 1er décembre 2025.
[26] Une faille dite "0-day" (ou "jour zéro") est une vulnérabilité logicielle encore inconnue de l'éditeur, donc dépourvue de correctif, ce qui la rend particulièrement précieuse pour qui l'exploite avant sa divulgation. Agence nationale de la sécurité des systèmes d'information (ANSSI), *CyberDico.*
[27] Google Threat Analysis Group, *Buying Spying: Insights into Commercial Surveillance Vendors*, février 2024.
[28] Thomas Rid et Ben Buchanan, « Attributing Cyber Attacks », *Journal of Strategic Studies*, vol. 38, no 1-2, 2015 : 4-37 ; sur la dénonciation publique comme pratique diplomatique. Florian J. Egloff et Max Smeets, « Publicly attributing cyber attacks: a framework », *Journal of Strategic Studies*, vol. 46, no 3, 2023 :502-533.

de la délinquance[29]. D'autres recourent au faux drapeau, qui consiste à endosser l'identité d'un tiers pour égarer l'enquête. L'attaque qui interrompit la diffusion de TV5 Monde en avril 2015, d'abord revendiquée par un prétendu *CyberCaliphate* arborant les signes de l'État islamique, en offre l'exemple le plus net, l'enquête ayant établi par la suite que ses auteurs appartenaient au groupe APT28, relevant du renseignement militaire russe. La France a formellement imputé cette opération au service de renseignement militaire de la Russie (GRU) le 29 avril 2025, en même temps que les tentatives d'ingérence dans l'élection de 2017 et une série d'attaques postérieures, dont l'une visait une organisation liée aux Jeux olympiques de 2024[30]. Prononcer publiquement une attribution engage la crédibilité de celui qui parle, dévoile une part de ses capacités et appelle une réponse, ce pour quoi l'Union européenne s'est dotée d'une boîte à outils cyberdiplomatique autorisant une attribution collective et l'adoption de sanctions contre les responsables désignés[31].

Encadrer pour agir : le modèle français du renseignement cyber

Encore faut-il, pour que l'attribution débouche sur une décision souveraine, que l'État dispose en amont d'un renseignement cyber capable et légitime. La décennie écoulée a vu la France combler sur ce point un retard singulier, en dotant d'un cadre légal une activité qui s'était développée dans une semi-clandestinité juridique. Adoptée dans le sillage de l'affaire *Snowden*, la loi du 24 juillet 2015 relative au renseignement a défini pour la première fois l'ensemble des techniques autorisées et les a placées sous le contrôle d'une autorité administrative indépendante, la Commission nationale de contrôle des techniques de renseignement[32]. C'est à elle que l'on doit l'introduction, d'abord expérimentale, de la technique dite de l'algorithme, destinée à repérer des signaux faibles par l'analyse automatisée des données de connexion. La loi du 30 juillet 2021 a pérennisé ce dispositif, en a élargi la portée aux adresses complètes consultées sur internet et a resserré les garanties procédurales qui l'entourent[33]. Celle du 25 juillet 2024 en a étendu la finalité au-delà de la seule prévention du terrorisme, jusqu'à la défense des intérêts de la politique étrangère et à la lutte contre les ingérences étrangères[34]. Cette évolution est cruciale, car l'outil conçu contre

[29] United States Department of Justice, « Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace », octobre 2020
Cybersecurity and Infrastructure Security Agency, avis AA24-038A, 7 février 2024.
[30] Ministère de l'Europe et des Affaires étrangères, « Russie : attribution de cyberattaques contre la France au service de renseignement militaire russe (APT28) », 29 avril 2025, consulté le 13 octobre 2026.
[31] Council of the European Union, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* (“Cyber Diplomacy Toolbox”), doc. 10474/17, June 19, 2017.
[32] Loi no 2015-912 du 24 juillet 2015 relative au renseignement, *Légifrance*.
[33] Loi no 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *Légifrance*.
[34] Loi no 2024-850 du 25 juillet 2024, *Légifrance*
Sénat, « Proposition de loi visant à prévenir les ingérences étrangères en France », rubrique *La loi en clair*.

la menace terroriste se trouve désormais tourné vers la rivalité entre États, aveu que le renseignement technique s'assume comme arme de la compétition entre puissances.

Ce cadre juridique s'appuie sur une communauté structurée et sur un effort financier considérable. Six services dits du premier cercle sont coordonnés depuis 2017 par la Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) rattachée à la présidence de la République, et se répartissent les missions. La Direction générale de la sécurité extérieure assurant la puissance technique dirigée vers l'étranger et la Direction générale de la sécurité intérieure le contre-espionnage sur le territoire[35]. La loi de programmation militaire 2024-2030 porte à quatre milliards d'euros l'enveloppe consacrée au domaine cyber, contre 1,6 milliard sur la période précédente, avec un renforcement explicite des capacités de la DGSE[36]. Prise dans son ensemble, cette construction compose un modèle dont l'originalité tient à l'alliance de la puissance et du contrôle, des moyens croissants s'y exerçant sous le regard d'un juge et dans les limites fixées par le législateur, là où la tradition anglo-saxonne est longtemps restée discrète sur ses fondements de droit[37]. On y reconnaît la forme proprement française de l'autonomie stratégique dans ce champ, qui ne parie pas sur une illusoire autosuffisance, hors de portée d'une puissance moyenne, mais sur la légitimité démocratique conférée à une capacité souveraine, gage de crédibilité auprès des citoyens comme des partenaires étrangers[38]. Il reste que ce renseignement opère sur des réseaux, des logiciels et des données dont la maîtrise échappe pour l'essentiel aux Européens, ce qui le renvoie à la question plus vaste de la souveraineté numérique, du nuage informatique aux systèmes de paiement[39].

Aucune des mutations décrites ne se laisse lire comme un simple gain de puissance. En reconfigurant le renseignement, le cyberespace a accru la capacité des États à connaître et à agir autant qu'il les a exposés, faisant de l'attribution comme de la maîtrise des infrastructures les conditions nouvelles de leur autonomie. Le renseignement cyber ne devient un véritable attribut de souveraineté qu'adossé à des moyens propres, à un encadrement juridique qui le

[35] CNRLT, « La CNRLT et la communauté française du renseignement ». *Revue Défense Nationale*, 2018/8 N° 813, 2018 : 9-13.
[36] Sénat, rapport d'information n°638 (2022-2023), « Pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030 », 24 mai 2023.
[37] Olivier Forcade et Bertrand Warusfel (dir.), *Le droit du renseignement*. Actes du colloque organisé par l'Académie du renseignement à l'École militaire, 8 février 2019(Paris : *La Documentation française*, 2020).
[38] Amaël Cattaruzza, *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data* (Paris :Le Cavalier Bleu, 2019).
[39] Camille Boulenguer et Sami Nakib, *Souveraineté européenne des paiements (2026-2035). De la dépendance structurelle à la construction d'une doctrine des paiements européenne* (Paris : IRIS, juin 2026).

légitime et à une aptitude autonome à désigner l'adversaire, faute de quoi il demeure une puissance empruntée.



IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

2 bis, rue Mercœur - 75011 PARIS / France

+ 33 (0) 1 53 27 60 60

contact@iris-france.org

iris-france.org

L'IRIS, association reconnue d'utilité publique, est l'un des principaux think tanks français spécialisés sur les questions géopolitiques et stratégiques. Il est le seul à présenter la singularité de regrouper un centre de recherche et un lieu d'enseignement délivrant des diplômes, via son école IRIS Sup', ce modèle contribuant à son attractivité nationale et internationale.

L'IRIS est organisé autour de quatre pôles d'activité : la recherche, la publication, la formation et l'organisation d'évènements.