Cyber : les enjeux pour la défense et la sécurité des Français

Louis Gautier

Dans Politique étrangère 2018/2 Été , pages 29 à 42
Éditions Institut français des relations internationales

ISSN 0032-342X
ISBN 9782365678155
DOI 10.3917/pe.182.0029
Date de mise en ligne : 08/06/2018

Article disponible en ligne à l'adresse
https://shs.cairn.info/revue-politique-etrangere-2018-2-page-29?lang=fr

CAIRN.INFO

Découvrir le sommaire de ce numéro, suivre la revue par email, s'abonner...
Scannez ce QR Code pour accéder à la page de ce numéro sur Cairn.info.

Distribution électronique Cairn.info pour Institut français des relations internationales.
Vous avez l'autorisation de reproduire cet article dans les limites des conditions d'utilisation de Cairn.info ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Détails et conditions sur cairn.info/copyright.
Sauf dispositions légales contraires, les usages numériques à des fins pédagogiques des présentes ressources sont soumises à l'autorisation de l'Éditeur ou, le cas échéant, de l'organisme de gestion collective habilité à cet effet. Il en est ainsi notamment en France avec le CFC qui est l'organisme agréé en la matière.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Cyber : les enjeux pour la défense et la sécurité des Français

Par **Louis Gautier**

Louis Gautier, ancien Secrétaire général de la défense et de la sécurité nationale (2014-2018), est conseiller-maître à la Cour des comptes et directeur de la chaire Grands enjeux stratégiques contemporains de l'université Paris-1 Panthéon-Sorbonne.

En janvier 2018, la France s'est dotée de sa première *Revue stratégique de cyberdéfense*. Ce document analyse les menaces existant dans le cyberespace, tout en constatant les défaillances de la gouvernance mondiale de l'internet. Il clarifie les principes d'organisation de la cyberdéfense française et présente l'État comme le garant de la cybersécurité de la Nation. Il plaide pour le rétablissement de la souveraineté numérique de la France et améliore les dispositifs de coopération public-privé.

politique étrangère

Année électorale et de changement politique, 2017 aura été marquée par des réflexions stratégiques sur la politique de défense et de sécurité de la France. À la veille de l'élection, en avril 2017, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) publiait *Chocs futurs*, rapport consacré à l'impact des transformations technologiques sur notre environnement stratégique et de sécurité. Cette étude prospective à 30 ans avait pour objectif d'appeler l'attention sur certaines évolutions ou révolutions technologiques pouvant modifier les paramètres d'action des armées et des forces de sécurité intérieure. Inscrit dans le temps long de la prévision, *Chocs futurs* poussait néanmoins à des décisions rapprochées pour tenir compte de tendances lourdes comme la banalisation de l'accès à l'espace extra-atmosphérique ou la montée des périls dans le cyberespace. Ce rapport a pu influer sur certains contenus de deux exercices lancés aussitôt après les élections législatives par le chef de l'État : la *Revue stratégique de défense et de sécurité nationale* et la *Revue stratégique de cyberdéfense*.

À la différence notable de *Chocs futurs*, ces documents officiels ont une finalité décisionnelle. Ils ont été commandés et conçus pour orienter

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

les politiques de défense et de sécurité, à commencer par les choix immédiats de programmation militaire. Leurs conclusions furent arrêtées en Conseil de défense en octobre 2017 et janvier 2018.

Ces deux revues, qu'il s'agisse de leurs modalités de préparation ou de leurs traductions concrètes, divergent dans leurs approches, même si leurs conclusions sur la cyberdéfense se recoupent et si la revue de cyberdéfense trouve aussi des débouchés concrets dans le projet de loi de programmation militaire (LPM) 2019-2025[1].

Élaborée en trois mois par une commission de personnalités qualifiées présidée par Arnaud Danjean, la *Revue stratégique de défense et de sécurité nationale*[2], est un document concis qui actualise le *Livre blanc* de 2013[3]. Elle procède à une analyse des menaces auxquelles notre pays est confronté pour redéfinir les missions des armées. Elle constitue l'exposé des motifs et le cadre stratégique de la LPM 2019-2025. Ses conclusions devaient donc être rapidement adoptées pour éclairer la mise en chantier des travaux interministériels sur la programmation.

La *Revue stratégique de cyberdéfense*, dont une version publique a été mise en ligne le 14 février 2018[4], n'était pas soumise à de telles contraintes. Suite à une décision présidentielle, le SGDSN s'est vu confier par mandat du Premier ministre en date du 21 juillet 2017 la conduite de cette *Revue* dont les travaux se sont étendus sur six mois. Exercice inédit pour notre pays qui n'avait auparavant, à la différence des États-Unis ou du Royaume-Uni, jamais conduit une telle réflexion[5], la *Revue* jette les bases d'une ambition de cyberdéfense pour notre pays. Elle dégage orientations générales et recommandations opérationnelles. Certaines de ses propositions ont trouvé un véhicule porteur dans le projet de LPM 2019-2025, la plupart des autres étant en attente de transformations juridiques ou budgétaires.

---

1. Notamment en ce qui concerne l'augmentation des effectifs du ministère des Armées affectés à la cyberdéfense (Direction générale de l'armement – DGA, commandement de la cyberdéfense – COMCYBER et Direction générale de la sécurité extérieure – DGSE) ou, de façon plus opportuniste, dans l'article 19 de la LPM.
2. *Revue stratégique de défense et de sécurité nationale 2017*, Paris, DICoD, 2017, disponible sur : <www.defense.gouv.fr>.
3. Ministère français de la Défense, *Livre blanc. Défense et sécurité nationale*, Paris, La Documentation française, 2013, disponible sur : <www.livreblancdefenseetsecurite.gouv.fr>.
4. SGDSN, *Revue stratégique de cyberdéfense*, 2018, disponible sur : <www.sgdsn.gouv.fr>.
5. La prise de conscience par les pouvoirs publics de l'acuité des enjeux de sécurité et de souveraineté liés à la numérisation n'est pourtant pas nouvelle. On peut songer à la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en 2009 et à sa montée en puissance, mais aussi à l'élaboration en octobre 2015 d'une Stratégie nationale pour la sécurité du numérique, et, sur le plan international, à l'organisation par l'ANSSI et l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), en avril 2017, d'une conférence sur les perspectives d'édification de la paix dans le cyberespace.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

La mise en perspective des trois documents permet de cerner ce qu'ils ont en partage sur le plan prospectif, notamment quant aux effets de la révolution numérique. Une inquiétude les traverse, liée aux sauts technologiques qui bouleversent déjà notre quotidien – *big data*, objets connectés, robotisation du champ de bataille –, ou qui s'annoncent : intelligence artificielle, neurosciences, ordinateur quantique… Ces transformations ont dès maintenant des conséquences stratégiques majeures. Tantôt elles renouvellent les enjeux de la compétition militaire entre grandes puissances, tantôt elles favorisent l'individualisation des menaces ; tantôt elles ouvrent de nouveaux espaces de conflictualité ; tantôt elles modifient nos paradigmes de sécurité en faisant émerger de nouveaux risques systémiques. C'est une évidence dans le cyberespace, mais aussi hors de cette dimension. Le facteur cyber intéresse désormais autant l'efficacité des systèmes d'armes que la manœuvre militaire elle-même. Plus globalement, pour nos sociétés de plus en plus numérisées et connectées, le risque cyber n'est pas seulement un risque d'atteinte à la sécurité informatique, mais à la sécurité tout court.

L'ambition de la *Revue stratégique de cyberdéfense* est justement de préparer notre pays aux défis globaux de la sécurité à l'ère numérique. Constatant que la France, en dépit d'efforts récemment accentués, accuse encore un déficit en la matière par rapport aux quatre puissances qui partagent avec elle des responsabilités internationales particulières (États-Unis, Chine, Russie et Royaume-Uni[6]), la *Revue* prône le durcissement de nos réseaux et une plus grande réactivité face aux menaces informatiques. Composé de trois parties, ce document livre, pour la première fois dans une production officielle, une évaluation complète des dangers cyber. En définissant le rôle de l'État comme responsable de la cyberdéfense du pays et garant de la cybersécurité de la société, la *Revue* pousse au renforcement de la gouvernance de notre dispositif national de cyberprotection. Elle plaide pour une reconsolidation de notre souveraineté numérique. Elle encourage l'élévation de l'« hygiène informatique » des agents économiques, ainsi que la diffusion auprès des citoyens d'une culture de la cybersécurité.

Les dangers du monde cyber

Le cyberespace, naguère idéalisé comme univers d'échange soustrait à toute entrave et à tout contrôle étatique, se révèle être aussi une dimension dans laquelle se déploient des logiques conflictuelles. Il constitue un terrain propice aux assaillants divers – activistes, groupes criminels,

6. Tous membres permanents du Conseil de sécurité des Nations unies et États nucléaires dotés au sens du Traité de non-prolifération (TNP).

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

acteurs étatiques – susceptibles de poursuivre un large spectre d'objectifs : vol ou chantage, espionnage, mais aussi destruction de ressources informatiques, sabotages et, dans le cas de tactiques dites hybrides, diffusion sur les réseaux de fausses informations et manipulation de l'opinion. Le degré de complexité et d'interconnexion atteint par les réseaux informatiques transforme également la donne générale de sécurité : des failles individuelles peuvent engendrer des risques systémiques, comme l'atteste la propagation massive de logiciels malveillants tels *WannaCry*[7] ou *NotPetya*[8] en 2017.

Des menaces croissantes en intensité, diversité et sophistication

À travers l'examen de nombreux exemples récents, telle l'attaque de 2015 contre TV5 Monde par APT 28 qui a précipité en France une prise de conscience, la *Revue* décrit les modes opératoires d'attaques informatiques en constante augmentation. Un certain nombre de causes contribuent à l'intensification de la menace : niveau insuffisant de la protection des réseaux, prolifération des outils malveillants, professionnalisation des groupes d'attaquants. Notre pays n'est pas à l'abri d'une cyberattaque de grande ampleur entraînant des dommages critiques.

La *Revue*, après avoir hiérarchisé en nombre et gravité les attaques répertoriées, constate que dans la majorité des cas, il s'agit soit d'actes de piratage économique, technologique ou d'espionnage politique, soit de cybercriminalité. Les actes de sabotage apparaissent cependant de plus en plus fréquents. Sont en outre observées des actions de déstabilisation d'acteurs publics ou privés, avec exfiltration puis divulgation massive de données sensibles. Si la plus grande partie des attaques observées concerne des opérations de piratage, de déni de service, des défigurations de site ou des actes de cybercriminalité, le développement d'attaques sophistiquées et furtives (de type APT[9]), avec un fort degré d'anticipation et de préparation, est très préoccupant pour notre sécurité, et pour notre démocratie rendue vulnérable aux tentatives de déstabilisation *via* les réseaux sociaux. Les ingérences observées aux États-Unis lors des présidentielles, détaillées dans le récent rapport du procureur spécial Robert Mueller, ont justifié

7. Cyberattaque mondiale, *WannaCry* a touché 300 000 ordinateurs de 150 pays. Elle est à l'origine du blocage pendant 48 heures du système de santé britannique.
8. Visant l'Ukraine, *NotPetya* a perturbé, en France, pourtant moins touchée que d'autres pays, le fonctionnement de quelques entreprises, à l'instar de Saint-Gobain qui enregistre alors une perte de chiffre d'affaires de l'ordre de 250 millions d'euros.
9. On parle de « menace persistante avancée », ou APT (« Advanced Persistent Threat »), pour désigner des modes d'action concernant des opérations menées dans la durée avec une prise en main partielle ou totale de réseaux et de bases de données. Ces APT sont classées et numérotées, dans l'ordre de leur occurrence chronologique. Ainsi, de récentes APT 28 et 29, autrement intitulées « Pawn Storm » ou « Cosy Bear », ont été communément sourcées comme provenant initialement de services de renseignement russes.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

en France, lors des élections de 2017, des mesures de surveillance et de précautions *ad hoc*. De telles ingérences ont aussi été évoquées comme ayant pu peser sur le référendum britannique relatif au Brexit.

Toutefois, parmi toutes les entreprises hostiles, celles que l'on doit à l'avenir le plus redouter en raison de possibles effets létaux, et contre lesquelles il faut se prémunir, sont les actions de sabotage ciblant les systèmes de sécurité (dans les communications, l'énergie et les transports principalement). En recherchant à l'avance, et en exploitant certaines failles informatiques, des accidents peuvent être provoqués et des dommages matériels graves causés. Un nombre limité d'États seulement est en mesure aujourd'hui de mener de telles actions de longue main, à partir de moyens d'infiltration, de capacités de commandement et de contrôle des réseaux, et avec des infrastructures d'exploitation des données. Mais ce nombre est appelé à croître et, demain, des organisations mafieuses ou terroristes pourraient chercher à exercer de tels chantages ou menaces.

Les actions de sabotage ciblent les systèmes de sécurité

À côté de ce type d'attaques dirigées et ciblées, il faut également prendre garde à des effets de vague provoqués intentionnellement ou accidentellement, induits par la propagation aveugle de logiciels malveillants, comme dans le cas de *NotPetya* visant à l'origine l'Ukraine et largement répandu sur notre continent. Alors que l'on observe la croissance des risques et le déploiement de capacités offensives par certains États, souvent aidés dans leur entreprise par des groupes de hackers mercenaires, la régulation internationale du cyberespace est, pour l'heure, inexistante.

Un monde cyber sans règle

L'augmentation des cybermenaces s'inscrit dans un contexte international où nul accord multilatéral n'a pu être trouvé pour établir des principes de gouvernance et des normes réglant les relations dans le cyberespace entre les États d'une part, les acteurs privés et publics d'autre part. Si les négociations du Groupe des experts gouvernementaux sur la cybersécurité (GEG), organisées depuis 2004 sous l'égide des Nations unies, avaient en effet permis de reconnaître l'applicabilité du droit international au cyberespace, et de consolider un socle d'engagements volontaires des États, l'échec du GEG 2016-2017 révèle une divergence fondamentale entre grands pays, notamment entre les membres permanents du Conseil de sécurité, sur l'architecture de sécurité devant régir les responsabilités étatiques et les relations interétatiques à l'ère numérique.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Face à l'échec de ces dernières négociations, la *Revue* préconise une reprise de l'initiative par la France, notamment à l'Organisation des Nations unies (ONU), à l'Organisation de coopération et de développement économiques (OCDE) et dans le cadre du G20, en vue de promouvoir des normes de comportement et des mesures de confiance dans le cyberespace. La Revue réaffirme certaines positions de notre pays. La France, résolument hostile à la pratique du *hack-back*[10], milite d'ores et déjà pour une prohibition de la vente à des acteurs privés des armes numériques et outils cyber offensifs ; elle est favorable au renforcement des mécanismes de contrôle de leur exportation hors de l'Union européenne.

Dans un univers numérique conflictuel, les opérateurs mondiaux comme les GAFAM (Google, Apple, Facebook, Amazon et Microsoft), ont évidemment un rôle à jouer, et des responsabilités à assumer alors que l'extraterritorialité de leurs activités, et l'appropriation massive des données qu'ils collectent et stockent, posent problème pour l'application de la loi des États[11]. Leur volonté de participer à l'édiction et à l'application de disciplines et de normes internationales reste floue, et forte leur résistance à se voir imposer des obligations par les États. Leur difficile mobilisation pour lutter contre la propagande de Daech sur internet le manifeste, tout comme les révélations découlant du scandale de Cambridge Analytica.

Dans un environnement dangereux et sans règles, il était devenu urgent de renforcer la main de l'État français, d'autant que notre modèle de cyberdéfense, établi sur des bases empiriques et largement prédéfini à l'origine par les capacités technologiques de la Direction générale de la sécurité extérieure (DGSE) et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), restait peu formalisé.

L'État, responsable de la cyberdéfense de la Nation

La cyberdéfense de notre pays repose sur un modèle d'organisation et de gouvernance séparant les missions et capacités offensives des missions et capacités défensives. Ce modèle se distingue du modèle choisi par

10. La détention de capacités cyberoffensives n'est en effet pas le monopole des États. Le secteur privé possède aussi de tels outils qui permettent de déployer des contre-mesures « agressives ». En France, le droit n'autorise pas les entreprises à répliquer lors d'une cyberattaque, pour récupérer les données dérobées ou s'en prendre aux infrastructures système de leurs attaquants. Aux États-Unis, une proposition de loi déposée par le sénateur Tom Graves – the *Active Cyber Defense Certainty* (ACDC) *Act* – veut remettre en cause le *Computer Fraud and Abuse Act* qui interdit également la pratique du « reverse hacking » sur le sol américain.

11. À l'exception notable des États-Unis qui, comme en matière fiscale, cherchent à appliquer un droit de suite s'agissant des données intéressant leur sécurité nationale ou leurs citoyens, *via* l'action des agences fédérales et du système judiciaire américain, ce qui s'avère problématique, notamment pour les Européens, tant la pratique est unilatérale et sans réciprocité.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

les pays anglo-saxons, dont les capacités de cyberdéfense sont concentrées dans la communauté du renseignement (National Security Agency – NSA, Government Communications Headquarters – GCHQ). Il présente d'incontestables avantages. En distinguant les missions et les moyens dédiés à la cyberprotection, confiés à l'ANSSI, de ceux dont l'objectif est le renseignement et les actions offensives, il facilite l'acceptation des interventions de l'État en matière de sécurité des systèmes d'information, tant dans l'administration que dans la sphère économique. Toutefois, notre modèle manquait d'une confirmation de ses principes de base, d'une description précise de son organisation et de sa gouvernance opérationnelle, d'une définition des objectifs assignés aux services de renseignement, autres que la DGSE et aux services judiciaires.

Clarifier les principes d'organisation de la cyberdéfense française

La *Revue stratégique de cyberdéfense* a d'abord précisé les missions de cyberdéfense : prévention, anticipation, protection, détection, attribution, réaction (remédiation, répression des infractions, actions militaires), et comment elles étaient réparties entre divers services ou agences de l'État : ANSSI, commandement de la cyberdéfense (COMCYBER), Direction générale de l'armement (DGA), DGSE, Direction générale de la sécurité intérieure (DGSI). Qu'il s'agisse de missions défensives ou offensives, vu la limite actuelle des moyens français[12], la *Revue* plaide pour un accroissement significatif des effectifs, à l'ANSSI, au ministère des Armées, à l'Intérieur et à la Justice. La consolidation du socle technologique constitué par l'ANSSI, la DGA et la DGSE, où sont réunies les compétences les plus pointues, est en particulier une priorité.

La *Revue* clarifie ensuite l'organisation et la gouvernance de la cyberdéfense. Elle formalise et met sur pied les chaînes opérationnelles, et consolide leurs modalités de direction et de coordination, sur les plans technique et stratégique, et pour la gestion des crises.

La chaîne « protection », placée sous la responsabilité du Premier ministre, a pour objet d'assurer de façon préventive et en cas d'attaque informatique la sécurité des réseaux de l'État et des opérateurs d'importance vitale (OIV). Le SGDSN anime cette chaîne, la responsabilité de la conduite des opérations étant confiée au directeur général de l'ANSSI. Par délégation de l'ANSSI, le COMCYBER est responsable de la conduite des opérations dans le périmètre du ministère des Armées. La chaîne « action

12. À titre d'exemple, les effectifs cumulés de l'ANSSI et de la DGSE sont inférieurs de plus de la moitié à ceux du GCHQ britannique ; le personnel de l'ANSSI (550 personnes) représente aujourd'hui un peu plus de la moitié du Bundesamt für Sicherheit in der Informationstechnik (BSI), son homologue allemand.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

militaire », sous le commandement du président de la République, chef des Armées, est en charge de la lutte informatique active et de la conduite des opérations de défense nationale. La chaîne « renseignement », sous l'autorité du gouvernement, mobilise principalement la DGSE et la DGSI, et les quatre autres services de la communauté du renseignement. Cette chaîne est particulièrement active en matière d'anticipation et d'attribution des attaques informatiques. La chaîne « investigation judiciaire » regroupe l'action des services de police et de gendarmerie, ainsi que celle de la justice face à la cybercriminalité.

La *Revue* renforce par ailleurs les mécanismes de gouvernance, avec l'officialisation ou la création d'instances de coordination chargées de la planification des moyens ou de la gestion des crises : le Comité directeur de la cyberdéfense, le Comité de pilotage de la cyberdéfense, le Centre de coordination (C4).

En complément des actions de prévention ou de remédiation, il convenait aussi d'ajuster nos ripostes et leur gradation, qu'elles se situent dans le domaine cyber (contre-ingérence, contre-mesures) et celui des actions clandestines, ou qu'elles impliquent des réactions visibles : diplomatiques, politiques, économiques, voire, en cas d'atteinte à nos intérêts stratégiques, militaires. Envisageant une doctrine d'action en cas d'agression, la *Revue stratégique de cyberdéfense* décline quelques options. Celles-ci, confidentielles, doivent être préparées à l'avance pour permettre aux autorités de réagir dans le *tempo* de la crise. Ces options dépendent d'un schéma de classement des attaques informatiques qui, lui, est public et respecte les normes juridiques nationales et internationales, notamment l'article 51 de la Charte des Nations unies. Ce schéma constitue un outil d'aide à la décision pour choisir et proportionner nos répliques. Il appuie une doctrine d'action dont le but est aussi de décourager les agressions par la menace de rétorsions. Enfin, ce schéma convergeant avec celui adopté par les États-Unis, permet de s'entendre avec nos alliés pour étalonner de possibles réactions communes, comme des mesures de coercition ou des sanctions.

Ajuster nos ripostes et leur gradation

Aussi pertinents et indispensables qu'ils soient, les modèles d'organisation et les éléments de doctrine sont cependant accessoires par rapport à l'objectif premier que constituent le durcissement de la sécurité et le renforcement de la résilience des réseaux informatiques de l'État, et de ceux des opérateurs d'importance vitale, ou en charge de services essentiels. Face à une attaque cyber, il faut en effet pouvoir garantir aux autorités publiques et à nos concitoyens la continuité de fonctions primordiales pour le pays.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Consolider la cyber cuirasse du pays

À l'image du corps humain qui, en situation de stress, préserve d'abord ses organes vitaux, les fonctions indispensables à la survie de la Nation doivent pouvoir résister à un choc cyber massif. Cette bonne tenue au choc dépend de la résistance, de la redondance et de la résilience de certains réseaux de l'État et de quelques délégataires de services publics. Au premier rang des priorités figure, à côté des impératifs de la défense nationale, la cyber-protection des secteurs de la communication et de l'approvisionnement électrique qui conditionne le fonctionnement, même en mode dégradé, des services en charge de la protection civile, de la sécurité publique, des urgences médicales et des hôpitaux. Au-delà de ces réseaux les plus sensibles, qui doivent bénéficier d'une sécurité sans compromis, l'ensemble des réseaux publics doit également faire l'objet d'une attention particulière, y compris ceux des collectivités locales. La *Revue* propose à cette fin, d'appuyer la création de pôles régionaux de ressources en cybersécurité, auxquelles contribueraient les collectivités locales, les équipes régionales de l'ANSSI et de certains services administratifs déconcentrés.

La *Revue* considère que les projets informatiques de l'État qui sont les plus importants ou les plus sensibles devraient systématiquement être soumis, dès leur phase de lancement, à l'avis de l'ANSSI. Elle préconise également d'optimiser l'utilisation du réseau interministériel de l'État, et d'inciter les ministères à recourir systématiquement aux services de sécurité qu'il offre – ce qui n'est pas le cas aujourd'hui. Ces fonctions de sécurité permettent en effet le blocage des trafics malveillants.

La *Revue* présente, en outre, un ensemble de propositions concernant les opérateurs d'importance vitale, nécessitant l'adoption de dispositions législatives ou réglementaires. Elle propose de hausser le niveau d'exigence des règles de sécurité applicables aux opérateurs des secteurs des communications électroniques et de l'approvisionnement en énergie électrique. Elle recommande également de porter une attention particulière aux entreprises prestataires de services numériques pour les OIV. Enfin, la *Revue* se déclare favorable à une transposition ambitieuse de la directive NIS[13], qui constitue une opportunité pour la France de protéger, au-delà du périmètre des OIV, un champ plus large d'activités. La *Revue* prend en compte

13. La directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 dite directive « Network and Information Security », autrement appelée directive NIS, doit être transposée en droit français le 9 mai 2018 au plus tard. Cette directive a pour objet d'assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne. Dans ce contexte, le projet de loi « portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité » a été déposé au Sénat le 22 novembre dernier.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

les défis nouveaux que représente la protection de nos élections contre le risque cyber, et celle de notre vie démocratique contre les manipulations de l'opinion *via* les réseaux sociaux. Elle insiste sur le fait qu'une éventuelle généralisation du vote par internet, si elle était envisagée, devrait être soumise à des prérequis rigoureux, comme le déploiement préalable d'une identité numérique robuste et généralisée à l'ensemble des électeurs. Elle recommande par ailleurs la mise en place d'un observatoire chargé d'analyser la propagation des *fake news* et de proposer, en concertation avec les autorités publiques juridiquement compétentes et les opérateurs, une démarche visant à en circonscrire la diffusion.

L'article 19 de la LPM

Face à des attaquants utilisant des moyens indirects pour atteindre leurs cibles, une implication accrue des opérateurs de communications électroniques et des hébergeurs apparaît nécessaire. Si l'ANSSI a développé des coopérations étroites avec certains de ces acteurs, le cadre contractuel dans lequel s'inscrit cette coopération est aujourd'hui insuffisant. Les mesures proposées par la *Revue*, portées par l'article 19 du projet de loi de programmation militaire 2019-2025, permettront de resserrer les mailles du filet et de jouer, en matière de prévention et de détection des attaques, sur une complémentarité des actions publiques et privées. Cette évolution législative va dans un sens triplement bénéfique pour la cyberdéfense du pays, la sécurisation des prestations offertes par les opérateurs, la protection des flux de données des utilisateurs finaux.

Le premier volet du dispositif légal proposé consiste à autoriser les opérateurs de communications électroniques à mettre en œuvre des systèmes de détection dans leurs réseaux pour repérer les attaques informatiques visant leurs abonnés. Il s'agit de dispositifs techniques qui, à partir de marqueurs d'attaque, analysent le trafic sans s'intéresser au contenu des messages. Pour leur permettre de détecter des attaques sophistiquées, l'ANSSI fournira aux opérateurs certains des marqueurs issus de sa propre base de données. En cas d'attaque informatique, les systèmes de détection déployés par les opérateurs produiront une alerte de sécurité. L'opérateur en informera alors l'ANSSI. Le second volet du dispositif consiste à autoriser l'ANSSI, si elle a connaissance d'une menace grave, à mettre en place sur les serveurs d'un hébergeur ou les réseaux d'un opérateur de communications électroniques un dispositif de détection local. Ce régime collaboratif, entre l'ANSSI et les opérateurs de communication, pour mieux traquer les virus, détecter précocement les attaques et en neutraliser les effets, sera contrôlé par l'Autorité de régulation des communications électroniques et des postes (ARCEP).

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

L'État, garant de la cybersécurité de la société

La troisième partie de la *Revue* part du constat que l'élévation d'une haute muraille pour assurer la cyberdéfense de la Nation ne suffit pas, si le rempart peut être sapé à la base. Une bonne cyberdéfense suppose un environnement général moins permissif, avec l'accroissement du niveau de cybersécurité de la société tout entière.

Pour cela, comme condition et finalité il convient en premier de soutenir une souveraineté numérique chancelante.

Le rétablissement de notre souveraineté numérique

À la différence des États-Unis ou de la Chine qui peuvent compter sur une industrie puissante, et s'appuyer sur des équipementiers mondiaux ou des opérateurs de poids, la capacité de la France à dégager dans l'espace numérique des marges autonomes d'appréciation, de décision et d'action, dépend de la qualification d'une offre de confiance par l'État et de la conservation de certaines compétences et technologies clés.

Parmi les technologies dont la maîtrise est nécessaire à l'exercice de notre souveraineté numérique, les plus spécifiques s'imposent d'évidence. Elles concernent le chiffrement des communications, la fabrication d'outils de détection et d'attaque, la mise en œuvre de radios mobiles professionnelles de nouvelle génération avec l'essor de la 5G. La *Revue stratégique de cyberdéfense* recommande donc logiquement le maintien d'une industrie nationale de pointe dans le domaine du chiffrement IP, ainsi que l'appui à l'émergence d'entreprises de référence dans le domaine de la *threat intelligence*. La *Revue* souligne l'importance des enjeux de souveraineté autour de l'intelligence artificielle, en particulier de la maîtrise des systèmes d'intelligence artificielle appliquée à la cyberdéfense. Constatant l'échec des tentatives de mise en place d'un *cloud* souverain, la *Revue* met néanmoins en garde contre la conservation de certaines données hors de France et la domination du marché du *cloud* par un nombre réduit d'acteurs étrangers. Face à ce constat, la *Revue* avance diverses solutions parmi lesquelles, pour les données publiques, leur stockage dans des entrepôts internes à l'administration et le recours à des prestataires de *cloud* bénéficiant d'une qualification par l'ANSSI avec la mise en œuvre de techniques de chiffrement homomorphes.

L'importance des enjeux de souveraineté autour de l'intelligence artificielle

Au-delà de ces conclusions concernant des aspects spécifiques mais très discriminants pour la sécurité nationale, le rétablissement de notre

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

souveraineté numérique passe par des politiques incitant les grands industriels français (Thalès, Atos, Orange, Airbus…) à compléter leur offre de produits et de services de cybersécurité, à favoriser la création d'entreprises de taille intermédiaire en aidant les petites et moyennes entreprises (PME) les plus performantes, à accompagner le développement des start-ups. L'émergence d'un marché européen de la cybersécurité est aussi un objectif à la réalisation duquel la France doit s'attacher, en protégeant des entreprises jugées sensibles face aux appétits des investisseurs étrangers, et en réservant aux seules entreprises européennes l'accès à certains marchés publics.

Améliorer le cadre de certification, encourager le développement de normes professionnelles

L'État intervient comme garant de la cybersécurité de la société comme prescripteur, certificateur et pourvoyeur de solutions de sécurité. Ces dernières années, il a été particulièrement actif dans l'édiction de normes de cybersécurité, notamment suite à l'adoption dans la LPM de dispositions confortant le rôle de l'ANSSI[14], tant pour auditer les réseaux et systèmes critiques que pour homologuer des solutions de sécurité. Mais le cadre actuel de certification est centré sur l'agrément de services ou de produits de haut niveau de sécurité. Il est mal adapté à l'évaluation de produits d'utilisation courante, comme les objets connectés pour lesquels il présente un coût et des délais prohibitifs. C'est pourquoi la *Revue* préconise la mise en place d'une certification élémentaire de cybersécurité, et une harmonisation au niveau européen de la certification de sécurité, en veillant à ce qu'elle s'effectue par le haut, sur les standards les plus robustes. Il apparaît également judicieux de favoriser sur le plan européen l'extension de la labellisation des produits de sécurité et des pratiques d'évaluation et de notation du risque cyber.

À cet égard, la *Revue* appelle à une implication plus forte des acteurs économiques dans la définition et la construction des pratiques et solutions de sécurité, en densifiant leur participation à la mise en place d'une offre de confiance, en proposant des disciplines sectorielles voire des normes professionnelles de précaution face aux risques cyber. Les spécialistes des marchés financiers, les commissaires aux comptes et les assureurs ont évidemment un rôle à jouer dans la définition et le contrôle de critères d'appréciation de ces risques. La constitution d'une base de données européenne

14. Notamment la prise de décrets et d'arrêtés sectoriels en application de l'article 22 de la loi de programmation militaire, loi du 18 décembre 2013.

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

répertoriant les incidents cyber pourrait faciliter le développement des mécanismes assurantiels et d'audit du risque cyber. En outre, la transformation numérique, qui conduit à l'automatisation et à la connexion massive des objets, impose de lier la prise en compte conjointe par domaine d'activité des risques physiques et des risques cyber, en particulier lorsque le fonctionnement de ces automates ou objets est susceptible d'avoir un impact sur la sécurité des personnes. Cette réflexion ne peut s'effectuer que par milieux ou par métiers, avec une forte implication des entreprises de chaque secteur d'activité. Il est essentiel que les acteurs-clés de la régulation sectorielle appréhendent le risque de cyberattaques au même titre que les autres risques, et émettent des exigences et des normes de cybersécurité adaptées.

La diffusion de la culture de la sécurité numérique dans la société

Il est indispensable de sensibiliser l'ensemble de la société, et chaque citoyen, au risque cyber. Dès l'école et le collège doit être dispensée une éducation au numérique incluant la maîtrise des bonnes pratiques et des règles de cybersécurité. Pour y parvenir, il est urgent d'intégrer cet apprentissage dans les parcours de formation initiale et continue des enseignants. Un *massive open online course* (MOOC) dédié conçu par le ministère de l'Éducation nationale avec le soutien de l'ANSSI est d'ailleurs envisagé comme première réponse.

Le niveau d'ambition de la France en matière de cyberdéfense est aujourd'hui contraint par la pénurie en personnels spécialisés, et par de fortes tensions en matière de recrutement et de gestion des ressources humaines. Le vivier, déjà trop étroit pour faire face à la demande des administrations et des employeurs spécialisés en sécurité du numérique, ne parvient pas à satisfaire un marché de l'emploi en extension rapide dans ce domaine. Il faut donc très activement augmenter l'offre de formations techniques et supérieures dans les prochaines années. Il s'agit là d'un chantier immense pour l'Éducation nationale et le ministère de l'Enseignement supérieur. Après avoir traité de nombreux défis, la *Revue* conclut sur ce dernier enjeu qui les conditionne tous.

***

Alors que des attaques informatiques sont susceptibles de porter gravement atteinte à la sécurité de la Nation, et que le niveau de la cybersécurité des entreprises et des citoyens doit être substantiellement relevé, la *Revue*

stratégique de cyberdéfense, à la suite d'une analyse complète et sans fard de la situation, débouche sur sept recommandations principales :

- accorder un haut degré de priorité à la protection des systèmes d'information de l'État et de certains opérateurs ;
- adopter une posture active de découragement des attaques et de réaction coordonnée ;
- rétablir pleinement notre souveraineté numérique ;
- améliorer l'efficacité de la réponse pénale efficace à la cybercriminalité ;
- promouvoir une culture partagée de la sécurité informatique ;
- contribuer à une Europe du numérique confiante et sûre ;
- promouvoir à l'international une gouvernance collective et maîtrisée du cyberespace.

PE

Institut français des relations internationales | Téléchargé le 03/09/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Mots clés
Cyberdéfense
Cybersécurité
Internet
Hacking