Le cyberespace : Un territoire multidimensionnel à défendre, à sécuriser et à protéger

Stéphanie Brochot

Auditrice - Institut d'Études de Géopolitique Appliquée - IEGA

Octobre 2021

ISSN : 2739-3283

Comment citer cette publication :

Stéphanie Brochot, « Le cyberespace : Un territoire multidimensionnel à défendre, à sécuriser et à protéger », Institut d'Études de Géopolitique Appliquée, Paris, 6 octobre 2021.

Institut d'Études de Géopolitique Appliquée - 31 Rue de Poissy 75005 Paris

E-mail : secretariat@institut-ega.org

Site internet : www.institut-ega.org

SOMMAIRE

Dans un système de globalisation et de mondialisation où les frontières ne sont plus clairement définies, toutes les interconnexions et les interactions deviennent des menaces potentielles pour les États qui doivent élaborer de nouvelles stratégies de défense, de sécurité et de renseignement afin de recueillir, évaluer, analyser, anticiper, protéger et défendre leur territoire.

Afin de maintenir un équilibre au sein des territoires et surtout maintenir la souveraineté étatique, la France a mis en évidence la nécessité de développer des techniques de renseignement en se dotant de moyens humains, financiers et matériels adaptés pour répondre aux enjeux majeurs des menaces liées au numérique.

I. Mise en perspective des services de renseignement

Les services de renseignement en France ont évolué de manière importante depuis des décennies avec notamment des prises de conscience multidimensionnelles en termes de sécurité nationale et de défense.

Cette évolution structurelle et organisationnelle a débuté depuis les années soixante avec les mouvements nationalistes et s'est consolidée avec les premiers attentats islamistes sur le territoire. Ces atteintes à la nation ont amené les services de renseignement à se réorganiser et à développer de nouveaux moyens et des nouvelles techniques.

Cette restructuration a donné lieu à un cadre législatif spécifique dans ce domaine d'intervention avec notamment la loi n° 86-1020 du 9 septembre 1986[1] relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État. Une législation ayant pour objectifs majeurs d'élaborer et de construire des dispositifs à la fois encadrés et opérationnels avec une attention particulière aux réponses coordonnées en termes de judiciarisation des faits d'attentats terroristes.

Une véritable stratégie française de lutte antiterrorisme se met en place. Différentes législations vont émerger jusqu'en 1996 avec notamment la loi n° 96-647 du 22 juillet 1996[2] afin de renforcer la répression du terrorisme et les atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire.

Un apport majeur pour les services de renseignement où une modalité nouvelle est introduite, celle de l'infraction spécifique d'association de malfaiteurs en relation avec une entreprise terroriste qui permet des interventions en amont. Les attentats terroristes de 2001 aux États-Unis ont souligné l'importance d'une communauté du renseignement dont l'expression est apparue en France autour des années 2000.

Les attentats de 2015 ont mis en lumière les écueils de l'organisation des services de renseignement en termes d'éclatement des services et de dysfonctionnement de coordination malgré les tentatives qui ont été élaborées pour améliorer ces faiblesses avec, notamment, la création en 2008 d'un coordonnateur du renseignement et du contreterrorisme.

Actuellement, les services de renseignement s'organisent en deux groupes. Ceux du premier cercle dont la direction générale de la sécurité intérieure (DGSI) qui est désignée comme étant le chef de file en

[1] Légifrance : Loi n° 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme <legifrance.gouv.fr>

[2] Légifrance : Loi n° 96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire <legifrance.gouv.fr>

matière de sécurité intérieure, et les services du deuxième cercle qui contribuent à ce maillage communautaire du renseignement français.

Les services de renseignement du premier cercle dont la DGSI :

→ La direction générale de la sécurité extérieure (DGSE) ;
→ La direction du renseignement et de la sécurité de la défense (DRSD) ;
→ La direction du renseignement militaire (DRM) ;
→ Le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) ;
→ Le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin).

Les services de renseignement du deuxième cercle :

→ La sous-direction anticipation opérationnelle (SDAO) ;
→ La préfecture de police de Paris ;
→ Le service central du renseignement territorial (SCRT) ;
→ La sous-direction anticipation opérationnelle (SDAO) ;
→ Le bureau central du renseignement pénitentiaire (BCRP) et les cellules interrégionales du renseignement pénitentiaire (CTRP).

Les articles[3] L811-1 et L811-2 du code de sécurité intérieure posent le cadre général d'intervention des services de renseignement en indiquant d'une part que *« la politique publique de renseignement concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation » ;* et d'autre part, que *« les services spécialisés de renseignement sont désignés par décret en Conseil d'Etat. Ils ont pour missions, en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces ».*

La numérisation, du fait des évolutions rapides, a eu pour effet de complexifier des systèmes d'information, les architectures des réseaux dans les établissements et les structures. À cette complexification se rajoute un enchevêtrement des dispositifs et des réseaux induisant des fragilités numériques.

En parallèle, un constat est effectif face à l'attente des individus d'avoir de nouvelles technologies toujours plus performantes et ceci au détriment de la sécurité individuelle et collective de la société mais aussi au détriment des libertés individuelles. Cela pose une

[3] Légifrance : Code de la sécurité intérieure : articles L811-1 et L811-2, version en vigueur au 15 avril 2021 <legifrance.gouv.fr>

problématique essentielle en matière de sécurité et défense face aux menaces numériques.

II. Les enjeux multidimensionnels des services de renseignement liés aux numériques

Approche sémantique et conceptuelle des cyberattaques à l'intérieur du cyberespace

Il est important dans un premier temps de comprendre ce que recouvre le cyberespace :

« *Le cyberespace, c'est d'abord et avant tout un espace d'information généré par l'interconnexion globale des systèmes d'information et de communication, dans lequel les données sont créées, stockées et partagées. Le terme désigne à la fois : l'infrastructure physique qui est à la source de cet environnement, à savoir les différents éléments qui composent l'internet, ce réseau planétaire de réseaux informatiques, comme les câbles, les serveurs, les routeurs, les satellites et tous les appareils connectés qui sont ancrés dans le territoire géographique physique et politique ; et l'espace intangible dans lequel circulent les données, l'information et les idées, l'espace où se produisent des interactions entre les individus qui sont derrière leur écran partout dans le monde à une vitesse quasi instantanée* »[4].

Le cyberespace est constitué de différentes couches :

→ ***Couche matérielle*** qui regroupe tous les matériels informatiques type ordinateurs et câbles sous-marin notamment.

→ ***Couche technique dite « couche logicielle »*** qui implique tous les grands acteurs de production de données tels que les GAFAM côté Amérique - Google, Apple, Facebook, Amazon et Microsoft ou BATX côté Chine - Baidu, Alibaba, Tencent et Xiaomi. Cette couche va être plus commerciale et économique.

→ ***Couche sémantique dite « couche informationnelle »*** qui va se développer par le Big Data. Cette couche est la plus complexe et il est difficile d'en avoir une vision globale.

Concernant l'approche conceptuelle d'une cyberattaque, il est important de rappeler qu'elle est définie de manière générale comme étant le fait de mettre en place un acte de malveillance envers des systèmes informatiques. L'attaque consiste à cibler différents dispositifs informatiques. Cela peut passer par des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques ou des appareils communicants comme les téléphones mobiles, les smartphones ou les tablettes.

[4] Frédéric Douzet : Le cyberespace, un enjeu majeur de géopolitique, La revue des médias, 2016, 2019 <https://larevuedesmedias.ina.fr/>

Approche par attaques et par couches :

→ ***Couche matérielle - Principe de fulgurance - le sabotage*** se présente sous la forme d'une panne organisée**.** Selon le type d'atteinte recherché, elle frappe tout ou une partie des systèmes informatiques.

→ ***Couche logicielle - Principe de discrétion - l'espionnage*** a pour objectif de récupérer le plus de données sans que l'organisation ne s'en rende compte.

→ ***Couche sémantique - Principe de déstabilisation - la subversion*** s'attache à utiliser de l'information pour décrédibiliser et atteindre l'image d'une entreprise, d'un État.

Dans le cyberespace, considéré comme un nouveau théâtre d'affrontements, des enjeux multidimensionnels existent, ce qui implique pour les services de renseignement de réorganiser leurs moyens et leurs techniques de renseignement.

Les enjeux et les impacts du cyberespace

Les évolutions plurifactorielles ont amené la communauté du renseignement français à développer une nouvelle stratégie de défense et de renseignement. L'élaboration de livres blancs est l'un des résultats de ces transformations et de cette prise de conscience face aux enjeux sécuritaires et de défense.

L'évolution sémantique sociétale met en évidence ces changements de doctrines en lien avec les nouvelles formes de menaces sur le territoire, faisant passer la dénomination de défense nationale à la défense, puis de la défense à la défense et à la sécurité nationale. La sécurité intérieure et la sécurité extérieure sont désormais liées.

Ce nouveau paradigme *« prend en compte les enjeux de la sécurité intérieure du XXI^{ème} siècle, en dessinant le pacte de protection et de sécurité des Français, plaçant l'humain au cœur de l'action »*[5].

Le dernier livre blanc élaboré en novembre 2020 intitulé *« le livre blanc de la sécurité intérieure »* met en exergue un principe essentiel de sécurité à hauteur d'homme et présente la source humaine comme un axe majeur. D'autres éléments clefs ont été présentés, notamment :

→ Le renseignement d'origine spatiale et la lutte contre la prolifération,
→ Le renseignement structuré en France,
→ Un cadre juridique adapté.

Les enjeux multiples face à la numérisation de la société ont fait émerger de nouvelles formes de menaces. Nous pouvons citer les manipulations informationnelles, une problématique d'influence pouvant induire des répercussions importantes sur un territoire voire des

[5] Ministère de l'intérieur : Le Livre blanc de la sécurité intérieur, novembre 2020, p.3 <livre-blanc-de-la-securite-interieure.pdf

crises sociétales majeures, notamment en lien avec la légitimité d'un État. Ce développement numérique à largement favorisé l'interconnexion entre les individus, les entreprises, les structures étatiques et toutes autres formes de réseaux. Cela a impliqué et implique de nombreuses sources et données qui permettent, d'une part, de créer des potentialités importantes en termes d'innovation, de nouvelles technologies et, de ce fait cela contribue au rayonnement étatique. D'autre part, cela engendre et met en exergue des vulnérabilités pouvant entraîner des risques voire des dangers imminents pour la sécurité des territoires.

L'utilisation de l'outil numérique peut être un facilitateur, un espace d'entre-soi pour les individus malveillants, notamment avec le Dark Web permettant par exemple de se procurer des armes en toute discrétion.

Dans le secteur numérique, il est aussi plus difficile de retrouver les cybercriminels dont la traçabilité avec le flux massif de données ouvertes n'est qu'une source relative. C'est aussi un espace où les individus sont moins détectables et moins visibles ce qui demande aux services de renseignement une adaptation constante.

III. Evolution du cadre juridique des services de renseignement dans le cyberespace

Le cadre légal dans lequel s'inscrivent les services de renseignement s'oriente autour d'un principe clef qui est le respect de la vie privée.

L'article L. 801-1 du code de la sécurité intérieure dispose : *« le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité »*[6].

Ce principe à valeur constitutionnelle est remis en cause afin de garantir la sécurité, l'intégrité et la défense du territoire national. Les services de renseignement habilités et missionnés dans un cadre d'intervention bien précis se voient confier des interventions qui induisent la mise en œuvre de techniques de renseignement, notamment la captation de données, l'espionnage clandestin, l'enregistrement et des techniques d'écoute numérique par exemple. Ainsi, le cyberespace est devenu une arme à la fois offensive et défensive. C'est également un théâtre d'opérations qu'il faut prendre en compte avec toutes les spécificités de ces attaques potentielles.

[6] Commission nationale de contrôle des techniques de renseignement : le cadre légal du renseignement <https://www.cnctr.fr/>

Une réglementation, bien que parcellaire, vient construire un cadre d'intervention sécurisant pour l'État qui œuvre dans une démarche à la fois défensive et offensive afin de garantir les intérêts fondamentaux de la nation. La France a reconnu disposer d'une capacité offensive[7] dans le domaine du numérique comme l'indique le livre blanc de la défense en 2008. Celui de 2013 souligne que les attaques peuvent se livrer dans cinq espaces déterminés : terre, air, mer, extra-atmosphériques et cyber.

Le groupe des experts gouvernementaux de l'OTAN a conclu en 2013 que le cyberespace devait être régi par les droits internationaux identiques aux autres espaces, malgré ses spécificités technologiques. Dès lors, il n'existe pas un droit dérogatoire, mais une soumission au droit commun de la guerre. Ainsi, toute attaque informatique constatée en vertu de l'article 51 de la Charte des Nations unies autorise la légitime défense pour la partie agressée. Il est important de souligner qu'il existe un principe de proportionnalité et de nécessité afin d'utiliser la cyber force[8].

La loi n° 2014-1353 du 13 novembre 2014[9] renforçant les dispositions relatives à la lutte contre le terrorisme a introduit des mesures administratives d'entrave et des moyens d'enquêtes supplémentaires. Il convient également de citer la loi n° 2015-1556 du 30 novembre 2015[10] relative aux mesures de surveillance des communications électroniques internationales afin d'élargir les techniques de captation, d'enregistrement et d'écoute ainsi que ***la loi n° 2016-731 du 3 juin 2016***[11] renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

Ce cadre légal met en place de nouveaux moyens administratifs d'entrave. Un service de renseignement pénitentiaire est créé. De nouveaux moyens donnés à Tracfin visant à entraver des sources financières liées aux terrorismes sont également misent en œuvre. ***La loi n° 2017-1510 du 30 octobre 2017***[12] renforçant la sécurité intérieure et la lutte contre le terrorisme met en place des mesures d'urgence afin d'enquêter sur des individus et ainsi permettre une efficacité et une rapidité des services de renseignement.

Dans cette dynamique transnationale des attaques, un commandement Cyber a été constitué le 1er janvier 2017. Il compte près

[7] Jean-Claude Mallet : Livre Blanc Défense et Sécurité Nationale, 2008, p.130 <http://bdc.aege.fr/>
[8] Olivier De Maison Rouge : Quel cadre juridique pour les cyberguerres ? Revue le journal de l'économie, 28 janvier 2020 <https://www.journaldeleconomie.fr/>
[9] Légifrance : Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme <legifrance.gouv.fr>
[10] Légifrance : Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales <legifrance.gouv.fr>
[11] Légifrance : Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale <legifrance.gouv.fr>
[12] Légifrance : Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme <legifrance.gouv.fr>

de 3 400 cyber-combattants. Entre 2014 et 2019, les effectifs du cyber ont doublé. La loi de programmation militaire 2019-2025 a mis en exergue la nécessité d'augmenter de plus de 1000 cyber-combattants les effectifs du commandement Cyber afin de répondre aux besoins croissants des nouveaux enjeux de la numérisation.

IV. Recommandations en cas de cyberattaques

Dès lors qu'il y a la connaissance d'une cyberattaque, il est essentiel d'effectuer un signalement sur le site dédié du gouvernement : ***cybermalveillance.gouv.fr***

Des dispositifs d'alerte, de déclaration de vulnérabilités existent avec le concourt de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dont le rôle est de faciliter une prise en compte coordonnée, ambitieuse et volontariste des questions de cybersécurité en France[13]. Elle accompagne les entreprises, les particuliers ainsi que les services de l'État dans sa démarche de sécurisation proactive de ses infrastructures numériques et digitales.

Il existe, également, des dispositifs mis en place pour signaler les infractions spécifiques aux technologies de l'information et de la communication où un dépôt de plainte peut être constitué. Dans ce cadre, la Police nationale et la Gendarmerie nationale ont mis en place un réseau territorial d'enquêteurs spécialisés en cybercriminalité. Il s'agit aussi de mobiliser les services de renseignement territorial qui sont une source humaine importante permettant de recueillir et d'analyser des informations environnementales et anthropologiques essentielles.

Afin de remédier efficacement à la situation d'une cyberattaque, il semble important de solliciter les modes d'action partagés afin de mobiliser le plus rapidement possible les organisations privées et publiques sur le territoire français et les territoires transnationaux avec lesquels des accords ont été signés.

Le recours aux technologies d'intelligence artificielle dont dispose la France et ses partenaires sont une source d'information essentielle afin d'exploiter, analyser et évaluer le volume important de données et ainsi anticiper et agir au plus vite en cas d'attaque cyber.

[13] L'édito du Directeur général - Agence nationale de la sécurité des systèmes d'information <ssi.gouv.fr>

Conclusion

Les cyberattaques sont une menace forte pour nos sociétés, étant donné le développement grandissant des technologiques numériques et de leur utilisation à des fins malveillantes.

Il est important de poursuivre le développement de connaissances, de techniques et de moyens face à l'impact des cyberattaques sur le territoire. Le portage étatique dans ce cadre est primordial. Pour ce faire, il est donc essentiel de :

→ continuer vers une dynamique de responsabilisation de tous les acteurs face à la cybersécurité,
→ accroître les réponses pénales en matière de cybercriminalité,
→ mettre en place des comités spécialisés ayant pour objectif d'étudier la stratégie, la législation et l'approche la plus adaptée face aux cybermenaces,
→ renforcer les programmes de sensibilisation liés à la cybersécurité,
→ renforcer et développer les centres d'alerte et de réaction aux attaques informatiques.