HADMÉRNÖK

XIV. Évfolyam 1. szám – 2019. március

10.32567/hm.2019.1.23

# LA CYBERSECURITE EN FRANCE: LE PASSE, LE PRESENT ET L'AVENIR

## CYBER SECURITY IN FRANCE: THE PAST, THE PRESENT AND THE FUTUR

MOLNÁR, Dóra

(ORCID : 0000-0002-1476-5253)

molnar.dora@uni-nke.hu

***Résumé***

*La France a déclaré son intention de devenir le premier état mondial en matière de cybersécurité. L'objectif – qui n'est pas inhabituel pour les français – est très ambitieux, mais le chemin à parcourir est encore long. Cependant, il est déjà certain que le pays a fait de grands progrès pendant ces dernières années. Elle a mis à jour son système de documents stratégiques et adapté ses organisations de cybersécurité pour répondre aux exigences de l'époque. Le pays est déjà conscient de la puissance cyber dominante en Europe, mais d'autres résultats sont attendus dans les années à venir. L'étude présente ce processus, en soulignant le point de départ existant au début des années 2010 et en examinant également les opportunités futures.*

***Keywords:*** *la cybersécurité, la France, la stratégie de cyber*

***Abstract***

*France's declared goal is to become the world's leading country in cyber security. Its aim is really ambitious – such as the French usually-, but there is still a long way to go. However, it is already certain that the country has been able to make great progress in recent years. He also updated his strategic document system and cyber security organization to meet the demands of the new age. As a result, the country is already among Europe's leading cyber powers, however further results are also expected in the coming years. The study presents this process, outlining the circumstances existed at the beginning of the 2010s and also looking at future opportunities.*

***Keywords:*** *cyber security, France, Cyber strategy*

..

A kézirat benyújtásának dátuma (Date of the submission): 2019.02.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2019.03.15.

## INTRODUCTION[1]

A partir du moment où les menaces vers et dans le cyberespace ainsi que les menaces activées par le cyberespace se sont développées, la cybersécurité et la cyberdéfense sont devenues un domaine politique clé pour les gouvernements du monde entier. Pendant longtemps, la France a pris du retard sur ses principaux partenaires stratégiques dans ces zones. Cependant, dans ces dernières années, le pays a entrepris des efforts considérables pour rattraper, conduisant à des réformes conceptuelles et organisationnelles et aussi à une augmentation substantielle de ressources. Cet article fournit un aperçu de la base conceptuelle de la politique de cybersécurité francaise, ansi que les éléments de son organisation qui sont indispensables à son opération. Je souligne l'importance de quelques efforts et initiatives récents qui peuvent préciser le futur de la cyberpolitique francaise.

Deux cyberattaques récentes ont montré à quel point la France devait rester vigilante. Les attentats terroristes de janvier 2015 en France – commencés par les attaques contre le magazine Charlie Hebdo – ont été accompagnés d'une vague d'attaques informatiques sur des sites web privés et publics sans précédent. Les pirates extrémistes radicaux ont revendiqué plus de 1500 attaques au cours de cette période. Une cyberattaque plus symbolique a toutefois été organisée le 8 avril 2015 contre la chaîne d'information télévisée de TV5 Monde, qui a abouti à un écran vide et à la diffusion des messages sur des réseaux sociaux prétendant provenir de TV5 Monde, mais soutenant le soi-disant État islamique.

Après ces événements, c'est sans coïncidence que le 20 janvier 2015, Bernard Cazeneuve, ministre de l'Intérieur, a exposé, lors du 7ème forum international de la cybersécurité à Lille, les trois défis de la cybersécurité auxquels la France devait faire face: la cyberdéfense pour protéger les institutions et les intérêts nationaux; assurer un niveau élevé de sécurité des systèmes d'information dans les secteurs publics et privés; et la lutte contre la cybercriminalité. [1] Depuis, ce segment de sécurité est devenu une priorité absolue en France, ce qui se manifeste dans les documents stratégiques. L'étude décrit d'abord l'évolution des stratégies officielles françaises de la cyberespace et montre ensuite comment cela se fait dans la pratique à travers les organisations.

## L'EVOLUTION DE LA STRATEGIE DE CYBERSECURITE FRANÇAISE

L'historique de la réglementation remonte à 2008 quand la France a adopté *le Livre blanc sur la défense et la sécurité nationale*. [2] Dans le Livre blanc, la cybersécurité – ainsi que la dissuasion nucléaire, les missiles balistiques et les sous-marins à propulsion nucléaire – constituaient un domaine prioritaire pour la France 'de conserver ses zones de souveraineté, concentrées sur la capacité nécessaire au maintien de l'autonomie stratégique et politique de la nation'. Dans le Livre blanc, les attaques à grande échelle perpétrées contre des systèmes d'information par des acteurs étatiques et non étatiques constituaient une préoccupation croissante, qualifiant la 'cyberguerre' comme 'préoccupation majeure'. D'après le Livre, la cybersécurité et la défense sont devenues une priorité distincte de la sécurité nationale. Le Livre blanc préconisait l'élaboration d'un nouveau concept de cyberdéfense et, notamment, 'la mise

[1] A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Egyed István Posztdoktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

en place d'une capacité offensive en matière de cyberguerre'. A la suite de cet examen stratégique, la France a constamment amélioré ses politiques et ses capacités en matière de cyber, qui étaient encore très modérées à cette époque. Un résultat majeur du Livre blanc de 2008 a été la création de nouvelles institutions de cybersécurité et de défense, principalement l'Agence nationale de la sécurité des systèmes d'information (ANSSI) – la plus haute agence du pays en matière de cybersécurité et de défense, dotée d'une juridiction nationale (dont la description est mentionnée ci-dessous).

En 2011, l'ANSSI a publié la première stratégie nationale en matière de cybersécurité, intitulée '*Défense et sécurité des systèmes d'information: Stratégie de la France'*. [3] La stratégie définit une grande ambition et trois tâches principales. Grâce à une posture cyber améliorée et à la coopération avec ses partenaires et alliés, la France aspire à devenir une puissance mondiale en matière de cyberdéfense et à appartenir au cercle restreint des nations en tête dans le domaine de la cyberdéfense. Pour atteindre cet objectif, la France doit d'abord préserver sa 'capacité de prendre des décisions par la protection des informations liées à sa souveraineté'. En d'autres termes, les institutions étatiques doivent pouvoir communiquer dans n'importe quelle situation et en toute confiance. Deuxièmement, étant donné l'importance croissante du cyberespace, le gouvernement doit renforcer la cybersécurité des infrastructures nationales critiques. Troisièmement, l'Etat doit garantir un haut niveau de sécurité dans le cyberespace, au-delà des systèmes d'information étatiques et critiques. La stratégie a identifié sept domaines dans lesquels d'autres actions étaient nécessaires:

- la connaissance de la situation;
- les capacités de détection, d'alerte et de réponse;
- les capacités scientifiques, techniques, industrielles et humaines;
- la protection des systèmes d'information de l'Etat et des opérateurs d'importance vitale;
- l'adaptation de la législation;
- la coopération internationale et
- la communication.

Les cyber-efforts français au cours des cinq années suivantes ont été un moteur de changement dans ces domaines. Les efforts n'ont pas ralenti après les élections présidentielles et le changement de président en 2012. Au contraire, le renforcement de la position de la France dans le cyberespace restait une ambition partagée par la plupart des partis politiques. Cela est bien mentionné dans le *Rapport d'Information du sénateur M. Jean-Marie Bockel sur la cyberdéfense.* [4] Le rapport définit dix priorités dont la première consiste à faire de la cyberdéfense (et aussi de la protection des systèmes d'information) une priorité nationale.

En conséquence, le nouveau *Livre blanc - Défense et sécurité nationale* adopté par le nouveau gouvernement en 2013 a considérablement renforcé l'attention portée à la cybersécurité et à la cyberdéfense. [5] Le Livre blanc de 2013 part du principe que 'la croissance continue de la cybermenace, l'importance croissante des systèmes d'information dans la vie de nos sociétés et le développement très rapide des technologies nous obligent à passer à un niveau supérieur pour maintenir les capacités de protection et de défense répondant à ces changements.' La revue stratégique plaide ainsi pour 'une augmentation très substantielle du niveau de sécurité et des moyens de défense de nos systèmes d'information'. En effet, il indique que la capacité de la France à se protéger et détecter les cyberattaques, si elles se produisent, et

identifier les auteurs de ces actes, est devenue une partie intégrante de la manière dont la France exerce sa souveraineté nationale.

Le Livre blanc recommande de renforcer les ressources humaines consacrées à la cybersécurité et à la défense afin d'atteindre la parité avec ses alliés britanniques et allemands. Il souligne la nécessité de s'efforcer de concevoir et de mettre au point des systèmes de sécurité de haut niveau, soutenus par d'importants crédits budgétaires et accordant une attention particulière aux réseaux de communications électroniques. En outre, le gouvernement promet de renforcer le secteur de l'industrie, de la science et de la technologie liés à la cybersécurité. Le Livre blanc appelle également à une politique ambitieuse de protection des systèmes d'information de l'Etat en maintenant des réseaux hautement sécurisés au sein des institutions de l'Etat, à des politiques de passation des marchés publics appropriées et à une gestion appropriée des équipements de communication mobile. Cette politique doit être complétée par une sensibilisation des administrations publiques décentralisées, des institutions régionales et des principaux utilisateurs du cyberespace. Etant donné que la cybersécurité d'un Etat dépend également de la sécurité de ses fournisseurs de biens et de services, le Livre blanc exige en outre que des clauses à cet effet soient insérées dans les contrats. En outre, le livre blanc promet que le gouvernement et le parlement définiront des normes de cybersécurité pour les exploitants d'infrastructures d'importance vitale, en précisant leurs droits et leurs responsabilités. Le Livre blanc recommande également des campagnes supplémentaires de sensibilisation du public pour changer les comportements et les habitudes des citoyens. Enfin, le Livre blanc réaffirme le soutien de la France à la mise en place d'une politique européenne visant à renforcer la protection des infrastructures critiques et des réseaux de communications électroniques.

Afin de se protéger contre les cyberattaques majeures, le Livre blanc conceptualise les réponses politiques selon deux axes. Premièrement, le gouvernement mettra en œuvre 'une posture solide et résiliente pour protéger les systèmes d'information de l'Etat, les opérateurs d'infrastructures essentielles et les industries stratégiques'. Deuxièmement, le gouvernement développera 'une approche gouvernementale globale et appropriée' aux cyberattaques. La France comptera sur les ressources diplomatiques, judiciaires et policières comme instruments de premier choix. *Cependant, le gouvernement n'exclut pas 'l'utilisation progressive des ressources du ministère de la Défense dans le cas où des intérêts stratégiques nationaux seraient menacés'*. Il est intéressant de noter que la formulation sur les cyber-capacités offensives a été atténuée dans le Livre blanc par rapport à la version de 2008, faisant référence de manière indirecte à 'une capacité informatique proactive'. Cette capacité aiderait à définir la menace et à identifier l'origine d'une attaque; permettre d'anticiper certaines attaques et de configurer les défenses en conséquence; et donner au gouvernement la possibilité d'intervenir à grande échelle, en fonction de l'ampleur et de la gravité de la cyberattaque. Malgré les termes vagues, le ministre de la défense, M. Jean-Yves Le Drian, a affirmé en juin 2013 qu'il souhaitait doter la France d'une 'capacité informatique offensive', en ajoutant des capacités de cyberattaques à ses systèmes d'armes nucléaires. Il a souligné que 'l'enjeu est la capacité de contrôle à distance ou la destruction d'infrastructures vitales' et demande à la France de rechercher une capacité offensive dotée de 'ressources plus ou moins réversibles, plus ou moins discrètes, mais toujours proportionnées à l'ampleur et à la gravité de la situation'. [6]

Le document central en vigueur en matière de cyber est *La stratégie nationale pour la sécurité du numérique*. [7] Adoptée en 2015, la stratégie répond aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liées. La stratégie définit les cinq objectifs suivants:

- garantir la souveraineté nationale;

- apporter une réponse forte contre les actes de cybermalveillance;
- informer le grand public;
- faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises;
- renforcer la voix de la France à l'international.

La Stratégie 2015 en matière de cybersécurité vise à faire de la France une 'république numérique', reconnaissant que les TIC sont à la fois un catalyseur de la croissance économique et de l'innovation, mais imposent également des risques informatiques. La stratégie est liée de manière opérationnelle à la stratégie 2011 et à de nombreuses mesures de cybersécurité décrites dans la stratégie numérique parallèlement aux objectifs de la stratégie en matière de cybersécurité. Par exemple, les deux documents cherchent à accroître la confiance des utilisateurs en ligne, à maintenir des niveaux élevés de recherche et développement en cybersécurité comme moteur de la croissance économique et à protéger les informations personnelles. Plus important encore, les deux documents reconnaissent que les TIC sous-tendent la croissance économique française, mais également que les systèmes informatiques doivent être résilients et sûrs pour que la France puisse pleinement tirer parti des avantages d'une croissance fondée sur les TIC. [8] Bien que la dernière stratégie ne comprenne pas de nouveaux fonds, un milliard d'euros était auparavant alloué aux efforts de cybersécurité.

Depuis l'acceptation de la stratégie de 2015, l'environnement géopolitique français s'est considérablement dégradé. La France est mise au défi par le sentiment de retrait de deux piliers essentiels de la sécurité internationale: l'engagement des États-Unis en faveur de la sécurité de l'Europe (qui a été ébranlé par la réticence du président Donald Trump à réaffirmer les garanties de sécurité énoncées à l'article 5 par l'OTAN); et le départ du Royaume-Uni de l'Union Européenne (qui absorbe une grande partie des efforts politiques et diplomatiques de Londres au détriment d'autres projets). *La Revue stratégique de défense et de sécurité nationale* [9] adoptée en 2017 cherche des solutions à la situation actuelle et à la nécessité plus large de diversifier les alliés et partenaires de la France. [10]

Le document met à jour le Livre blanc de 2013, qui décrit cinq fonctions stratégiques de l'armée française (dissuasion, prévention, protection, intervention, anticipation) et ouvre la voie à la loi de programmation pour les achats militaires français 2019-2024. En matière de cyber, la revue stratégique soutient que la France pourrait être dans une meilleure position. Alors que les États-Unis dominent le secteur, la Chine est en train de devenir un formidable challenger et l'Europe reste vulnérable.

Dernier mais non le moindre, le document stratégique le plus récent en matière de cyber est *La revue stratégique de cyberdéfense*. [11] Publiée le 8 février 2018 et présentée le 12 février 2018 par Louis Gautier, le secrétariat général de la défense et de la sécurité nationale, la revue fontionne comme une synthèse de la doctrine de la défense nationale en matière de cybersécurité qui affirme la nouvelle ambition pour la France dans la cyberdéfense. [12] C'est pour cela qu'elle est aussi appelée comme le Livre blanc de la cyberdéfense qui est le premier grand exercice de synthèse stratégique dans ce domaine. Louis Gautier a comparé la Revue stratégique de la cyberdéfense au Livre blanc français sur la défense et la sécurité nationale de 1972 qui a établi la doctrine nucléaire de la France, la définissant ainsi comme un ouvrage fondateur de la cyber-politique française.

La revue stratégique se compose de trois parties. La première, consacrée aux 'dangers du cyber-monde', évalue les menaces, leur évolution et les acteurs impliqués. Il réaffirme

également le rejet par la France du concept de 'cyberdifférence' en expliquant que la dissuasion ne concerne que le nucléaire. La deuxième partie, intitulée 'L'État, responsable de la cyberdéfense de la nation', détaille l'approche française en matière de cyberdéfense. Il réaffirme le principe de la séparation des capacités et des missions défensives et offensives, ce qui implique que l'ANSSI ne mène aucune mission offensive et opère strictement au niveau défensif. L'examen considère le modèle français comme une alternative à la vision américaine, dans laquelle, selon les français, la plupart des cyber-capacités défensives sont concentrées dans la communauté du renseignement. [13] En France, l'ANSSI n'a aucun lien organique avec le ministère de la Défense ou les agences de renseignement, mais elle conserve l'autorité et les outils pour fournir une assistance défensive à des tiers et les conseiller en matière de cyber-protection.[2] Il détaille également la stratégie internationale de la France en matière de cyberdéfense, y compris ses positions en droit international. La troisième partie, intitulée 'L'État, responsable de la cybersécurité de la société', définit le concept de souveraineté numérique au sens juridique du terme souveraineté.

En ce qui concerne les questions juridiques, la revue respecte la position politique française selon laquelle les principes et les règles du droit international s'appliquent à la conduite des États dans le cyberespace, mais elle va plus loin que la simple reconnaissance de l'applicabilité du droit international au cyberespace. Elle détaille les obligations internationales spécifiques et les réactions possibles aux faits internationalement illicites. Il affirme également que les cyber-opérations pourraient constituer des violations de la souveraineté de l'État, du principe de non-intervention, de l'interdiction du recours à la force et de l'obligation de diligence raisonnable. La revue décrit également les réponses possibles aux cyberattaques. Si la situation l'exigeait, il serait alors possible d'adopter des mesures de rétorsion, de recourir à des mécanismes exceptionnels d'autoprotection et/ou de prendre des contre-mesures pacifiques. Les circonstances les plus graves peuvent nécessiter une réaction impliquant le recours à la force. La revue détaille les trois formes de mesures unilatérales d'auto-assistance que la France pourrait adopter pour faire face à une cyber opération conforme au droit international: des mesures de rétorsion, des contre-mesures et de la défense légitime.[3] En outre, cette approche des réponses est conforme à l'évolution récente du droit interne, notamment depuis l'adoption de l'article 21 de la loi de 2013 sur la planification militaire, codifié à l'article L2321-2 du code de la défense. (La revue semble répéter le contenu de l'article 21.) [14]

## LES ORGANISATIONS DE LA CYBERSECURITE

La France a organisé sa cybersécurité et sa défense de manière centralisée, conformément aux traditions historiques de son Etat, à la différence des approches adoptées par les États-Unis et l'Allemagne, par exemple. Comme indiqué précédemment, *l'ANSSI* est la plus haute agence de cybersécurité et de défense en France. [15] Reflétant l'importance de la cybersécurité aux yeux de l'État français, l'ANSSI est sous l'autorité directe du Premier ministre. Plus précisément, l'ANSSI fait partie du Secrétariat général de la défense et de la sécurité nationale (SGDSN), qui

[2] Inversement, certaines autres institutions sont chargées des opérations cyber offensives et de la collecte de renseignements.

[3] Certains Etats (notamment la Chine, Cuba et la Russie) ont rejeté l'applicabilité des contre-mesures, de la défense légitime et du droit international humanitaire au cyberespace.

assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité et collabore étroitement avec la présidence de la République.[4]

L'ANSSI a quatre missions: détecter et mettre en œuvre les premières réactions aux cyberattaques; soutenir le développement de produits et services fiables pour les institutions de l'État et les acteurs économiques; conseiller et soutenir les institutions publiques et les opérateurs d'infrastructures essentielles; ainsi que de sensibiliser et de communiquer activement sur les cybermenaces. En ce qui concerne le deuxième objectif, l'ANSSI a lancé en janvier 2018 la démarche de valorisation des activités de qualification et de certification baptisée Visa de sécurité ANSSI. Comme M. Mounir Mahjoubi, Secrétaire d'État chargé du Numérique a expliqué: 'Son objectif est d'accompagner les entreprises, en particulier les TPE/PME, les administrations, les collectivités locales et les citoyens dans leurs choix de solutions de sécurité'. [16] Les 110 premiers fournisseurs de solutions de cybersécurité ont déjà été reconnus.

Comme le demandait le Livre blanc de 2013, La loi de programmation militaire pour les années 2014-2019 (LPM) [17] prévoyait une législation explicite sur les normes en matière de cybersécurité, en particulier pour les réseaux gouvernementaux et les opérateurs privés d'une importance vitale (OIV).[5] Le Code de la défense français définit ces opérateurs comme 'des opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, ils sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste'. [19] Les opérateurs d'importance vitale sont conçus par l'État français[6] et comptent actuellement plus de 200 opérateurs dans douze secteurs d'activités.[7]

Dans le cadre du mandat du LPM, l'ANSSI pourrait

- définir des règles de sécurité obligatoires pour les systèmes critiques des opérateurs d'importance vitale; devraient être informés des incidents survenus sur des systèmes critiques d'opérateurs d'importance vitale;
- imposer des inspections de sécurité;
- mandater des mesures spécifiques en cas de crise majeure.

Ces tâches ont été remplies avec trois décrets de l'ANSSI publiés en mars 2015.[8] Cette approche intrusive vis-à-vis des opérateurs d'importance vitale, en matière de cybersécurité, contraste notablement avec les approches de nombreux autres Etats, qui travaillent souvent avec des normes reconnues par le secteur et un partage volontaire d'informations sur les cyber-menaces et les attaques. Il va sans dire que les opérateurs d'infrastructures vitales devront

[4] Conformément á la priorité no. 3 du rapport du sénate de 18 juillet 2012, l'ANSSI intitute un pôle juridictionnel spécialisé á compétence nationale pour primer les attaintes graves aux systèmes d'information.
[5] Selon l'actualisation de la loi de programmation militaire, le budget initiale de 3.8 Md euros a été élevé á 162,4 milliard d'euros courant sur 2015 et 2019. Voyez [18]
[6] Conformément à la priorité no. 6 du rapport du sénat de 18 juillet 2012 ('renforcer la protection des systèmes d'information des opérateurs d'importance vitale').
[7] Concernant les opérateurs des services essentiels (OSE), la France a identifié 122 OSE au stade de l'échéance du 9 novembre 2018 fixée par la directive NIS. Voyez [20]
[8] Ce sont les Décrets No. 2015-349/350/351. [21]

dépenser des sommes considérables en cybersécurité pour respecter ces normes, mais le gouvernement français estime que les avantages l'emporteront sur les coûts pour les entreprises françaises.

Il y a aussi des ministres qui participent à la formulation de la cybersécurité, cependant c'est *le Ministère de la Défense* qui joue le rôle le plus décisif.[9] Le ministère de la défense dispose de ses propres structures de cybersécurité et de défense qui travaillent en étroite collaboration avec l'ANSSI et d'autres ministères chargés des tâches liées à la cybersécurité. Le ministère considère le cyberespace comme un domaine militaire dans son propre droit. Le ministère a pris à cœur la mission de cyberdéfense en 2011 en publiant le Concept commun pour la cyberdéfense, qui définit le cadre, les principes et les capacités requises pour les opérations militaires dans le cyberespace. Cela a été suivi par la Doctrine commune pour la cyberdéfense dans laquelle le ministère a établi son organisation en matière de cyberdéfense. La doctrine commune a créé le poste d'officier général chargé de la cyberdéfense sous l'autorité du chef de la défense français. Le «cyber général» remplit deux rôles. Il joue un rôle opérationnel dans Le Centre de planification et de conduite des opérations (CPCO), et deuxièmement, il est responsable de la coordination et du développement de la cyberdéfense au sein du ministère de la Défense ainsi que dans les trois services.

Le 7 janvier 2014, la ministre de la défense a présenté une nouvelle initiative cyber du ministère. Son pacte de cyberdéfense vise à développer les capacités cybernétiques du MOD et à les mettre à la disposition de toute la société française.[10] Deux mesures du pacte méritent une attention particulière: le centre d'excellence en cyberdéfense et la cyberdéfense citoyenne. Le ministère de la défense a officiellement lancé *le centre d'excellence en matière de cyberdéfense* en février 2014. Il est hébergé par la Direction générale des armements pour la sécurité de l'information, qui instaure elle-même d'importants efforts en matière de cybercriminalité et intègre ses compétences en matière de formation, de recherche et de développement. La poursuite du développement de la cyberindustrie française est un autre aspect important du centre, le gouvernement et les institutions locales voulant faire de la région de Rennes un pôle cyber de premier plan en France et en Europe.

L'autre initiative novatrice du ministère de la défense, en collaboration avec la gendarmerie française, est *Le Réseau cyberdéfense de la réserve citoyenne* (RCC). L'idée d'une réserve spécialisée dans ce domaine est issue du concept interarmées de cyberdéfense et des travaux interministériels menés en 2011. '*La réserve spéciale est un vecteur intéressant de liens entre la société civile et la société militaire'* – comme Luc-François Salvador, colonel dans la réserve citoyenne et coordinateur national de la réserve citoyenne cyber précisé. [24] Elle est constituée de volontaires agréés auprès d'autorités militaires en raison de leurs compétences, de leur expérience, mais aussi de leur intérêt pour les questions relevant de la défense nationale.[11] La réserve comprendra 4440 personnes en 2019. Le RCC vise à faire de la cyberdéfense une priorité nationale par le biais de programmes de sensibilisation réunissant des professionnels, des étudiants avancés et des étudiants ayant une expertise dans le domaine de la cyberactivité.

[9] L'autre ministère est le ministère de l'Intérieur qui a pour mission de lutter contre toutes les formes de cybercriminalité, visant les institutions et les intérêts nationaux, les acteurs économiques et les collectivités publiques, et les particuliers. [22]

[10] Il comporte six lignes d'efforts avec un total de cinquante initiatives. Voyez [23]

[11] Six groupes de travail ont été constitués: "élus et journalistes", "Jeunes", "Evolution de l'engagement citoyen", "thinks tanks et réflexion stratégique", "PME/PMI" et "Grandes entreprises". Voyez [25]

[26] L'acteur majeur du recrutement et de la gestion des réservistes de cyberdéfense est Le Centre de la réserve et de la préparation opérationnelle de cyberdéfense (CRPOC) qui a été établi en 2015, mais commancera l'opération l'année prochaine. Il y a deux autres centres interarmés. L'un est Le Centre d'analyse en lutte informatique défensive (CALID). Créé en 2006, il pilote 24H/24 la détection, le traitement et la réponse aux cyberattaques, et il fonctionne comme le centre opérationnel expert en lutte informatique défensive. Le centre est basé á Paris et Rennes sera opérationel á partir de 2019. L'autre centre (qui commencera l'opération aussi en 2019) s'appelle Le Centre d'audits de la sécurité des systèmes d'information (CASSI). Créé en 2006, il fonctionne comme centre national dont la mission d'audit couvre les domaines de la sécurité des systèmes d'information (SSI) et les signaux parasites compromettants (SPC). [27]

Tous les deux centres sont rattaché au *COMCYBER*, l'unité opérationnelle commandant. Placé sous l'autorité directe du chef d'état-major des armées, le COMCYBER est responsable de la manœuvre cyber globale. Créé en décembre 2016, il sera operable en 2019 déployant 2600 combattants numériques et recevra un engagement initial de 2,1 milliards d'euros. Comme Jean-Yves Le Diran, le ministre de la défense explique la création de ce nouvel institut: 'L'émergence d'un nouveau milieu, le cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre », a indiqué Jean-Yves Le Drian. « Nos capacités cyber offensives doivent nous permettre de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives.' [28] Frédérick Douzet, professeur à l'Institut Français de Géopolitique de l'Université Paris 8 souligne les spécificités uniques du COMCYBER vis-à-vis des commandes d'autres pays: 'La nouvelle organisation française est différente des États-Unis ou du Royaume-Uni car les activités des services de renseignement ne relèvent pas du même commandement que les opérations cyber-militaires. L'Allemagne a mis en place une nouvelle cyber-armée, mais elle est beaucoup plus large car elle intègre non seulement le cyber, mais également toutes les informations géographiques, les technologies de l'information, le renseignement et les communications opérationnelles. Considérant que la France est en train de créer une unité dédiée à la cyberdéfense sous un petit commandement au plus haut niveau stratégique. Cela montre à quel point le cyberespace est devenu une priorité pour le ministère français de la Défense.' [29]

## L'AVENIR

La France est impliquée dans beaucoup de forums internationaux où les problèmes de cybersécurité sont abordés. Elle a choisi cette voie pour pouvoir utiliser le meilleur du cyberespace à l'avenir – conformément à sa politique souple.

Tout d'abord, la France est particulièrement active au sein de l'ONU où les règles de comportements responsables dans le cyberespace sont discutées. Elle a participé aux cinq derniers groupes d'experts gouvernementaux des Nations Unies sur la cybersécurité. Parmi les forums, on y trouve aussi l'Alliance Atlantique, le groupe 'Ise-Shima Cyber Group' au sein de G7 ou l'OSCE. [22] Sa participation aux organisations internationales est en ligne avec sa politique qui met beaucoup l'accent sur la diplomatie.

Ainsi, ce n'est pas un hasard si la France a accueilli le Forum sur la Gouvernance de l'Internet (FGI) cette année dont le thème était 'Internet of Trus'. La treizième édition du Forum a été organisée à l'UNESCO à Paris entre le 12 et 14 novembre, 2018. Au cours duForum, le Président de la République, Emmanuel Macron, a lancé *l'Appel de Paris pour la confiance et*

*la sécurité dans le cyberespace*. [30] Selon l'appel, la France réaffirme son soutien à un cyberespace ouvert, sûr, stable, accessible et pacifique, et aussi que le droit international s'applique à l'usage des technologies de l'information et de la communication (TIC) par les États. Cependant, la France souligne la nécessité de développer une vaste coopération dans le domaine du numérique et également la nécessité d'une approche multi-acteurs. La déclaration de haut niveau a déjà reçu l'appui de 43 États, mais aussi d'entreprises privées et d'organisations de la société civile. [31]

L'appel est une des nombreuses initiatives francaises courantes en France. Le but de cette politique est que la France puisse être connue comme une grande puissance en cyber dans le monde entier.

En septembre 2013, le ministre de l'Economie, de l'Industrie et du Numérique a lancé l'initiative '*Une nouvelle France industrielle*'. [32] Le 33ème des 34 projets de cette initiative concerne la cybersécurité. Dirigé par le directeur général de l'ANSSI, ce plan vise à augmenter de manière significative la demande et l'offre de solutions de cybersécurité fiables; aider les entreprises françaises de cybersécurité à conquérir des parts plus importantes des marchés étrangers; et renforcer les entreprises françaises. L'un des premiers résultats de ce plan est la création du *label France Cybersecurity*, un label attribué aux solutions de haute sécurité conçues et exploitées en France. [33] En janvier 2018, les 72 premières solutions en ligne ont reçu le label. [34]

L'autre initiative lancée en 2017 est le projet *2017/2027*. Le projet lancé par France Stratégie vise à éclairer les enjeux de la prochaine élection présidentielle. [35] Parmi les thématiques, on y trouve le thème de 'tirer parti de la révolution numérique parce qu'il transforme l'économie, parce qu'il rebat les cartes de la compétition et parce qu'il pose des questions fondamentales à la société.' Trois enjeux majeurs se sont dégagés: le soutien à l'innovation, l'acquisition de compétences numériques et l'appropriation des outils numériques dans le fonctionnement démocratique. Cette forme de la pensée montre l'importance du domaine cyber dans le quotidien de la société française.

Les initiatives nationales et internationales susmentionnées ne sont que des orientations d'innombrables participations, mais elles montrent également à quel point le pays est déterminé à atteindre son objectif de devenir un leader mondial du cyberespace. Il est même possible que la puissance dominante du futur centre européen de compétences et de recherche en cybersécurité qui sera établi soit la France.[12]

## CONCLUSIONS

Pour faire respecter les intérêts de la France, il est fait souvent appel aux outils de la diplomatie douce, pour laquelle il s'agit d'un véritable grand maître sur le marché mondial. Cette vaste connaissance du pays peut également être utilisée en cybersécurité. Dans le domaine de la cyber diplomatie, le pays a déjà pris les premières mesures importantes. Les tâches de la cyber diplomatie ont été placées sous la direction d'un seul homme au sein du ministère des Affaires étrangères en ligne avec la stratégie digitale de 2015. La position de l'ambassadeur pour la cyberdiplomatie et l'économie numérique a été fournie par M. David Martinon en 2015 qui

[12] Le 12 septembre 2018, le Président de la Commission européenne, Jean-Claude Juncker a annoncé dans son discours sur l'état de l'Union la création d'un réseau de centre de compétences nationaux ainsi que la création d'un centre européen de compétences et de recherche en cybersécurité. Voyez [36]

occupe également le poste d'ambassadeur pour le numérique depuis le 22 novembre 2017.[13] C'est une décision importante qui donne à M. Martinon compétence sur des sujets ayant trait au numérique dont ce ministère a la charge – parmi d'autres – les négociations internationales sur la cybersécurité. Comme il l'a dit dans son interview: 'Aujourd'hui, je suis chargé de promouvoir et de mettre en pratique la stratégie internationale française pour les affaires et la technologie numériques, qui ne représente pas seulement la vision du ministère des affaires étrangères, mais constitue véritablement une approche 'tout le gouvernement' des questions numériques'. [38] M. Martinon a été aussi spécialement chargé par le président et le premier ministre, sous l'autorité du ministre des Affaires étrangères et européennes, de dialoguer directement avec les principales plateformes numériques américaines sur la lutte contre Internet à des fins terroristes. [39]

La France attache une grande importance aux relations bilatérales, spécialement vis-à-vis de l'Allemagne. La coopération entre les deux pays est déjà très intense, ce que conforte le premier rapport conjoint. [40] Ce premier rapport conjoint concrétise l'intensification du partenariat franco-allemand qui sera développé en tant que moteur de la politique de cybersécurité au sein de l'espace européen. Pour cette première édition, ANSSI et BSI[14] ont choisi de se concentrer sur les activités malveillantes associées aux ransomware et à la crypto-extraction, qui constituait une menace croissante des citoyens pour les grandes entreprises fournissant des services essentiels et passant par des petites et moyennes entreprises ayant un impact direct sur leurs activités. Dans leur analyse commune, les deux agences conviennent que la situation de la menace concernant Ransomware est toujours alarmante, même plus de deux ans après la publication des premières attaques de Ransomware. [41]

Mais tout cela en vain s'il n'y a pas de succès significatif dans la sensibilisation de la population. Alors que le gouvernement prend les mesures nécessaires pour que le pays soit véritablement une cyberpuissance, il subsiste un retard considérable dans la préparation de la société par rapport à l'Etat. 28% de la population est en difficulté vis-a-vis du numérique: 16% ne se connectent jamais à l'internet et 12% ont des compétences numériques très faibles. Ce problème est directement lié à l'âge de non-internautes: 62% d'eux sont âgés de plus de 65 ans. En plus, 84% de non-internautes sont peu diplomés. [42] Vu les nombreuses mesures positives prises par le pays, on ne peut nier qu'elles seront tout aussi efficaces dans ce domaine et tout sera donné à la France pour devenir un cyber-majeur.

## REFERENCES

[1] *FIC2015 Discours de Bernard Cazeneuve et Thomas De Meziere*" 7ème forum international de la cybersécurité, Lille, le 20 Janvier 2015, https://www.youtube.com/watch?v=v9NPGaVHqmU [2018.11.09.]

[2] *Le Livre blanc sur la défense et la sécurité nationale*. Juin 2008. https://www.diplomatie.gouv.fr/IMG/pdf/0000.pdf [2018.11.01.]

[13] Une initiative similaire existe également dans le secteur des entreprises. Il serait utile de nommer un *directeur cybersécurité* en charge de la supervision de l'ensemble du risque cyber, avec un périmètre dépassant le simple système d'information. Voyez: [37]

[14] Bundesamt für Sicherheit in der Informationstechnik

[3] *Défense et sécurité des systèmes d'information: Stratégie de la France. 2011.* https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf [2018.11.01.]

[4] *Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense*, Par le Sénateur M. Jean-Marie BOCKEL. Sénat Session extraordinaire de 2011-2012. Enregistré á la Présidence du Sénat le 18 juillet 2012. http://www.senat.fr/rap/r11-681/r11-6811.pdf [2018.11.01.]

[5] *Livre Blanc. Défense et sécurité nationale. 2013.* Paris https://www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf [20018.11.01.]

[6] *Cyberdéfense: la France reconnaît son retard.* Le Monde, le 3 juin 2013., https://www.lemonde.fr/international/article/2013/06/03/cyberdefense-la-france-reconnait-son-retard_3423012_3210.html [2018.11.11.]

[7] *La stratégie nationale pour la sécurité de la numérique 2015*. https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf [2018.11.16.]

[8] *France cyber readiness at a glance*. Potomac Institute for Policy Studies. September 2016. http://www.potomacinstitute.org/images/CRI/CRI_France_Profile_PIPS.pdf [2017.10.13.]

[9] *La Revue stratégique de défense et de sécurité nationale 2017*. https://www.defense.gouv.fr/content/download/514655/8664340/file/Revue+strat%C3%A9gique+de+d%C3%A9fense+et+de+s%C3%A9curit%C3%A9+nationale+2017.pdf [2018.11.16.]

[10] Boris, TOUCAS: *Understanding the Implications of France' Strategic Review on Defense and National Security*. October 19, 2017, CSIS, https://www.csis.org/analysis/understanding-implications-frances-strategic-review-defense-and-national-security [2018.11.16.]

[11] *La Revue Stratégique de Cyberdéfense*. SGDSN, le 12 février 2018., http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf [2018.11.15.]

[12] Communiqué de presse, Paris, le 8 février 2018. https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=52C71CD2-4382-4B5A-AF7A-FC3299391DD7&filename=53.pdf [2018.11.15.]

[13] Boris, TOUCAS: *With its new 'White Book', France looks to become a world-class player in cyber space.* March 29, 2018., https://warontherocks.com/2018/03/with-its-new-white-book-france-looks-to-become-a-world-class-player-in-cyber-space/ [2018.11.16.]

[14] Francois, DELERUE, Aude, GÉRY: *France's Cyberdefense Strategic Review and International Law.* March 23, 2018., https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law [2018.11.16.]

[15] Agence nationale de la sécurité des systèmes d'information https://www.ssi.gouv.fr/en/ [2018.11.01.]

[16] *L'Agence nationale de la sécurité des systèmes d'information (ANSSI) remet ses premiers Visas de sécurité*. Communiqué de presse, Paris, le 22 juin 2018. https://www.ssi.gouv.fr/uploads/2018/06/communique_de_presse_visa-de-securite_ceremonie_2018_anssi.pdf [2018.10.13.]

[17] *Loi no. 2013-1168 du 18 décembre 2013 relative á la programmation militaire pour les années 2014 et 2019 et pourtant diverses dispositions concernant la défense et la sécurité nationale.* https://www.legifrance.gouv.fr/affichTexte.do;?cidTexte=JORFTEXT000028338825 [2018.11.01.]

[18] *Actualisation de la loi programmation militaire (LPM) 2014-2019.,* publié le 10 Juin 2016. https://www.defense.gouv.fr/english/portail-defense/issues2/defence-policy/la-loi-de-programmation-militaire-lpm-2014-2019/actualisation-de-la-loi-de-programmation-militaire-lpm-2014-2019/lpm [2018.11.01.]

[19] *Code de la défense* (12 novembre 2018) Article 1332-1. https://www.legifrance.gouv.fr/telecharger_pdf.do?cidTexte=LEGITEXT000006071307 [2018.11.01.]

[20] *Directive NIS: l'ANSSI accompagne les premièrs opérateurs de services essentiels.* Communiqué de presse, Paris, le 9 novembre 2018. https://www.ssi.gouv.fr/uploads/2018/11/communique-de-presse-nis-et-ose_vf.pdf [2018.11.01.]

[21] Les Décrets No. 2015-349/350/351. https://www.ssi.gouv.fr/publication/publication-du-decret-n-2015-349-du-27-mars-2015-relatif-a-lhabilitation-et-a-lassermentation-des-agents-de-lautorite-nationale-de-securite-des-systemes-dinfo/ et https://www.ssi.gouv.fr/publication/publication-du-decret-n2015-350-du-27-mars-2015-relatif-a-la-qualification-des-produits-de-securite-et-des-prestataires-de-service-de-confiance-pour-les-besoins-de-la-securite-nationale/ et https://www.ssi.gouv.fr/uploads/2015/03/20150330_ANSSI_Communique_Presse_Decret-2015-351.pdf [2018.11.01.]

[22] *La France et la cybersécurité.* https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/ [2018.11.17.]

[23] *Pacte Défense Cyber. 50 mesures pour changer d'échelle*. http://www.defense.gouv.fr/content/download/237702/2704402/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf [2018.11.01.]

[24] Nelly, MOUSSU: *Des réservistes spécialisés en cyberdéfense.* Publié le 13 Septembre, 2012., https://www.defense.gouv.fr/english/actualites/articles/des-reservistes-specialises-en-cyberdefense [2018.11.01.]

[25] RÉGIS, Ollivier: *Le réseau de la réserve citoyenne cyberdéfense dévoilé.* Publié le 11 Avril 2013. https://lecolonel.net/le-reseau-de-la-reserve-citoyenne-cyberdefense-devoile/ [2018.11.01.]

[26] Les réserves de cyberdéfense. https://www.gouvernement.fr/risques/les-reserves-de-cyberdefense [2018.11.01.]

[27] *La cyberdéfense*. le 17 octobre 2018., https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/la-reserve-de-cyberdefense [2018.11.01.]

[28] Dominique, FILIPPONE: *La France crée un commandement cyberdéfense*. Publié le 13 décembre 2016., https://www.lemondeinformatique.fr/actualites/lire-la-france-cree-un-commandement-cyberdefense-66778.html [2018.11.01.]

[29] Tom, REEVE: *France unveils cyber command in response to 'new are in warfare'*. Publié le 16 décembre 2016., https://www.scmagazineuk.com/france-unveils-cyber-command-response-new-era-warfare/article/1475678 [2018.11.01.]

[30] *Appel de Paris pour la confiance et la sécurité dans le cyberespace.* le 12 novembre, 2018. https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf [2018.11.17.]

[31] *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace.* Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018.). https://www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31.pdf [2018.11.17.]

[32] *La Nouvelle France Industrielle.* Présentations des feuilles de routes des 34 plans de la nouvelle France Industrielle. Le Gouvernement de la République Francaise, 2013.https://www.economie.gouv.fr/files/files/PDF/nouvelle-france-industrielle-sept-2014.pdf [2018.11.16.]

[33] *Label France Cybersecurity.* https://www.francecybersecurity.fr/ [2018.11.18.]

[34] *Label France Cybersecurity. Catalogue 2018 des offres labellisées.* https://www.francecybersecurity.fr/wp-content/uploads/2018/01/FCS_Catalogue_2018_web.pdf [2018.11.18.]

[35] *2017-2027.* http://francestrategie1727.fr/thematiques/tirer-parti-de-la-revolution-numerique/ [2018.11.01.]

[36] *L'état de l'Union en 2018: la Commission européenne propose des mesures visant á garantir des élections européennes libres et équitables.* Strasbourg, le 12 septembre 2018. http://europa.eu/rapid/press-release_IP-18-5681_fr.htm [2018.11.18.]

[37] *Cybersécurité. Visualiser, comprendre. décider*. Cigref Rapport d'octobre 2018. https://www.cigref.fr/wp/wp-content/uploads/2018/10/Cigref-Rapport-Cybersecurite-Visualiser-Comprendre-Decider-Octobre-2018.pdf [2018.11.18.]

[38] *Interview: Ambassador or Digital Affairs David Martinon.* May 4, 2018., https://franceintheus.org/spip.php?article8589 [2018.11.17.]

[39] *Nomination de David Martinon au poste d'ambassadeur pour le numérique (le 22 novembre 2017*). https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites/article/nomination-de-david-martinon-au-poste-d-ambassadeur-pour-le-numerique-22-11-17 [2018.11.17.]

[40] *ANSSI/BSI Common situational picture*. Vol. 1. – July 2018. https://www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf [2018.11.17.]

[41] *ANSSI and BSI present their first „Common situational picture".* BSI Press release, July 20, 2018. https://www.bsi.bund.de/EN/Press/press_releases/Press2018/ANSSI-BSI_1st_Common_situational_picture_20072018.html [2018.11.17.]

[42] *Les bénéfices d'une meillure autonomie numérique*. Rapport au secrétaire d'État auprès du Premier ministre, chargé du Numérique, juillet 2018. http://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-benefices_autonomie_numerique-12072018_0.pdf [2018.11.09.]

## KIBERBIZTONSÁG FRANCIAORSZÁGBAN: A MÚLT, A JELEN ÉS A JÖVŐ

*Absztrakt*

*Franciaország deklarált célja, hogy a világ vezető államává váljon a kiberbiztonság területén. A cél – a franciáktól nem szokatlan módon – igen ambiciózus, eléréséhez azonban még hosszú út vezet. Annyi azonban már most is bizonyos, hogy az elmúlt években az ország nagy előrehaladást tudhatott magáénak. Frissítette stratégiai dokumentumrendszerét és a kiberbiztonsági szervezetrendszerét is hozzáigazította a kor követelményeihez. Ezzel az ország már most is az európai vezető kiberhatalmak körében tudhatja magát, de a következő években további eredmények várhatók. A tanulmány ezt a folyamatot mutatja be, ismertetve a kiindulópontnak számító 2010-es évek elején meglévő viszonyokat s kitekintve a jövőbeli lehetőségekre is.*

***Kulcsszavak:*** *kiberbiztonság, Franciaország, kiberstratégia*