ASSOCIATION DE SOUTIEN À L'ARMÉE FRANÇAISE

"LA CYBERDÉFENSE"

ASAF
ASSOCIATION DE SOUTIEN
À L'ARMÉE FRANÇAISE

LA SÉLECTION DES ARTICLES PROPOSÉS DANS CE DOSSIER A POUR SEUL OBJET D'OFFRIR UNE VARIÉTÉ D'ANALYSES QUI PERMETTRA AU LECTEUR DE SE FAIRE UNE OPINION PLUS STRUCTURÉE.
ELLE N'ENGAGE AUCUNEMENT L'ASAF.

CRÉATION : 1ER MARS 2023
DERNIÈRE MISE À JOUR : 25 JUILLET 2023

LA CYBERDÉFENSE

Rédigé par Adrien de La Tournelle et Chloé Daniel
Maquetté par Laure Fanjeau

SOMMAIRE

Pour accéder aux articles, cliquer sur le titre de la partie.

Les articles sont classés par thèmes et par ordre de publication sur le site de l'ASAF.
Les nouveaux articles sont en rouge.

CONTEXTE **2**
SITUATION ACTUELLE **3**
ILLUSTRATIONS **4**
DÉCLARATIONS ET DOCUMENTS OFFICIELS **5**
Défense et sécurité nationale. Le Livre Blanc, 2008 5
Défense et sécurité nationale. Le Libre blanc, 2013 5
Défense et sécurité des systèmes d'information. Stratégie de la France (ANSSI, 2011) 5
La cyberdéfense : un enjeu mondial, une priorité nationale. Rapport d'information n° 681 (2011-2012), déposé le 18 juillet 2012 (Sénat). 6
Revue stratégique et de défense nationale (2017) 6
Revue stratégique de cyberdéfense (SGDSN, 12/02/2018) 6
Rapport d'information déposé en application de l'article 145 du Règlement par la Commission de la défense nationale et des forces armées en conclusion des travaux d'une mission d'information sur la cyberdéfense et présenté par M. Bastien LACHAUD et Mme Alexandra VALETTA-ARDISSON (Assemblée nationale, 2018) 6
Revue nationale stratégique (2022) 7
Les doctrines de lutte informatique 7
POINTS À SURVEILLER **8**
1. L'investissement professionnel 8
2. Le positionnement français face aux autres acteurs cyber 8
3. Le maintien d'une certaine éthique et transparence 8
4. Quelle souveraineté numérique français et/ou européenne 8

Les questions, commentaires et remarques peuvent être faites à l'adresse suivante :
numerique@asafrance.fr

CONTEXTE

La garantie de la souveraineté numérique représente un défi majeur pour la France, tant au niveau national que pour ses forces armées, étant donné l'augmentation des attaques informatiques. Dans un contexte où les luttes de pouvoir, les crises et les conflits contemporains se déroulent de plus en plus dans l'espace numérique, les armées considèrent désormais le combat cybernétique comme un mode d'action à part entière, dont les effets s'associent aux autres dans une stratégie globale, tout en maintenant une distinction entre le temps de paix et le temps de conflit armé.

La compétition et les conflits ne se limitent plus aux milieux traditionnels tels que la Terre, la Mer, l'Air et l'Espace. Avec l'essor de l'utilisation des données numériques, ils s'étendent désormais à ce nouveau domaine. Ainsi, la dimension cyber est maintenant envisagée comme une arme utilisée dans toutes les opérations. La cyberdéfense est donc un enjeu stratégique crucial, garantissant la souveraineté nationale. En collaboration avec de nombreux acteurs, le ministère des Armées joue un rôle actif dans la protection, la défense des systèmes d'information et la conduite d'opérations dans le cyberespace.

La reconnaissance du rôle essentiel de la cyberdéfense militaire a été confirmée dans la revue stratégique de défense et de sécurité nationale de 2017, ainsi que dans la revue stratégique de cyberdéfense de février 2018. C'est une notion qui avait déjà été mentionnée dans les Livres blancs de 2008 et 2013. Cette reconnaissance s'est traduite par l'adoption de la Loi de programmation militaire 2019-2025, qui prévoyait une augmentation significative des ressources financières et humaines, avec un budget de 1,6 milliard d'euros et le recrutement de plus de 1 000 cyber-combattants. Les budgets alloués à la cyberdéfense ces 4 dernières années dans le cadre de la LPM 2019-2025 ont bien été « respectés » et « ont permis d'atteindre un premier niveau de maturité » en la matière[1].

Cet effort répond à une nécessité croissante. Les travaux doctrinaux publiés en 2019 sur la Lutte informatique défensive (LID) et la Lutte informatique offensive (LIO) dans les opérations militaires complètent la stratégie de cyberdéfense et contribuent à la préparation de l'avenir des opérations militaires en intégrant progressivement cette nouvelle capacité dans la stratégie globale des forces armées.

La cyberdéfense française s'organise notamment autour du Commandement de la cyberdéfense (COMCYBER) mais aussi l'ANSSI (Agence nationale de la sécurité des informations), la DGSI (renseignement intérieur) et la DGSE (renseignement extérieur), la DRSD et la DGA.

[1] Rapport d'information déposé en application de l'article 145 du Règlement par la Commission de la défense nationale et des forces armées en conclusion des travaux d'une mission d'information sur le bilan de la loi de programmation militaire 2019-2025 et présenté par M. Thomas GASSILLOUD, MM. Yannick CHENEVARD et Laurent JACOBELLI (15/03/2023).

SITUATION ACTUELLE

Le constat est le suivant : la France est une cible privilégiée pour les acteurs étatiques et para-étatiques du cyber aux intérêts divers. Outre ces menaces à l'échelle nationale, les attaques cybercriminelles, en particulier les rançongiciels, représentent aussi un grave problème pour les entreprises et les institutions françaises, engendrant des pertes financières considérables et mettant parfois en danger des vies humaines. Enfin, la menace cyberterroriste et cyberactiviste, bien qu'imprévisible, est toujours présente. Face à cette réalité, la France doit renforcer ses capacités de cyberdéfense pour faire face aux menaces grandissantes qui pèsent sur sa sécurité nationale.

Pour continuer de renforcer les capacités de défense française dans le domaine cyber, la LPM 2024 - 2030 dispose d'un volet dédié à la cybersécurité. Ce dernier prévoit quatre mesures pour permettre à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) « d'augmenter sa connaissance des modes opératoires des cyberattaquants, de mieux remédier aux effets de leurs attaques et d'alerter plus efficacement les victimes des incidents ou des menaces pesant sur leurs systèmes d'information. »[2].

La sensibilisation à la menace cyber ne cesse de se développer. Récemment, le général Thierry Bauer, adjoint du général commandant de la cyberdéfense (Comcyber), s'est exprimé sur la dimension cyber dans les conflits actuels et futurs lors du Séminaire interarmées des grandes écoles militaires (Sigem) pour sensibiliser les élèves-officiers aux enjeux numériques. Cette sensibilisation n'est pas que nationale, puisqu'au sein de l'OTAN a eu lieu en début 2023 un grand exercice de cyberdéfense : "*Locked Shields*". Dans le cadre de celui-ci, les alliés, dont la France, s'entraînent à protéger des systèmes informatiques contre des attaques en temps réel et à prendre des décisions tactiques et stratégiques dans des situations critiques.

La France a encore des progrès à faire dans ce domaine à mesure que les puissances stratégiques internationales s'érigent comme étant de plus en plus menaçantes et agressives. Moteur de l'Union européenne, ce développement doit aussi se faire à l'échelle régionale. Les États membres doivent encore renforcer leur résilience face aux cybermenaces et accroître « leur cybersécurité et leur cyberdéfense communes contre les comportements malveillants et les actes d'agression dans le cyberespace. »[3]. Les défis ne cessent d'évoluer donnant un rôle important aux différents services chargés de prévenir les menaces cyber et d'en adapter les moyens de défense français.

[2] Projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense. (07/06/2023). Vie publique.

[3] Cyberdéfense: le Conseil souligne dans des conclusions qu'il importe de renforcer encore la résilience de l'UE face aux cybermenaces. (23/05/2023). Conseil de l'UE.

ILLUSTRATIONS

Les mots clés du domaine cyber

Mots clés

Cyberdéfense : ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace pour garantir l'effectivité de l'action des forces armées,la réalisation des missions confiées et le bon fonctionnement du ministère. La cyberdéfense est à différencier de la cybercriminalité qui correspond à l'ensemble des crimes et délits traditionnels ou nouveaux réalisés, via les réseaux numériques.

Cyberespace : le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs de services en ligne.

Cyberattaques : acte malveillant de piratage informatique dans le cyberespace. Les cyberattaques peuvent être l'action d'une personne isolée, d'un groupe, d'un État. Elles incluent la désinformation, l'espionnage électronique qui pourrait affaiblir l'avantage compétitif d'une nation, la modification clandestine de données sensibles sur un champ de bataille ou la perturbation des infrastructures critiques d'un pays (eau, électricité, gaz, communication, réseaux commerciaux). La cyberdéfense du ministère vise à détecter et contrer les cyberattaques dont la cible et la finalité sont liées au ministère des Armées.

Sécurité des systèmes d'information : ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

© Site archives du ministère des Armées

Les 10 commandements cyber

1/ Les infections virales, jamais je ne transmettrai.
Passer par le SAS antivirus ou le PID du réseau concerné. Ne jamais mêler support personnel et ordinateur professionnel.

2/ Mes données sensibles, j'effacerai.
Effacer les données sensibles des clés après chaque utilisation. Préférer la transmission de fichiers par message électronique.

3/ À chaque virus trouvé, je rendrai compte sans délai.
Alerter le correspondant en cas de virus.

4/ Sur Internet, prudemment je naviguerai.
Depuis mon ordinateur professionnel, ne naviguer que sur des sites connus et sûrs.

5/ Mes mots de passe, personne ne pourra deviner.
Créer des mots de passe impersonnels et avec toutes sortes de caractères. Ne les dévoiler à personne.

6/ Sur mon poste de travail, ma session je verrouillerai.
Verrouiller automatiquement sa session, même pour 2 minutes d'absence.

7/ Mon adresse mail pro, qu'à des personnes de confiance je donnerai.
Ne pas partager son adresse mail permet de prévenir et limiter les attaques par envoi de mails infectés.

8/ La prudence me guidera quand mails et fichiers joints, j'ouvrirai.
Contrôler l'expéditeur, l'objet du mail, de la pièce jointe, la date et l'heure d'envoi avant ouverture. En cas de doute, conserver le mail et alerter le correspondant SSI.

9/ Mes informations sensibles, aux moyens de transmissions j'adapterai.
N'envoyer aucun fichier sensible par Internet sans protection. Pour envoyer des mails DIFFUSION RESTREINTE, contacter le correspondant SSI pour connaître la procédure.

10/ La politique de sécurité, jamais ne contournerai.
Un poste infecté entraîne la corruption de dizaines de milliers d'autres. Violer intentionnellement la politique de sécurité entraîne des sanctions disciplinaires et pénales.

© ministère des Armées

DÉCLARATIONS ET DOCUMENTS OFFICIELS

Défense et sécurité nationale. Le Livre Blanc, 2008

Bien que le terme de « cyber » ne soit évoqué que 6 fois dans ce document de 402 pages, le Libre blanc de 2008 reconnaît l'existence d'une menace cyber dans un monde évolutif. « En outre, dans la mesure où le cyberespace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace. Des règles d'engagement appropriées, tenant compte des considérations juridiques liées à ce nouveau milieu, devront être élaborées. »

Pour en savoir plus :
https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/084000341.pdf

Défense et sécurité nationale. Le Libre blanc, 2013

Cinq ans plus tard, la « lutte contre la cybermenace » apparaît comme un des « moyens de la stratégie » de défense française qui constitue les 160 pages de ce document. « Nous devons veiller à protéger les Français, y compris face aux risques de la cybermenace » rappelle le président de la République François Hollande dans la préface.

Pour en savoir plus :
https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/134000257.pdf

Défense et sécurité des systèmes d'information. Stratégie de la France (ANSSI, 2011)

Première stratégie officielle quant au rôle de la France dans le cyberespace, ce texte rend compte de façon réaliste de l'enjeu géopolitique qui se pose dans ce domaine. Il est rédigé par l'ANSSI, créée en 2009 dans le but de doter la France d'une capacité structurée de défense et de sécurité. « L'objectif de ce document est de préciser les grandes lignes de la stratégie poursuivie par la France [...] dans le cyberespace, la sécurité de nos compatriotes, de nos entreprises et de la Nation. ».

Pour en savoir plus :
https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

La cyberdéfense : un enjeu mondial, une priorité nationale. Rapport d'information n° 681 (2011-2012), déposé le 18 juillet 2012 (Sénat).

La France est-elle suffisamment préparée pour se protéger et se défendre face aux attaques informatiques ? Que faut-il entendre par « cyberdéfense » ? Telles sont les questions auxquelles tente de répondre se rapport sénatorial à l'aune de l'émergence de la considération de la menace cyber.

Pour en savoir plus :
https://www.senat.fr/rap/r11-681/r11-6811.html

Revue stratégique et de défense nationale (2017)

Entre la renforcement des menaces dans le cyberespace, la reconnaissance de l'espace numérique contesté, et la volonté de préparer l'avenir avec une intégration de l'innovation et du numérique, la RSDN de 2017 concrétise les opérations cyber de la France.

Pour en savoir plus :
https://www.diplomatie.gouv.fr/IMG/pdf/2017-revue_strategique_dsn_cle4b3beb.pdf

Revue stratégique de cyberdéfense (SGDSN, 12/02/2018)

Le Secrétariat général de la Défense et de la Sécurité nationale publie un texte de 167 pages qui vient affirmer l'ambition française dans le milieu de la cyberdéfense. Il s'agit de reconnaître l'imprévisibilité des attaques cyber aux conséquences potentiellement dramatiques pour mieux affirmer sa souveraineté numérique à travers un dispositif national de protection et de défense informatique robuste.

Pour en savoir plus :
https://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf

Rapport d'information déposé en application de l'article 145 du Règlement par la Commission de la défense nationale et des forces armées en conclusion des travaux d'une mission d'information sur la cyberdéfense et présenté par M. Bastien LACHAUD et Mme Alexandra VALETTA-ARDISSON (Assemblée nationale, 2018)

Ce rapport tente de remettre en lumière les enjeux liés à la cyberdéfense française. Qu'est ce que la cyberdéfense ? Qu'est ce qui fait la spécificité du milieu cybernétique ? Quel est le modèle français en la matière, comparé à d'autres modèles étatiques ? Quelles sont les pistes d'évolution envisageables ?

Pour en savoir plus :
https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b1141_rapport-information

Revue nationale stratégique (2022)

Le gouvernement fait en 2022 le constat très clair d'un retour de la « guerre de haute intensité » et donc du besoin de la France de s'y préparer, avec des stratégies hybrides mais aussi l'arme cyber. Ces stratégies hybrides et cyber ressortent comme des éléments clés dans lesquels la France doit renforcer ses capacités et sa résilience (objectifs stratégiques n°4 et 9), alors qu'existe une menace cybercriminelle dans un phénomène de guerre mondialisée. La cyberdéfense n'est autre qu'un véritable enjeu à maîtriser dans une volonté de répondre ou de riposter à des manœuvres ou à des attaques, en particulier dans le champ informationnel contre les intérêts français. Si la France bénéficie de certains acquis dans ce domaine, elle reconnaît ne pas devoir manquer de les consolider.

Pour en savoir plus :
https://www.sgdsn.gouv.fr/files/files/Revue%20nationale%20strat%C3%A9gique%20-%20Fran%C3%A7ais.pdf

Les doctrines de lutte informatique

- La lutte informatique défensive (LID)
  https://www.defense.gouv.fr/sites/default/files/ministere-armees/Politique%20minist%C3%A9rielle%20de%20lutte%20informatique%20d%C3%A9fensive.pdf
- La lutte informatique offensive (LIO)
  https://www.defense.gouv.fr/sites/default/files/ministere-armees/Lutte%20informatique%20offensive%20%28LIO%29.PDF
- La lutte informatique d'influence (L2I)
  https://www.defense.gouv.fr/sites/default/files/ema/Doctrine%20de%20lutte%20informatique%20d%25u2019influence%20%28L2I%29.pdf
- La droit international appliqué aux opérations dans le cyberespace
  https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf

POINTS À SURVEILLER

1. L'investissement professionnel

Quelles mesures concrètes la France prend-elle pour rester à la pointe de l'innovation et de la recherche en matière de cybersécurité ? Comment la France assure-t-elle le développement et le recrutement de talents dans le domaine de la cyberdéfense pour faire face à la concurrence internationale ? Quels sont les investissements spécifiques alloués à la formation et à la sensibilisation des professionnels de la cybersécurité en France ?

- CYBER : un séminaire pour sensibiliser les futurs officiers à la cyberdéfense. (17/03/2023). Ministère des Armées.
- CYBER : l'importance du cyberespace d'après les généraux Bauer et Thierry Blanc. (30/11/2022). Ministère des Armées.
- Machi, V. (08/11/2022). CYBER : quatre questions au responsable de la cybermission militaire française. Defense news.

2. Le positionnement français face aux autres acteurs cyber

Comment la France détecte-t-elle les nouvelles menaces émergentes et anticipe-t-elle les tactiques utilisées par les attaquants ? Quelles sont les mesures prises pour renforcer la résilience et l'adaptabilité des infrastructures et des systèmes face aux attaques sophistiquées ? Quelles collaborations la France a-t-elle établies avec d'autres pays pour partager des informations sur les menaces cybernétiques et renforcer la réponse collective ?

- Gain, N. (13/03/2023). CYBER : « accélerer la cybersécurisation » de la BITD française. Forces opérations blog.
- COOPÉRATION : le COMCYBER participe à un exercice international de grande envergure de l'OTAN. (09/12/2022). Ministère des Armées, EMA.

3. Le maintien d'une certaine éthique et transparence

Comment la France définit-elle les lignes directrices éthiques pour ses opérations de cyberdéfense, en particulier lorsqu'il s'agit de contre-attaques ou de ripostes cybernétiques ? Quelles sont les garanties mises en place pour prévenir les atteintes aux droits fondamentaux des individus lors d'opérations de cyberdéfense ? Comment la France assure-t-elle la transparence et la responsabilité de ses actions de cyberdéfense tout en préservant les secrets liés à la sécurité nationale ?

- CYBER : l'exercice de cyberdéfense DEFNET 2023 pour sensibiliser les jeunes au cybercombat. (24/03/2023). Ministère des Armées, EMA.

4. Quelle souveraineté numérique française et/ou européenne

Quelles sont les initiatives de coopération internationale mises en place par la France pour promouvoir des normes communes en matière de souveraineté numérique et de cybersécurité ? Quels apprentissages la France tire-t-elle du contexte international ?

- LU : Passer à l'échelle en matière de cybersécurité. (Juin 2023). Institut Montaigne.
- Bergmann, M. & Monaghan, S. (07/07/23). GÉOPOLITIQUE : « la tâche de l'OTAN à Vilnius est simple : transformer la défense européenne ». Defense news.
- Tisseyre, D. (07/06/2023). ENTENDU : les enjeux de la Cyberdéfense. Defense News.
- COOPÉRATION : le COMCYBER invite les cybercommandeurs européens au CYBERCO. (02/04/2023). Ministère des Armées, EMA.
- GUERRE EN UKRAINE - Cyberespace : la bataille des récits. (23/02/2023). Ministère des Armées.
- CYBER : l'Europe renforce sa coopération dans la cyberdéfense. (16/11/2022). Ministère des Armées.