

LE MONDE DU CYBER

EDITO

« Au cours de l'année 2023, l'ANSSI a pu constater des évolutions notables dans la structure et les méthodes des attaquants informatiques. Les opérations d'espionnage stratégique et industriel se maintiennent à un niveau élevé, et se concentrent de plus en plus sur des individus et des structures non gouvernementales qui créent, hébergent ou transmettent des données sensibles. Pour atteindre leurs objectifs, les acteurs de la menace perfectionnent leurs techniques afin d'éviter d'être détectés et suivis, voire identifiés. La menace d'attaques à but lucratif se maintient également à un niveau élevé, alimentée par des acteurs aux profils de plus en plus divers. L'écosystème cybercriminel profite aujourd'hui d'outils et de méthodes diffusés large ment pour cibler des secteurs particulièrement vulnérables, avec des conséquences parfois graves pour la continuité d'activité et la protection des données à caractère personnel. [...] »

ANSSI

Conclusion « PANORAMA DE LA 2023 »

A travers ce dossier, découvrez les articles, ouvrages et reportages publiés sur le site espritsurcouf.fr traitant du cyber. Afin de vous simplifier la lecture des articles, ces derniers sont classés en fonction de leur nature : articles, ouvrages, reportages, revue de presse.

Que contient ce monde du CYBER que nous avons décrit à plusieurs fois dans ESPRITSURCOUF ? C'est l'objectif « ambitieux » de ce dossier ? Le terme cyber recouvre l'ensemble des activités liées à l'utilisation offensive du cyberspace : Cyber sécurité, les actions de piratage informatique et les moyens de s'en protéger. Cyber défense, l'utilisation du piratage informatique à des fins militaires et les moyens de s'en protéger. Cyber espionnage, l'utilisation du piratage informatique à des fins de renseignement économique, technologique, politique ou militaire. Cyber surveillance, les actions menées par un Etat pour surveiller sa population par des moyens numériques (par exemple : la reconnaissance de visages en Chine) et où par la censure d'internet et des réseaux sociaux. Cyber guerre, affrontement entre plusieurs Etats, utilisant des moyens cyber. Cyber criminalité, criminalité constitutive d'une infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau ». La manipulation offensive des réseaux sociaux en les utilisant à des fins d'influence politique par la diffusion massive d'infox (« fake news ») ou d'informations confidentielles compromettantes.

SOMMAIRE

DEFINITION DU MOT CYBER.....	3
1. Définition du mot « Cyber »	3
2. Quelle est la différence entre la Cybersécurité et la Cyberdéfense ?.....	3
APPARITION, DEVELOPPEMENT DE LA CYBERSECURITE	6
1. Chronologie succincte.....	6
2. Développement	7
APPARITION, DEVELOPPEMENT DE LA CYBERDEFENSE	9
1. Chronologie succincte.....	9
2. Développement	9
ARTICLES PUBLIES SUR LE SITE en 2024 – 2023	11
1. Géopolitique	11
2. Humeurs.....	12
3.. Défense	12
QUELQUES SITES DE BASE A CONNAITRE	14
1. Sites officiels	14
2. Ecole de formation.....	15
3. Assistance.....	15
RESSOURCES	16
VIDEOS	20
PODCAST	22
LIVRES.....	23

DEFINITION DU MOT CYBER

1. Définition du mot « Cyber »

Il ne se passe un jour sans que nous lisions, dans des posts publiés sur les réseaux sociaux ou dans les médias traditionnels, le mot « Cyber ». Vulgairement, ce mot est utilisé pour parler du numérique, du monde d'internet.

Mais de quoi s'agit-il exactement ? Grammaticalement parlant, il s'agit du préfixe d'origine grecque « *kubernan* » qui signifie « gouverner ». Le sens actuel a pour origine le mot anglais « *cyberspace* ». Ce dernier fut inventé par l'auteur américain de science-fiction, William Gibson, dans son livre intitulé *Neuromancer* en 1984.

Aujourd'hui nous pouvons l'utiliser de deux manières :

- Associé à un autre mot (ex. : *culture cyber, ère cyber, génération cyber*)
- Seul où le sens peut être différent selon le contexte (ex. *le cyberspace, la cyberculture ou l'ensemble des nouvelles technologies*).

Certains écrits mentionnent que le mot « cyber » serait réapparu au milieu du xx^e siècle afin d'être utilisé pour former des mots liés aux nouvelles techniques de communication numériques, multimédia, Internet. Il est également utilisé pour désigner la cybernétique (étude des processus de contrôle et de communication chez l'être vivant et la machine) !

En France, nous parlons régulièrement dans les médias de CYBERSECURITE et de CYBERDEFENSE. Mais de quoi s'agit-il réellement ?

Le modèle français de cybersécurité et de cyberdéfense repose sur une **séparation claire, au sein de l'État, entre les missions défensives et offensives.**

Cyberdéfense : Ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberspace 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.

2. Quelle est la différence entre la Cybersécurité et la Cyberdéfense ?

Il s'agit de deux concepts étroitement liés mais distincts dans le domaine de la protection des systèmes d'information. Pour comprendre la différence entre les notions de cybersécurité et

cyberdéfense, il faut avant tout réussir à cerner et délimiter la différence existant entre la sécurité et la défense ...

Quelle différence existe-t-il entre la sécurité et la défense ?

La **sécurité** est un état recherché tandis que la **défense** est une posture.

Quelle différence existe-t-il entre la cybersécurité et la cyberdéfense ?

La **cybersécurité** fait référence à la protection des systèmes d'information de manière générale. Elle englobe les technologies, organisations, processus, dispositifs, concepts, les lois ... visant à protéger les systèmes contre diverses menaces et risques informatiques.

La **cyberdéfense**, quant à elle, est plus spécifiquement liée à la défense nationale. L'Agence nationale de la sécurité des systèmes d'information définit la cyberdéfense comme « l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberspace les systèmes d'information jugés essentiels ».

La cyberdéfense est présentée par le D^r Charles-Emond Bichot comme l'ensemble des moyens de sécurité secondaire (ce qui résiste pendant l'évènement de sécurité) : systèmes, services et procédures qui fonctionnent dans une organisation pour protéger son système d'information, pris au sens large, pendant une cyberattaque. Dans ce modèle, il faut comprendre la cybersécurité, vue dans le cadre de la lutte informatique défensive, comme la somme de la cyberprotection (sécurité primaire, "avant l'évènement"), de la cyberdéfense (sécurité secondaire, "pendant l'évènement") et de la cyber résilience (sécurité tertiaire, "après l'évènement")

Selon Nicolas Ténèze, la cyberdéfense rassemble la cybersûreté, la cybersécurité, la cyberrésilience (lutte informatique défensive), et la cyberagression (lutte informatique offensive). Les approches proactives et réactives sont comprises dans certaines de leurs composantes.

En résumé, la cybersécurité vise une protection plus large et préventive, tandis que la cyberdéfense est orientée vers la stratégie de défense nationale, souvent avec une dimension réactive face aux cyberattaques.

3. Autres définitions

Cyberspace : Le cyberspace 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 cyberspace. 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.

APPARITION, DEVELOPPEMENT DE LA CYBERSECURITE

1. Chronologie succincte

Décembre 2013 - La Loi de programmation militaire pour 2014-2019 est votée

L'article 15 détaille

- Les obligations que le Premier ministre peut imposer aux opérateurs d'importance vitale en matière de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles ;
- Les sanctions pénales prévues et applicables en cas de non-respect de ces obligations.

Le fait que ces obligations soient traitées dans la Loi de programmation militaire montre simplement que la défense et la sécurité nationale doivent être traitées globalement et de manière cohérente.

21 février 2014, Jean-Marc Ayrault, Premier ministre, déclare que la cybersécurité « est une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement »

Un peu plus d'un an plus tard, le **6 juillet 2015**, Axelle Lemaire, secrétaire d'État au numérique, indique que « *Le Gouvernement présentera dès la rentrée prochaine une stratégie nationale globale sur la cybersécurité* ». C'est chose faite le 16 octobre 2015, Manuel Valls, alors Premier Ministre, présente **la Stratégie nationale pour la sécurité du numérique**.

Les objectifs ET orientations fixés par cette stratégie, élaborée avec l'ensemble des ministères, sont au nombre de deux :

1. Conforter la sécurité et la défense de nos infrastructures critiques ;
2. Accompagner la transition numérique en définissant les leviers humains, techniques et opérationnels nécessaires à l'innovation, au développement économique et à la confiance des Français dans le numérique.

3 mars 2017 - Constitution du groupement d'Intérêt Public « Action contre la Cybermalveillance » également appelé « GIP ACYMA » réunissant les acteurs publics et privés de la cybersécurité.

17 octobre 2017 - Ouverture de la Cybermalveillance.gouv.fr au public dont les objectifs sont :

Page 6 sur 27

Dossier « Monde du cyber »

Réalisé par Laure Fanjeau

site : www.espritsurcouf.fr

Mai 2024

- Assiste les victimes d'actes de cybermalveillance ;
- Informer et sensibiliser sur la sécurité numérique ;
- Observer et anticiper le risque numérique.

2. Développement

La cybersécurité et le plan Vigipirate

Elle est un des 12 domaines du plan Vigipirate qui concerne directement l'ANSSI, les OIV et leurs sous-traitants, ainsi que les Administrations.

Domaines d'action du plan Vigipirate et ses mesures

Le plan *Vigipirate* prévoit douze domaines d'action. Il s'agit des secteurs qui pourraient être visés par une menace terroriste, et dont la protection et la mobilisation sont indispensables pour la réponse à cette menace.

1. Alerte-intervention ;
2. Rassemblements ;
3. Installations et bâtiments ;
4. Installations dangereuses et matières dangereuses ;
- 5. Cybersécurité ;**
6. Secteur aérien ;
7. Secteur maritime ;
8. Transports terrestres ;
9. Santé ;
10. Chaîne alimentaire ;
11. Réseaux (communications électroniques, eau, électricité, hydrocarbures, gaz) ;
12. Etranger (ressortissants français résidents ou voyageurs, emprises représentatives de l'État français, personnel de l'État français, entreprises françaises, transport maritime et aérien).

Chaque domaine d'action fait l'objet d'une stratégie de vigilance et de protection, qui se décline en objectifs de sécurité et en mesures.

Au total, le plan *Vigipirate* compte une centaine de mesures permanentes et environ deux cents mesures additionnelles. Certaines mesures sont obligatoires (celles qui s'appliquent aux services de l'État, celles qui font référence à des obligations légales des différents acteurs...) Les autres sont des recommandations.

Source : [Wikipedia](#)

Création d'un label cybersécurité

Un **label « France Cybersecurity »** a été créé pour sensibiliser les utilisateurs et répond à plusieurs besoins et objectifs :

- Promouvoir les solutions de cybersécurité françaises et accroître leur visibilité à l'international ;
- Sensibiliser les utilisateurs et donneurs d'ordre internationaux à l'importance de l'origine française d'une offre de cybersécurité et aux qualités qui lui sont propres ;
- Attester auprès des utilisateurs et donneurs d'ordre, la qualité et les fonctionnalités des produits et services ainsi labellisés ;
- Accroître globalement leur usage et élever le niveau de protection des utilisateurs.

APPARITION, DEVELOPPEMENT DE LA CYBERDEFENSE

1. Chronologie succincte

Juillet 2009 - Création de l'ANSSI. Aujourd'hui cet engagement pour la défense et la sécurité de la France dans le cyberspace fait l'objet d'un document de stratégie à l'attention de tous.

2013 - Le *Livre blanc sur la défense et la sécurité nationale de 2013*, reprenant les éléments de celui de 2008, a intégré de manière plus approfondie la menace cybernétique dans la stratégie nationale. Soulignant qu'une attaque contre les systèmes d'information d'importance vitale pouvait relever de la sécurité nationale, ce document fondateur a fait de la cyberdéfense une priorité. [...]

2. Développement

La cyberdéfense au sein du ministère des Armées

Enjeu et priorité stratégique, la cyberdéfense est garante de la souveraineté nationale. Avec de nombreux acteurs, le ministère des Armées participe activement à la protection et à la défense des systèmes d'information dans le cyberspace.

La cyberdéfense, priorité ministérielle et enjeu militaire

L'affrontement dans le cyberspace est désormais une réalité. La menace cyber est permanente et en évolution continue. Profitant des opportunités offertes par le cyberspace, le nombre et l'intensité des attaques menées dans ce milieu ne cessent de croître, visant le profit financier, la captation de données, la déstabilisation des institutions par la manipulation des opinions ou la paralysie de systèmes étatiques et privés. Les Armées intègrent désormais le combat cybernétique comme un mode d'action à part entière dont les effets se combinent aux autres dans une manœuvre globale.

Enjeu et priorité stratégique, la cyberdéfense est garante de la souveraineté nationale. En lien avec de nombreux acteurs, le ministère des Armées participe activement à la protection, à la défense des systèmes d'information et des systèmes d'armes, ainsi qu'à la conduite de opérations dans le cyberspace.

Les acteurs militaires de la cyberdéfense

Au sein du ministère des Armées, le Commandement de la cyberdéfense – placé sous l'autorité directe du chef d'état-major des armées – rassemble l'ensemble des forces de cyberdéfense du ministère sous une autorité interarmées. Il a pour mission la défense des

systèmes d'information, ainsi que la conception, la planification et la conduite des opérations militaires dans le cyberspace. Il a une mission de fédération et de conduite des actions des différents acteurs du ministère.

[...]

Découvrez le COMCYBER [en cliquant ICI](#)

Domaine d'action la cyberdéfense

La stratégie française pose **quatre objectifs stratégiques** :

1. Etre une puissance mondiale de cyberdéfense et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie ;
2. Garantir la liberté de décision de la France par la protection de l'information de souveraineté ;
3. Renforcer la cybersécurité des infrastructures vitales nationales ;
4. Assurer la sécurité dans le cyberspace.

Sept axes d'effort :

1. Anticiper, analyser Détecter, alerter, réagir ;
2. Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines ;
3. Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales ;
4. Adapter notre droit ;
5. Développer nos collaborations internationales ;
7. Communiquer pour informer et convaincre.

Source : [ANSSI](#)

ARTICLES PUBLIES SUR LE SITE en 2024 – 2023

1. Géopolitique

« Europe, un avenir crédible »

Jean-Dominique Giuliani, Président de la Fondation Robert Schuman
N°234 - 03/05/2024

Au moment où les peuples européens vont élire leurs députés, dans deux articles successifs l'auteur pose les questions sur le futur de l'Europe, il trouve des réponses dans le discours d'Emmanuel Macron à la Sorbonne, Mais le Président saura-t-il les concrétiser rapidement ? Au lecteur, à l'électeur de faire sa réflexion et son choix. [...]

Pour lire l'article, [cliquez ICI](#)

« Confiscation des avoirs russes : un profond dilemme »

Yannick Harrel, Doctorant en sciences de l'ingénieur
N°233 - 19/04/2024

L'auteur souligne la dichotomie qu'il peut y avoir entre les effets d'annonce, quant à la perspective de saisie des avoirs russes, et la complexe réalité aux lourdes conséquences juridiques, financières et politiques. [...]

Pour lire l'article, [cliquez ICI](#)

« Ukraine, trois scénarios »

Michel Goya, Docteur en Histoire moderne et contemporaine
N°205 - 12/01/2023

C'est en janvier 2023 que l'auteur offrait un regard sur le conflit russo-ukrainien à travers plusieurs perspectives quant à son évolution. Ses hypothèses sur le devenir du rapport de force donnent donc lieu à plusieurs scénarios qui restent tout à fait d'actualité, en cette fin d'année. Preuve aussi que le conflit s'inscrit dans la durée avec un rythme de progression opérationnelle resté, somme toute, assez faible. À l'inverse des pertes humaine qui, morts et blessés confondus pour les deux camps, s'élèvent à plus d'un demi-million.... [...]

Pour lire l'article, [cliquez ICI](#)

« Guerre en Ukraine : Vers un nouvel ordre mondial ? » (2^{ème} partie)

Général de Division (2s) Jean-Claude Allard

N°208 – 24/02/2024

Dans une première partie ([voir N°225](#)), Jean-Claude Allard dressait un état global de la guerre russo-ukrainienne du conflit. Ici, il se penche sur le caractère multifactoriel du conflit, porteur d'un nouvel ordre mondial en gestation. [...]

Pour lire l'article, [cliquez ICI](#)

« De Pyongyang à Moscou, le rapprochement russo-nord-coréen »

Tom Dash, Diplômé d'un Bachelor en Relations internationales de l'ILERI

N°224 – 03/11/2023

La visite d'une délégation russe à Pyongyang en juillet dernier annonçait une rencontre à haut niveau entre Kim Jong-un et Vladimir Poutine laquelle fut suivie d'une visite de Sergueï Lavrov en octobre. Si la Corée du Nord semble avoir tout à gagner de ce rapprochement, tel n'est pas le cas pour la Russie qui, déjà affaiblie, risque de voir sa position se détériorer davantage à long terme. [...]

Pour lire l'article, [cliquez ICI](#)

2. Humeurs

« 2023, symphonie d'un nouveau monde »

Vincent Gourvil, Pseudonyme d'un haut fonctionnaire et Docteur en sciences politiques

N°228 - 29/12/2023

Cette fin 2023 est l'occasion, pour l'auteur, de dresser une rétrospective de l'année écoulée en matière de relations internationales et de conflictualité. Ce qui, conjointement, ouvre sur des perspectives et préoccupations majeures pour l'année à venir. Les opinions exprimées ici n'engagent que leur auteur. [...]

Pour lire l'article, [cliquez ICI](#)

3.. Défense

« L'intelligence artificielle dans l'industrie de défense en France »

N°226 - 01/12/2024

Alors qu'aux États-Unis, l'IA paraît instable, comme le montre l'affaire de Sam Altman, ancien PDG licencié d'OpenAI, qui vient de revenir à la tête de l'entreprise, cet article explore les ambitions françaises dans le domaine de l'intelligence artificielle (IA) appliquée à la défense. Il cherche à mettre en lumière la dynamique française et les défis à relever, notamment en matière d'innovation, de réglementation et d'éthique. [...]

Pour lire l'article, [cliquez ICI](#)

« Retour sur la LPM » (Loi de programmation militaire)

Victor Denis, Etudiant en relations internationales et le général de brigade (2s) François Chauvancy

N°173 – 22/09/2024

Quel regard porter sur les besoins de nos armées ? Quels choix budgétaires avons-nous fait ? Qu'est-ce que cette LPM raconte des relations entre politiques et militaires ? L'auteur nous propose quelques éléments de réponse dans son entretien avec le général François Chauvancy (2S).

Pour lire l'article, [cliquez ICI](#)

QUELQUES SITES DE BASE A CONNAITRE

1. Sites officiels

[Agence nationale de la sécurité des systèmes d'information | SGDSN](#)

Créée en 2009, l'ANSSI, autorité nationale de cybersécurité, propose au Premier ministre les mesures destinées à répondre aux crises affectant la sécurité des systèmes d'information des autorités publiques et des opérateurs régulés. Elle coordonne l'action gouvernementale et anime l'écosystème national. [...]

Son action pour la protection de la Nation face aux cyberattaques se traduit en quatre grandes missions : défendre, connaître, partager, accompagner. [...]

[Commandement de la cyberdéfense | Ministère des Armées \(defense.gouv.fr\)](#)

Le COMCYBER rassemble l'ensemble des forces de cyberdéfense du ministère des Armées. Il a pour mission la défense des systèmes d'information – dont les systèmes d'armes, ainsi que la conception, la planification et la conduite des opérations militaires dans le cyberspace. [...]

[Page d'accueil DGNUM | Ministère des Armées \(defense.gouv.fr\)](#)

Au cœur de nos capacités militaires et de notre fonctionnement, le numérique renforce la simplicité, l'efficacité et la rapidité du ministère des Armées.

Créée en 2018 à l'initiative de Florence Parly, ministre des Armées, dans le cadre de l'Ambition Numérique ministérielle en déclinaison de l'Action Publique 2022, la DGNUM (Direction générale du numérique et des systèmes d'information et de communication) est le chef d'orchestre de la transformation numérique du ministère des Armées. [...]

[Cybersécurité : formation en ligne gratuite pour tous - francenum.gouv.fr](#)

Comment se former à la cybersécurité et protéger efficacement son entreprise contre les cyberattaques et les risques informatiques ? La sensibilisation et l'accompagnement des personnels des TPE PME en termes de bonnes pratiques est essentielle pour la sécurité numérique.

Une formation sur la cybersécurité gratuite et ouverte à tous en 11 modules est mise à disposition depuis 2019 par SERENE-RISC, réseau de mobilisation des connaissances des centres d'excellence du Gouvernement du Canada. Objectif : protéger contre les risques en ligne et en minimiser les conséquences par la diffusion des connaissances. Ces modules sont notamment mis à disposition des bibliothèques au Canada. Une offre de formation très intéressante. [...]

NATO - Cyberdéfense

Les cybermenaces pesant sur la sécurité de l'Alliance sont complexes, destructrices, à visée coercitive, et de plus en plus fréquentes. Le cyberspace est le théâtre d'une contestation permanente, et des actes de cybermalveillance s'y déroulent quotidiennement, allant d'attaques peu sophistiquées jusqu'à des attaques menées à l'aide de technologies de pointe. La réponse de l'OTAN et des Alliés consiste à renforcer la capacité de l'Alliance à détecter et prévenir les actes de cybermalveillance et à y répondre. L'Organisation et les Alliés s'appuient sur des moyens de cyberdéfense forts et résilients pour accomplir les trois tâches fondamentales de l'Alliance que sont la dissuasion et la défense, la gestion et la gestion des crises et la sécurité coopérative. L'Alliance doit être préparée à défendre ses réseaux et opérations contre les cybermenaces toujours plus complexes auxquelles elle est confrontée. [...]

2. Ecole de formation

42 | Apprendre à coder. Casser les codes. Formation gratuite

42 : ce que l'enseignement de l'informatique a de meilleur à proposer. Innovante, différente et ouverte, la formation met l'accent sur les projets et le travail de groupe plutôt que sur l'enseignement théorique. Un concentré de nouveautés pédagogiques pour permettre aux talents de demain de se révéler.

3. Assistance

Assistance aux victimes de cybermalveillance

Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger. [...]

Cyberharcèlement (harcèlement sur internet) | Service-Public.fr

Le harcèlement par internet est appelé *cyberharcèlement*. Il s'agit d'un *délict Acte interdit par la loi et puni d'une amende et/ou d'une peine d'emprisonnement inférieure à 10 ans*. Si vous êtes victime d'un harcèlement en ligne, vous pouvez signaler les faits à la police ou à la gendarmerie et demander la suppression des contenus *illicites / interdit par la loi*. Vous pouvez également déposer plainte contre l'auteur du cyberharcèlement et / ou contre *l'hébergeur internet, personne physique ou dirigeant d'une personne morale qui stocke des écrits, des sons, des images ou des vidéos réalisés par des tiers (hébergeurs d'un réseau social, d'un forum, d'un jeu en ligne, d'un blog)*. Nous vous présentons les étapes à suivre. [...]

RESSOURCES

« Livre Blanc sur la défense et la sécurité nationale 2013 »

Ministère de la Défense / SGA / SPAC - 29/04/2013

Publié le 29 avril 2013, le Livre blanc sur la défense et la sécurité nationale constitue le quatrième exercice du genre (*après ceux de 1972, 1994 et 2008*). Il répond au souhait, exprimé par le Président de la République à l'été 2012, de disposer d'un nouveau document fixant la politique de défense et de sécurité de la France pour les cinq ans à venir.

Depuis 2008, ce document couvre le champ de la défense mais aussi celui de la sécurité nationale, prenant ainsi en compte la continuité des risques et menaces de toute nature pesant sur notre Nation et la nécessité d'apporter une réponse globale à ces défis. Document de diplomatie publique, mais aussi document de référence pour l'ensemble des acteurs en charge de la programmation et de la planification des ressources, il constitue à ce titre le document cadre de la stratégie de défense française pour les années à venir, ainsi que pour les diverses politiques qui la composent : politique de défense, stratégie militaire et capacitaire, stratégie technologique et industrielle, politique de ressources humaines, etc.

[...]

Pour télécharger le Livre Blanc, [cliquez ICI](#)

« Les évolutions de la cybersécurité : contraintes, facteurs, variables... »

DGRIS - 06/2015 - N° 1506388759

De la lecture des multiples stratégies, politiques, plans, programmes de cybersécurité et cyberdéfense publiés de par le monde ces dernières années, paraît émerger un consensus, une convergence de tous, reconnaissant la nécessité d'organiser et assurer la sécurité et la défense du domaine cyber, c'est-à-dire tout d'abord la sécurité et défense de l'ensemble des systèmes techniques eux-mêmes, et celles des sociétés qui sont traversées par ces systèmes. De la sécurité des systèmes dépend celle de l'Etat-nation. Le consensus prend forme dans l'acceptation par tous de la trame d'un récit relativement simple, constitué de quelques briques élémentaires. Ce récit tourne autour de trois protagonistes : il y a « nous », « La menace », et « le cyberspace ».

[...]

Pour télécharger le rapport, [cliquez ICI](#)

« Revue stratégique de cyberdéfense »

SGDSN - 12/02/2018

Véritable Livre blanc de la cyberdéfense, il est le premier grand exercice de synthèse stratégique dans ce domaine.

Page 16 sur 27

Dossier « Monde du cyber »

Réalisé par Laure Fanjeau

site : www.espritsurcouf.fr

Mai 2024

Organisé en trois parties, il dresse un panorama de la cybermenace, formule des propositions d'amélioration de la cyberdéfense de la Nation et ouvre des perspectives visant à améliorer la cybersécurité de la société française.

La revue stratégique de cyberdéfense, confiée par le Premier ministre Edouard Philippe à Louis Gautier, secrétaire général de la défense et de la sécurité nationale, marque le début d'une stratégie de cyberdéfense fondée sur le durcissement de la protection des systèmes informatiques de l'Etat et des organismes d'importance vitale ainsi que le renforcement de la sécurité numérique pour les citoyens, les institutions et l'ensemble des acteurs qui participent du dynamisme économique, industriel, social et culturel de notre pays.

[...]

Pour télécharger la revue stratégique, [cliquez ICI](#)

« Revue nationale stratégique 2022 »

SGDSN - 12/11/2022

Revue nationale stratégique, présentée le mercredi 9 novembre par le Président de la République.

Mercredi 9 novembre 2022, à l'occasion d'un déplacement à Toulon, le Président de la République a dévoilé la revue nationale stratégique (RNS). Ce document dresse le panorama de notre environnement de défense et de sécurité, aussi bien national qu'international, puis identifie les enjeux stratégiques, opérationnels et capacitaires auxquels la France sera confrontée dans les prochaines années.

L'invasion de l'Ukraine, le durcissement de la compétition stratégique, le retour explicite du fait nucléaire dans la compétition stratégique et un recours accru aux modes d'action non militaires sont autant d'éléments factuels qui démontrent la nécessité de mener une réflexion sur l'évolution de notre outil de défense, dans le cadre de l'autonomie stratégique européenne, de nos alliances et de partenariats renouvelés. La prise en compte du risque de conflit de haute intensité et de l'emploi de stratégies hybrides doit particulièrement guider nos réflexions pour accroître notre résilience.

La RNS 2022 présente ainsi dix objectifs stratégiques que la France se fixe pour assurer son rôle de puissance d'équilibres et garantir la sécurité de ses intérêts.

[...]

Pour télécharger la revue stratégique, [cliquez ICI](#)

« Panorama de la cybermenace 2023 »

ANSSI – 02/2024

Cette troisième édition du Panorama de la cyber menace décrit les principales tendances constatées en 2023 par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Ce document se concentre sur les intentions des attaquants, leurs capacités et les opportunités exploitées pour compromettre des systèmes d'information (SI), en fournissant des exemples concrets d'incidents traités par l'ANSSI durant l'année. Le niveau de la menace

informatique continue d'augmenter, dans un contexte marqué par de nouvelles tensions géopolitiques et la tenue d'événements internationaux sur le sol français. L'ANSSI estime aujourd'hui que les attaquants réputés liés à la Chine, à la Russie et à l'écosystème cybercriminel constituent les trois principales menaces tant pour les systèmes d'information français les plus critiques que pour l'écosystème national de manière systémique. Cette année encore, l'espionnage stratégique et industriel est la menace qui a le plus mobilisé les équipes de l'ANSSI. L'agence note une augmentation significative du ciblage d'entités travaillant dans des domaines stratégiques – groupes de réflexion, instituts de recherche et base industrielle et technologique de défense (BITD) – ou qui assurent la transmission de données sensibles, comme les entreprises de télécommunications et de fourniture de services numériques (ESN). Pour ce faire, les attaquants continuent de perfectionner les techniques qui leur permettent de s'introduire sur des systèmes d'information, de s'y propager, d'exfiltrer des informations ou de se prépositionner, et d'éviter d'être détectés. En parallèle, l'ANSSI constate une augmentation du nombre d'attaques contre des téléphones portables professionnels et personnels afin d'espionner des individus ciblés. Cette tendance est notamment soutenue par la prolifération de solutions offensives commercialisées par des entreprises privées

Pour télécharger le rapport, [cliquez ICI](#)

Collection Gestion de crise cyber



Face à une menace informatique toujours croissante et en mutation, l'amélioration de la résilience numérique par l'entraînement à la gestion de crise cyber n'est plus seulement une opportunité, mais bien une nécessité pour toutes les organisations. L'ANSSI met à leur disposition la collection « Gestion de crise cyber », destinée à les

accompagner dans la préparation et la gestion de crise cyber. Cette collection vise à apporter une expertise transverse sur l'ensemble des aspects de la gestion de crise cyber, et se compose ainsi de trois tomes : Organiser un exercice de gestion de crise cyber, Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique et Anticiper et gérer sa communication de crise cyber. [...]

Collection Cyberattaques et remédiation



Les dégâts financiers et matériels que peut occasionner une attaque informatique sont considérables. Si un incident majeur est partiellement ou mal remédié, ses effets peuvent s'étendre dans la durée. Ce fort potentiel de déstabilisation exige, à la fois des

organisations cibles et des prestataires de cybersécurité, un savoir-faire dans l'endiguement de ces cyberattaques, dans la reprise de contrôle du système d'information compromis et dans le rétablissement d'un état de fonctionnement suffisant. La remédiation est l'étape clé pour y parvenir. L'ANSSI a donc élaboré un corpus s'articulant en trois volets (stratégique, opérationnel et technique) afin de partager son expérience de la mise en œuvre et du pilotage de la remédiation [...]

VIDEOS

Cybermonde - L'avenir c'est maintenant | ARTE



Durée : 01:31:40

Date de mise en ligne : 17 avril 2024

Année de réalisation : 2023

Disponible jusqu'au 10/07/2024

Réalisé par Charles Ferguson et Shimon Dotan

Compte YouTube où est publié le documentaire :
Chaîne ARTE

Présentation : La promesse d'Internet, l'or noir des data, l'intelligence artificielle, la cyberguerre : en quatre tableaux, revue des récents bouleversements causés par l'irruption du cyber dans nos vies. Le préfixe cyber est issu d'un mot de grec ancien qui signifie "contrôler". Mais sommes-nous réellement capables de maîtriser des technologies qui nous dépassent ? Depuis 2016 et les ingérences étrangères dans l'élection américaine, puis celles ayant accéléré l'avènement du Brexit, les évolutions du cyber ont pris une place quasi monopolistique dans nos vies, aussi bien dans le cadre privé qu'à l'échelle de nos sociétés. De l'invention d'Internet au nouvel or noir des data, sans oublier la frénésie actuelle causée par le bond en avant de l'intelligence artificielle et l'importance prise par la guerre cyber, actuellement au premier plan de la stratégie russe contre l'Occident (suivant la vieille doctrine soviétique des trois D : "duperie, dénégation et désinformation"), revue des récents bouleversements de notre nouveau "cybermonde". [...]

Pour visionner le reportage, [cliquez ICI](#)

Cyber, un combat virtuel bien réel | #JDEF



Durée : 00:27:04

Date de mise en ligne : 27/06/2022

Réalisé par la DICOd

Nom de l'émission : #JDEF

Compte YouTube où est publié le documentaire :
Ministère des Armées

Présentation : Pour répondre à la multiplication et à l'intensification de la menace dans le cyberspace, pour protéger ses réseaux et ses systèmes de plus en plus numérisés et

Page 20 sur 27

Dossier « Monde du cyber »

Réalisé par Laure Fanjeau

site : www.espritsurcouf.fr

Mai 2024

connectés, le ministère des Armées s'attache depuis une dizaine d'années à muscler ses capacités de cybergdéfense. Le détail en images dans ce numéro inédit du Journal de la Défense.

Pour visionner le reportage, [cliquez ICI](#)

Cyberguerre : un nouvel enjeu stratégique pour l'OTAN | #cdanslair



Durée : 00:47:32

Date de mise en ligne : 15/06/2021

Réalisé par France 5

Nom de l'émission : C dans l'air

Compte YouTube où est publié le documentaire : C dans l'air

Présentation : La cyberguerre est une nouvelle menace qui était au cœur des discussions du sommet de l'OTAN. Joe Biden souhaite une alliance des démocraties contre la Chine, la Russie, la Corée du Nord, des Etats autoritaires souvent accusés de manier l'arme cyber. Un nouvel enjeu stratégique pour l'OTAN.

Pour visionner le reportage, [cliquez ICI](#)

La dimension cyber dans la guerre moderne | OPENBOXTV.fr



Durée : 00:38:11

Date de mise en ligne sur le compte YouTube d'Espritsurcouf : 30/05/2024

Réalisé par OPENBOXTV.fr

Compte YouTube où est publié le documentaire : EspritSurcouf avec autorisation d'Alain Juillet

Présentation : Dans cette nouvelle émission, Alain Juillet et Claude Medori reçoivent Arnaud Coustillère, pionnier de la cybergdéfense française (vice amirale d'escadre (2s), président du Pôle d'Excellence Cyber, ancien Comcyber.) Avec qui nous découvrons l'évolution et le poids du cyber dans les opérations militaires modernes.

Pour visionner le reportage, [cliquez ICI](#)

PODCAST



Durée : 01:17:00

Date de mise en ligne : 14/05/2024

Nom du Podcast : Collimateur

Réalisé par Rubicon – IRSEM

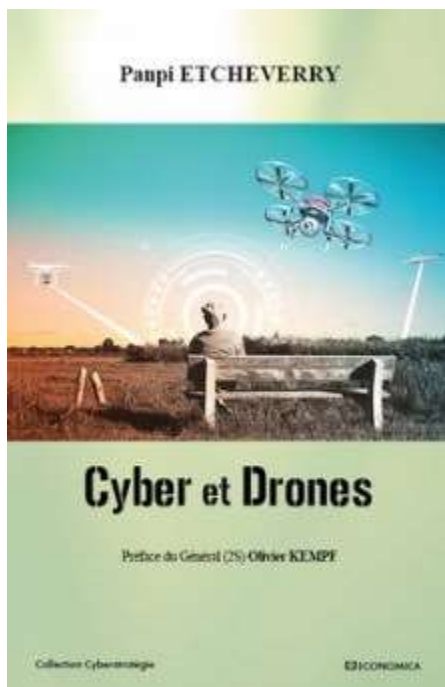
Présentation : Dans cette nouvelle émission, Alain Juillet et Claude Medori reçoivent Arnaud Coustillère, pionnier de la cyberdéfense française (vice amirale d'escadre (2s), président du Pôle d'Excellence Cyber, ancien Comcyber.) Avec qui nous découvrons l'évolution et le poids du cyber dans les opérations militaires modernes.

Collimateur plonge aujourd'hui dans un domaine central et méconnu des conflits contemporains : la guerre électronique et ses ressorts, avec l'officier et chercheur Anthony Namor — émission en partenariat avec l'Institut français des relations internationales (IFRI) et coanimée avec Élie Tenenbaum.

Pour écouter le podcast, [cliquez ICI](#)

LIVRES

Livre : « Cyber et Drones » de Panpi Etcheverry aux éditions Economica – 2018



Développez vos connaissances en Cyberstratégie avec le livre Cyber et drones

La guerre contemporaine a muté grâce à l'apport de nouveautés technologiques : les deux plus évidentes sont le cyber et les drones. Voici des armes qui permettent d'agir à distance et permettent souvent l'anonymat stratégique. Alors que l'on pensait que ces engins augmentaient la visibilité, voici qu'en fait ils accroissent la dissimulation, mais aussi l'observation et la frappe. Ils sont la première vague d'une nouvelle course aux armements qui touche désormais les grandes puissances. Simultanément, ils sont accessibles à des groupes moins structurés et irréguliers. Une nouvelle grammaire de la guerre se met en place, articulée autour de deux éléments d'apparence fort éloignés, l'un très tangible, le drone, l'autre apparemment très fugace, le cyber. Pourtant, ils partagent de nombreux points en commun,

bien repérés par cet ouvrage. Ils annoncent des bouleversements plus profonds encore, ceux de la transformation digitale qui se déroule sous nos yeux : données massives, intelligence artificielle, infonuagique, chaînes de blocs, impression 3D... Pour autant, comme toute révolution technologique, des fondamentaux demeureront, plus ou moins perceptibles : d'abord, l'existence de l'ennemi, volonté adverse douée de son libre arbitre. Ensuite, le brouillard de la guerre, tout autant épaissi que dissipé par ces nouveaux outils. Les rapports de force et les oppositions de sociétés humaines demeureront mais s'exprimeront sous de nouvelles formes : ce livre permet de les anticiper.

FICHE D'IDENTITE DU LIVRE

Auteur : Panpi Etcheverry

Editeur : Economica

Préface de : Olivier KEMPF

Nombre de pages : 180

Type de livre : Broché

Période de parution : 03/09/2018

Prix : 19€

Format : 15.5 X 24 cm

Où acheter le livre ? [Sur le site de la maison d'édition Economica](http://www.economica.com)

Page 23 sur 27

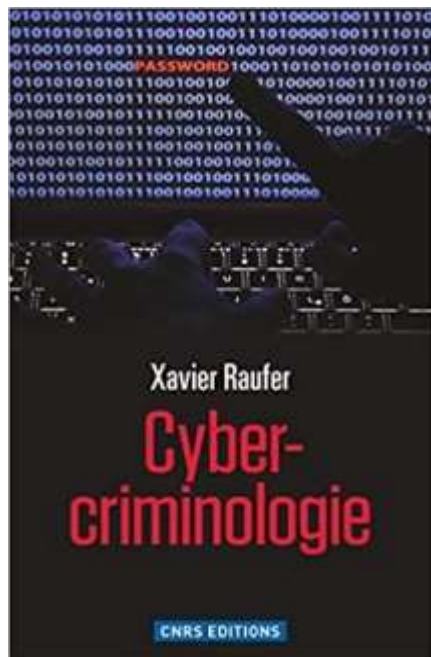
Dossier « Monde du cyber »

Réalisé par Laure Fanjeau

site : www.espritsurcouf.fr

Mai 2024

Livre : « Cyber-criminologie » de Xavier Raufer aux éditions Cnrs - 2015



Les victimes de la cyber-criminalité se comptent aujourd’hui par dizaines de millions, des stars de cinéma au client lambda d’Amazon ou de Google. Comment, à partir de quels ordinateurs et avec quels codes informatiques les nouveaux gangs du Net opèrent-ils ? C’est ce que révèle le nouveau livre de Xavier Raufer. Fondé sur des informations jusque-là éparses ou seulement connues des spécialistes, Cyber-criminologie dévoile la gravité d’un phénomène qui menace non seulement Monsieur et Madame tout le monde, mais aussi les grandes entreprises – à commencer par les géants du Net - les Etats, les banques, les universités. Quelques exemples suffisent

Des dangers qui vont de pair avec la croissance exponentielle du Net.

FICHE D’IDENTITE DU LIVRE

Auteur : Xavier Raufer

Prix : 20€

Editions : Cnrs

Format : 14.2 x 1.9 x 22 cm

Date de parution : 29/01/2015

Pages : 240 pages

Poids de l’article : 320 g

ISBN-10 : 227108556X

ISBN-13 : 978-2271085566

Où acheter le livre ? [Sur le site de Amazon.fr](http://www.amazon.fr)

Livre : « Cyber, La guerre permanente » par Jean-Louis Gergorin aux éditions La Procure - 2019



CYBER : Fake news, scandale Facebook-Cambridge Analytica, virus WannaCry

Un essai sur la guerre de l'information que se livrent les états à l'ère de la globalisation digitale, présentant les dangers de l'espace numérique et les solutions pour y faire face. Les auteurs dévoilent les acteurs, les forces et les enjeux, les risques et les menaces, avant de prévoir les scénarios possibles pour le futur.

©Electre 2019.

De la propagande djihadiste à l'ingérence électorale et de la manipulation ciblée à la cyber-attaque tous azimuts, le nouveau conflit mondial a commencé. Il a pour champ de bataille virtuel Internet. Il change la donne politique, bouleverse l'ordre géopolitique, multiplie les capacités et les formes d'agression. Il abolit la distinction entre la guerre et la paix, la sécurité et la liberté, les oligarchies et la démocratie.

De Moscou à Washington, en passant par Tel Aviv, Téhéran, Londres ou Paris, mais aussi des laboratoires secrets de la Silicon Valley aux agences de renseignement du Vieux-Continent, voici, enfin révélée, la vraie face cachée de la globalisation numérique. Dévoilant les acteurs, les épisodes et les dessous des cartes de cette lutte planétaire, décryptant l'état des forces et des enjeux, des risques et des menaces, dessinant les scénarios de demain, ce livre sans précédent, informé et percutant, nous place face à l'urgence de rompre avec l'ignorance ou la passivité.

Un grand document qui se lit comme un thriller. Un cri d'alerte indispensable sur notre proche avenir. Un manuel de résistance à la guerre permanente de l'information.

FICHE D'IDENTITE DU LIVRE

Auteur : Jean-Louis Gergorin

Éditions : La Procure

Thèmes : Géopolitique et histoire militaire

Format : 24×16 cm

Nombre de pages : 319 pages

ISBN : 2-204-11085-X

EAN : 9782204110853

Prix : 21,00€

Page 25 sur 27

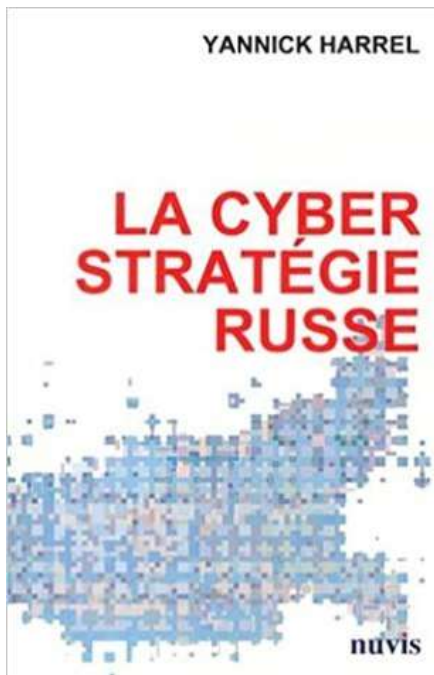
Dossier « Monde du cyber »

Réalisé par Laure Fanjeau

site : www.espritsurcouf.fr

Mai 2024

Livre : « LA CYBER STRATEGIE RUSSIE » par Yannick Harrel aux éditions Phebe Nuvis - 2013



Depuis l'avènement de l'informatique et des réseaux numériques, le cyberspace s'impose dans la majeure partie des activités humaines, aussi bien dans les secteurs civil que militaire. En raison de sa place désormais incontournable, il fait l'objet d'études et de réflexions au travers d'une discipline nouvelle : la cyberstratégie. Bénéficiant d'une filiation avec la cybernétique dont elle reprend certains éléments, la cyberstratégie peut être définie comme la « science de gouverner par le biais de systèmes de contrôle, d'information et de communication caractéristiques de ce nouveau champ stratégique qu'est le cyberspace ». La stratégie des pouvoirs à l'ère du numérique n'est pas un tout monolithique, et des spécificités nationales apparaissent, aux États-Unis, en Russie, en France et ailleurs. Jusqu'à présent, la cyberstratégie russe n'avait jamais bénéficié d'étude

sérieuse ; elle était réduite à des approximations ou perçue à travers le prisme d'études très parcellaires. Ne faisant aucunement l'impasse sur la prégnance des services de renseignement comme sur l'intérêt croissant du monde militaire pour ce nouvel espace, l'auteur de ce livre analyse les capacités et alliances potentielles de la Russie en matière de cyberspace, tout en évaluant l'émergence d'un « art de la guerre numérique » spécifiquement russe.

INFORMATIONS SUR L'AUTEUR

Yannick HARREL, expert agréé du monde russe et de son proche étranger, a étudié à Moscou et à Veliky Novgorod, puis travaillé à Saint-Pétersbourg. Membre de l'alliance GéoStratégique et animateur du blog Cyberstratégie Est-Ouest, il est chargé de cours en cyberstratégie économique et financière à Strasbourg. Il est par ailleurs l'auteur de nombreuses contributions, dont l'une fut récompensée en 2011 par le Prix Amiral Marcel Duval, décerné par la Revue de Défense Nationale française.

FICHE IDENTITE DU LIVRE

Auteur : Yannick Harrel

Prix : 25,00€

Editions : Phebe Nuvis édition

Format : 14 x 2 x 24 cm

Date de parution : 14 mars 2013

Pages : 248 pages

ISBN-10 : 2363670515

Page 26 sur 27

Dossier « Monde du cyber »

Réalisé par Laure Fanjeau

site : www.espritsurcouf.fr

Mai 2024

ISBN-13 : 978-2363670519

EAN : 9782262051624

Où acheter le livre ? [Sur le site d'Amazon](#)