Les pays face aux risques de cyberguerre
Veille sur les menaces et les solutions

Valérie Doye

25/03/2022

Sommaire

Introduction

Attaque électronique contre les systèmes informatiques, la cyberguerre vise à utiliser ces dispositifs comme moyen de propagande et de désinformation, ou bien à paralyser les activités vitales d'un pays.

Ce document traite de la cyberguerre en général, il s'appuiera sur des faits d'actualités notamment liés aux conflits entre l'Ukraine et la Russie.

Après avoir défini le cyberespace et les trois enjeux géopolitiques, nous passerons en revue les infrastructures critiques ainsi que les opérateurs d'importance vitale pouvant être déstabilisées sans avoir besoin de déplacer des soldats sur place. Les lieux susceptibles d'être touchés sont nombreux : Data Centers, centrales nucléaires, usines, hôpitaux, entreprises, banques, transport, réseaux télécoms… En somme, toutes les entités informatisées peuvent être menacées.

Enfin, après avoir abordé les moyens mis en place par les Etats afin de se protéger, nous étudierons les mesures prises par la France afin d'assurer sa souveraineté Européenne dans le cyberespace ainsi qu'un panorama des métiers de la cybersécurité.

Le cyberespace, cinquième terrain d'opérations militaires en parallèle de la terre, la mer, le ciel et de l'espace

Le cyberespace donne une nouvelle dimension aux conflits géopolitiques, c'est un domaine stratégique pour la Défense.

Il bouleverse tout, des paradigmes stratégiques classiques jusqu'à nos économies et nos modes de vie. Parce qu'il est le cadre de l'émergence de nouvelles menaces, d'actes criminels, de nouveaux combats militaires, de la collecte de renseignement, des politiques d'influence, le cyberespace oblige aussi à repenser les normes internationales et la sécurité collective. Il remet au premier plan la question de la protection des libertés individuelles et de l'avenir de la démocratie.

(Douzet, Papaemmanuel, Abdalla, & Coustillière, 2017)

Les tensions internationales actuelles causées par l'invasion de l'Ukraine par la Russie s'accompagnent d'effets dans le cyberespace. Si les combats en Ukraine sont principalement conventionnels, l'ANSSI constate l'usage de cyberattaques dans le cadre du conflit. Dans un espace numérique sans frontières, ces cyberattaques peuvent affecter des entités françaises et il convient sans céder à la panique de l'anticiper et de s'y préparer. Aussi, afin de réduire au maximum la probabilité de tels événements et d'en limiter les effets, l'ANSSI partage des bonnes pratiques de sécurité ainsi que des éléments sur la menace et invite l'ensemble des acteurs à s'en saisir.

(ANSSI, March 02, 2022)

Côté russe, alors que le conflit russo-ukrainien en cours continue de s'intensifier, le gouvernement a publié une liste massive contenant 17 576 adresses IP et 166 domaines qui, selon lui, sont à l'origine d'une série d'attaques par déni de service distribué (DDoS) visant son infrastructure nationale.

« Si la zone DNS de votre organisation est desservie par un opérateur de télécommunications étranger, transférez-la dans l'espace d'information de la Fédération de Russie. », recommandation de la NCCCI (Centre National de Coordination des Incidents Informatiques de Russie).

(Lakshmanan, March 03, 2022)

Un serveur **DNS** (**Domain Name Systems**) permet de faire la relation entre un nom d'ordinateur et son adresse IP, prérequis indispensable pour toute connexion sur le réseau Internet.

L'empoisonnement du cache DNS est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse. Une fois que le serveur DNS a été empoisonné, l'information est mise dans un cache, rendant ainsi vulnérables tous les utilisateurs de ce serveur. Ce type d'attaque permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à de l'hameçonnage (dans le cas du DNS, on parle de pharming) ou comme vecteur de virus et autres applications malveillantes.

(Wikipédia, Empoisonnement du cache DNS, 2020)

Contrairement à la croyance populaire, il n'y a plus de nos jours physiquement et uniquement **treize serveurs racine du DNS**, mais plutôt treize « identités de serveur » dont les noms sont de la forme `lettre.root-servers.net` où `lettre` est une lettre comprise entre **A** et **M**. Cependant, ces « identités » (ou serveurs de noms `(en)`) ayant chacune une seule adresse IP assignée, sont communément référées comme étant les « **serveurs racines** ».

Douze organisations contrôlent ces serveurs, deux sont européennes (RIPE NCC et Autonomica, une division de Netnod), une organisation Japonaise (WIDE), les autres étant américaines. Neuf de ces serveurs ne sont pas de simples machines mais correspondent à plusieurs installations réparties dans des lieux géographiques divers, il y avait ainsi au 19 juillet 2019 plus de 997 sites dans 53 pays qui hébergeaient un serveur racine du DNS. En 2007, on comptait 130 sites.

Dans ce contexte, on comprend que les serveurs racines ont une importance stratégique et qu'ils doivent être sécurisées avec un niveau de sécurité très élevé pour lutter contre le DNS poisoning.

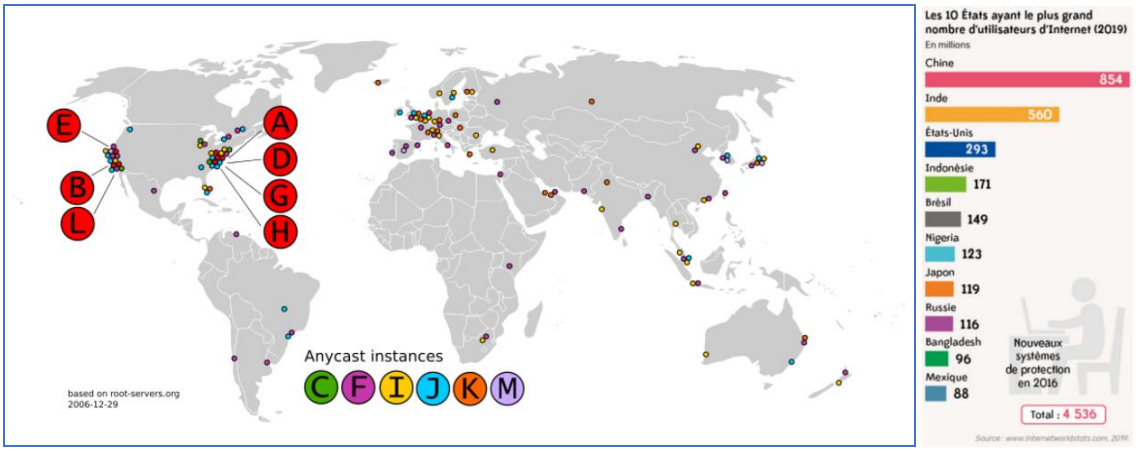

Figure 1 : Localisation des serveurs racines du DNS et nombre d'utilisateurs Internet

(Wikipédia, Les serveurs racine du DNS, 2022) (Cote, Godeau, Janin, & Le Quintrec, 2020)

Le cyberespace, trois enjeux géopolitiques

On peut définir le cyberespace comme un réseau d'interconnexion planétaire des moyens et systèmes de communication, intégrant à la fois les infrastructures physiques — très fortement inscrites dans des territoires, dans la géographie physique, facilement cartographiée — mais aussi l'espace immatériel, plus difficile à appréhender, plus intangible, mais néanmoins hautement stratégique.

Son centre de gravité s'est déplacé depuis quelques années vers le Sud, l'Asie, la Chine et l'Inde.

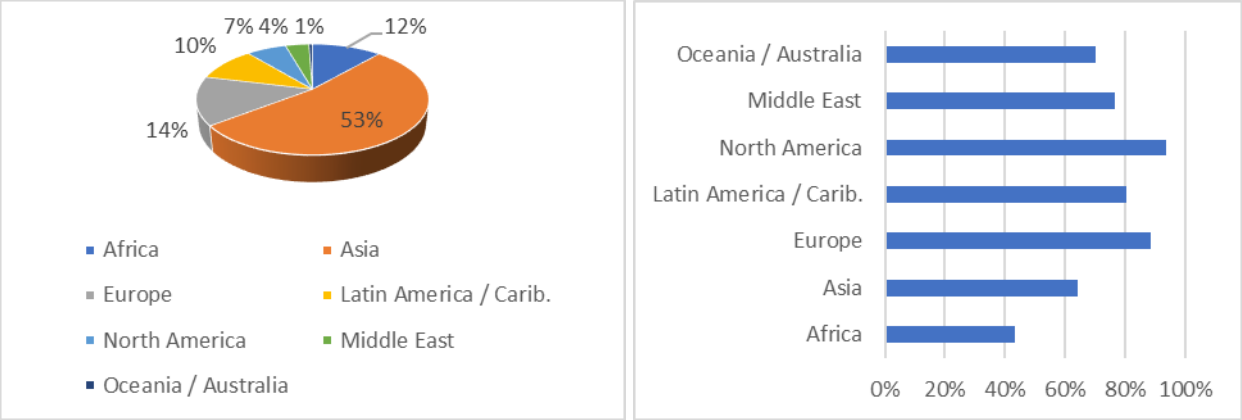

Figure 2 : Taux d'utilisateurs Internet et Taux de pénétration d'Internet par zone géographique (Stats, 2022)

Courbes crées d'après les chiffres recensés sur le site internetworldstats

Le cyberespace est aussi la représentation d'un territoire indépendant, d'un espace de liberté, hors des contraintes du monde réel, conception dominante chez les pionniers de l'Internet, rétifs au contrôle des États. Cette conception imprègne encore beaucoup de militants.

De la même manière, l'idée d'un « cyberespace territoire » est revenue sur le devant de la scène dans les années 2000 *via* les États, pour lesquels il s'agit d'un territoire sur lequel il faut faire respecter les frontières et la souveraineté étatique.

(Douzet, Papaemmanuel, Abdalla, & Coustillière, 2017)

Les Etats-Unis sont partisans d'un Internet libre où **acteurs GAFAM et société civile** ont un rôle à jouer aux côtés des Etats. Au contraire, Chine et Russie défendent la souveraineté des Etats sur les réseaux, ce qui est propice à la censure.

Pour l'instant, le cas russe est très, très loin de ce qu'il se passe en Chine. Le régime de Pékin interdit quasiment tous les sites qui ne sont pas chinois, et les plus importants. Facebook, Instagram et Twitter ne sont pas autorisés dans le pays, mais ce n'est pas tout. Sont interdits

Google (et toute sa suite d'outil, comme Gmail, Maps, Drive, ou encore YouTube), Wikipedia, Snapchat, Reddit, Netflix, Twitch, Spotify, WhatsApp, Messenger… la liste est encore très longue. (Gayte, Mars, 2022)

Le cyberespace est le cadre d'au moins **trois enjeux spécifiques pour la géopolitique.**

Un cyberespace sans frontière

Il contribue d'abord à **brouiller la frontière entre la guerre et la paix**. Beaucoup d'opérations étatiques sont conduites en secret, difficiles à attribuer, et restent sous le radar de la guerre, de ce qui peut être considéré comme une agression armée, compliquant la réponse stratégique et tactique des États.

La première arme de la cyberguerre, c'est l'information ou plutôt, la **désinformation**. Et si tous les grands médias traditionnels (journaux, télés, radios) couvrent le conflit sur place avec des envoyés spéciaux et des correspondants locaux qui partagent leurs observations en temps quasi réel, avec des témoignages, des reportages et des images certifiées, les réseaux sociaux sont exploités pour diffuser des fausses informations et de la **propagande**.

Dans le cadre du conflit entre l'Ukraine et la Russie, le monde des hackers s'est mis en marche, ils prennent parti. De nombreux groupes sont entrés en guerre, certains militent pour les Russes d'autres pour les Ukrainiens, comme le célèbre groupe de hackers Anonymous.

(Le groupe de hackers Anonymous offre 52 000 $ en Bitcoin à tout soldat russe qui se livre avec son char, March 04, 2022)

Plusieurs exemples de telles attaques sont connus.

Le lancement du **malware Stuxnet** contre les centrifugeuses iraniennes de Natanz en 2010 constitue alors une attaque hors limite, expérimentale, que l'on peut voir comme une forme de recherche d'une troisième voie entre diplomatie coercitive et action armée. Les tensions entre les États-Unis et la Chine autour de la distinction entre espionnage stratégique légitime et espionnage économique dérobant des secrets d'affaires sont un autre exemple de ces opérations agressives mais sous le radar de ce qui pourrait déclencher une guerre.

Les opérations menées par les Russes dans le cadre du conflit ukrainien, combinaison de moyens, d'attaques contre des infrastructures critiques et de **désinformation médiatique**. Le piratage du Parti démocrate américain, enfin, relève de la guerre informationnelle, la divulgation d'informations sensibles pouvant être perçue comme une déstabilisation du système électoral américain aux effets stratégiques majeurs. Les États-Unis ont été jetés dans une situation où ils ont dû élaborer soigneusement une réaction appropriée et inédite.

Le **logiciel espion Pegasus**, utilisé par des dizaines d'États à travers le monde, a révélé qu'il était capable de s'infiltrer illégalement sur les smartphones de dizaines de milliers de personnes dont 600 femmes et hommes politiques après enquête. Une arme numérique utilisée contre des journalistes, des avocats, des militants et des responsables politiques de nombreux pays, dont la France.

(Untersinger, « Projet Pegasus » : révélations sur un système mondial d'espionnage de téléphones, July 18, 2021)

Le logiciel **Pegasus** développé par la société Israélienne de sécurité informatique **NSO Group** avait pour objectif initial d'aider les services de renseignement à lutter contre la criminalité et le terrorisme.

Les actions que Pegasus est en mesure de mener au sein d'un appareil infecté n'en sont pas moins spectaculaires. Loin d'être un simple logiciel d'écoute, Pegasus a le pouvoir d'aspirer toutes les données se trouvant dans un appareil : carnet de contacts, photographies, messages, appels… Même les messageries sécurisées, telles que Signal ou encore WhatsApp, ne lui résistent pas.

(Pimenta, July 19, 2021)

Si tous les faits venaient à être avérés, on pourrait alors affirmer qu'il s'agit de l'affaire de cyber-espionnage la plus importante que le monde ait connu depuis les **révélations d'Edward Snowden**, devenu en 2013 le lanceur d'alerte le plus célèbre de la planète. Il a tout risqué pour révéler au monde le projet du gouvernement américain : un programme secret de surveillance capable de s'infiltrer dans la vie privée de chacun. Ses révélations ont inspiré la création du **RGPD** européen (le Règlement général de protection des données).

(Snowden, 2019)

Le prochain grand défi est la cyberdéfense active, sujet mis en avant par les États-Unis : cette expression désigne l'autorisation faite aux acteurs du secteur privé de s'auto-défendre et mener des actions qui pourraient à terme provoquer des conflits entre États.

Les discussions internationales sur le cyberespace portent de plus en plus sur la définition de comportements responsables et de conduites appropriées en temps de paix, que ce soit pour les États ou les compagnies privées.

Un cyberespace de conflictualité et de coopération entre les acteurs

Le cyberespace suppose aussi des **interactions entre de nombreux domaines**. Cet espace est le cadre d'activités transfrontières, supposant des conflits de juridictions et des réseaux partagés entre civils et militaires, États et acteurs privé. On constate un véritable entrelacement des enjeux et des acteurs, une grande diversité de motivations qui se rencontrent pourtant sur un même réseau. Le cyberespace est le lieu d'interactions multiples et complexes entre différents domaines, d'enjeux liés et indissociables. On observe également une grande disparité des moyens parmi les nations, mais aussi entre nations et acteurs privées. Cela provoque à la fois une course aux armements cyber et des tentatives répétées pour établir des règles du jeu afin de limiter l'escalade des conflits et les menaces sur la paix internationale.

L'aide de l'opérateur **Starlink** apportée au gouvernement Ukrainien leur permet de bénéficier d'un service internet haut débit en orbite terrestre basse (LEO) de **SpaceX**, beaucoup plus difficile à bloquer que l'internet conventionnel.

Un internaute sur Twitter l'a bien résumé ainsi : « les Ukrainiens ont désormais accès au système internet par satellite le plus rapide et le plus robuste jamais créé. Cela rend impossible pour la Russie de désactiver entièrement l'accès à l'internet ukrainien sans cyberattaque des centres de données étrangers ».

Un cyberespace avec l'émergence de nouvelles puissances cyber

Enfin, le cyberespace est le lieu de l'**émergence de nouvelles puissances cyber**. La question de l'émergence des plateformes d'intermédiation (telles que **Google**, **Amazon**, **Facebook**, plus récemment **Uber** ou **Airbnb**, mais aussi **Baidu**, etc.) est aujourd'hui capitale. De plus en plus de décisions vont être basées sur des bases de données et des algorithmes, ce qui pose des questions sur la souveraineté des États. Ces plateformes opèrent à travers les frontières et collectent et contrôlent des masses de données énormes mais leur distribution n'est pas uniforme, ce qui peut générer des déséquilibres importants. Les États doivent, pour accéder à certaines données, négocier directement avec ces plateformes. On mesure mal leur géographie et il n'existe pas encore de cadre conceptuel pour comprendre leur influence sur le jeu géopolitique.

En Europe, nos données partent massivement sur des plateformes américaines (problématique pour l'Europe occidentale). Ces données sont captées par des acteurs privés sans que l'on sache qui les contrôle, qui les utilise, qui les collecte, sans non plus qu'on détermine ce qu'est une donnée stratégique. Or cette définition de la donnée stratégique est un enjeu majeur parce que c'est un enjeu de souveraineté. Pouvoir collecter, comprendre et contrôler les données ferait notre autonomie stratégique.

Les enjeux géopolitiques du cyberespace sont énormes et conditionneront la construction du monde de demain, la construction d'une nouvelle sécurité collective, la stabilité du cyberespace et de son futur, le futur aussi de la démocratie et des libertés individuelles, à l'heure où les algorithmes peuvent modifier le rapport à la vérité et donc à la démocratie.

(Douzet, Papaemmanuel, Abdalla, & Coustillière, 2017)

La cyberguerre, impacts sur des infrastructures critiques et des opérateurs d'importance vitale

Une cyberattaque peut entraîner des problèmes de sécurité d'ordre publique mais aussi de graves perturbations sur les infrastructures critiques d'un pays ou d'une entreprise.

Infrastructures numériques

- **Réseaux satellites**

En Ukraine et dans d'autres pays, le géant de l'Internet satellitaire Viasat indique avoir subi une panne après une cyberattaque impactant ses services internet.

(Les services de l'opérateur satellitaire Viasat en Ukraine freinés par une cyberattaque, March 02, 2022)

Les opérateurs satellitaires se mobilisent actuellement pour venir en aide à l'Ukraine, envahie par son voisin russe depuis la semaine dernière, à l'image de SpaceX. Appelé à la rescousse par Mykhailo Fedorov, vice-premier ministre et ministre de la Transformation numérique de l'Ukraine, le patron du géant spatial Elon Musk indique via Twitter avoir fait parvenir des antennes de son service d'internet satellitaire Starlink sur le sol ukrainien.

(Vaughan-Nichols, Les services de l'opérateur satellitaire Viasat en Ukraine freinés par une cyberattaque, February 22, 2022)

En France et en Europe, des milliers d'internautes ont été privés d'Internet du fait d'une probable cyberattaque sur un réseau satellitaire, survenue au début de l'offensive russe en Ukraine, selon des sources concordantes.

Selon Orange, « près de 9 000 abonnés » d'un service Internet par satellite de sa filiale Nordnet, en France, étaient privés vendredi soir d'internet à la suite d'un « cyber-événement » survenu le 24 février 2022 au sein de Viasat, un opérateur de satellite américain dont il est le client.

(Des milliers d'internautes en France et en Europe sans Internet à la suite d'une probable cyber-attaque, March 05, 2022)

- **Réseaux 5G**

Les réseaux 5G allient encore plus de technologies différentes que les réseaux 4G, ce qui entraîne une complexité de réseau rarement égalée, et donc une sécurité bien difficile à assurer pour les opérateurs comme pour les clients.

(Langlois, June 2021)

L'administration américaine, qui a fait part de ses vives inquiétudes sur les risques potentiels d'espionnage lors des déploiements d'infrastructures 5G.

(Chol & Fontaine, 2019)

Un monde basé sur la 5G sera plus interconnecté car les données seront partagées entre les appareils et entre les applications. Il **augmentera considérablement la surface des attaques**, en multipliant les points où les hackers peuvent entrer dans le réseau.

(Bousquet, January, 2020)

- **Réseaux câbles sous-marins**

L'administration américaine émet les mêmes mises en garde concernant les réseaux sous-marins, par lesquels transitent aujourd'hui 95% du trafic de voix et de données au niveau planétaire. Washington considère, à juste titre, ces câbles comme une partie importante de ses infrastructures vitales, essentielles au bon fonctionnement de l'économie mondiale. Ces câbles sont vulnérables car peu protégés.

- (Chol & Fontaine, 2019)

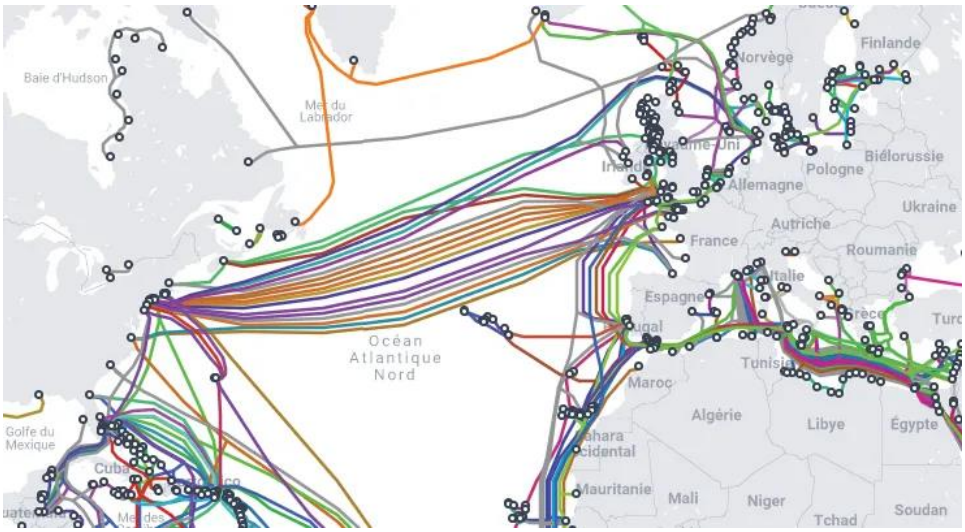

Figure 3 : Réseaux de câbles sous-marins

Le navire de recherche océanographique Yantar est l'une des armes russes les plus dangereuses contre les infrastructures numériques. Ce navire espion russe est spécialisé dans l'attaque des fibres optiques sous-marines. Il est équipé de deux sous-marins capables de couper des câbles

optiques sous-marins, de déposer des mouchards pour lire les contenus qui y circulent, et d'enlever des mouchards posés par d'autres pays.

(Manaranche, May 27, 2020)

Depuis plusieurs années, les géants américains de l'Internet (GAFAM) sont responsables de plus de la moitié des déploiements au niveau mondial. Ils ont ainsi financé une quinzaine de lignes de câbles sous-marins entre les Amériques, l'Europe et l'Asie.

(Chol & Fontaine, 2019)

- **Data Centers**

À l'ère du numérique et avec l'explosion du Big Data, les centres de données sont devenus des infrastructures indispensables et représentent des enjeux stratégiques pour les États. D'après le recensement de la plateforme Cloudscene, sur plus de 8 100 centres de données répertoriés dans le monde au mois d'octobre 2021, environ le tiers sont installés aux Etats-Unis (2 705).

Comme le montre le graphique ci-dessous, les Etats-Unis dominent ainsi très largement le classement mondial des pays les mieux équipés en la matière, devant l'Allemagne (466), le Royaume-Uni (449) et la Chine (415).

Avec 247 centres de données recensées sur son territoire, **la France se classe quant à elle au 8ème rang mondial**, derrière l'Australie (270) et devant le Japon (205).

Ensemble, les huit pays de cette liste hébergent environ 63 % des data centers de la planète.

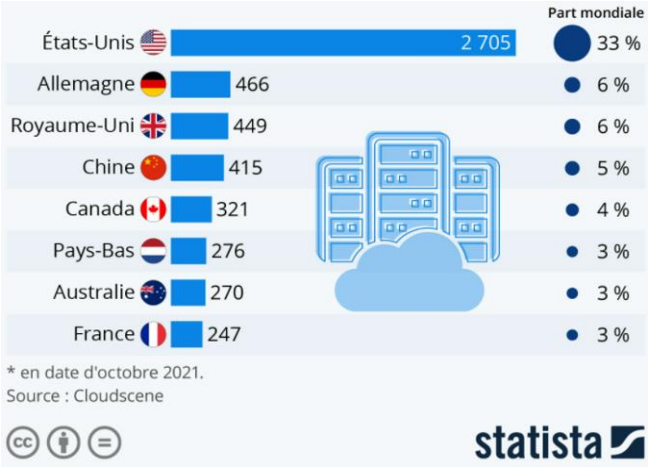

Figure 4 : Nombre de Data Centers recensés dans le monde (Gaudiaut, October 18, 2021)

Si cette statistique donne un bon aperçu de la répartition de ce type d'infrastructures à travers le monde, il faut toutefois garder en tête qu'elle ne renseigne pas sur la taille des data centers, certains pouvant avoir des capacités de stockage beaucoup plus élevées que d'autres.

Infrastructures de la vie courante

- **Réseaux d'eau**

Les infrastructures de l'eau, barrages hydrauliques, systèmes d'irrigation, réseaux urbains, usines de potabilisation ou de traitement des eaux usées, fonctionnent de plus en plus sur la base de systèmes informatiques sophistiqués, ce qui les rend potentiellement vulnérables à des « cyberattaques ». En outre, on observe une tendance récente au sein des entreprises de l'eau, pour des raisons d'économies et de réduction des coûts, à connecter leurs systèmes opérationnels à l'internet, pour pouvoir effectuer une partie des opérations de contrôle et de maintenance à distance. Mais l'utilisation accrue de ces systèmes à distance a pour effet d'ouvrir davantage les systèmes opérationnels des réseaux ou des usines à des intrusions extérieures, particulièrement si les mesures de sécurité nécessaires – firewalls, cryptage, mots de passe sécurisés… – ne sont pas en place. Dans la plupart des cas, en raison des faibles barrières de sécurité entre les systèmes, il suffit d'une défaillance humaine anodine – comme le fait pour un employé d'ouvrir une pièce jointe infectée dans son logiciel de courrier électronique – pour ouvrir une brèche dans tout le système.

(La cybersécurité concerne-t-elle les réseaux d'eau ?, September 7, 2021)

(Petitjean, June 30, 2016)

- **Réseaux d'électricité**

Rappelons qu'avant même que la Russie ne lance son opération militaire, elle avait déjà attaqué l'Internet ukrainien. Bien avant que les chars ne commencent à entrer en Ukraine, la Russie avait en effet injecté des logiciels malveillants et lancé des attaques par déni de service sur de nombreux sites web ukrainiens. Des années auparavant, la Russie était parvenue à couper l'électricité à Kiev, la capitale de l'Ukraine.

(Vaughan-Nichols, Les services de l'opérateur satellitaire Viasat en Ukraine freinés par une cyberattaque, February 22, 2022)

« Les Russes avaient *été capables d'attaquer l'Ukraine et de couper l'électricité pendant plusieurs jours à Kiev en 2015-16*", rappelle Gérôme Billois, expert en cybersécurité chez Wavestone, au micro de TF1. ». (Diwo & Mariel)

- **Parcs éoliens**

Depuis jeudi 24 février 2022, une succession de cyberattaques cible des infrastructures du pays envahi, mais aussi d'autres États européens. Ces derniers jours, 5800 éoliennes ont ainsi été touchées par ces agressions d'un genre nouveau. Selon le fabricant, l'origine du dysfonctionnement ne fait que très peu de doutes. "Les services de communications ont été interrompus presque exactement au même moment que l'invasion russe en Ukraine", dénonce Enercon dans un communiqué, faisant clairement de Moscou le coupable. *(Mariel, March 02, 2022)*

- **Centrales nucléaires**

« Les risques de cyber-attaques contre les centrales nucléaires se multiplient », titrait Le Monde déjà en 2015. Ces risques augmentent avec la numérisation croissante de l'industrie nucléaire qui offre de nouvelles portes d'entrée aux attaquants. Hacktivistes, services secrets, mafieux ou terroristes tentent de voler des informations, de monnayer leurs intrusions dans le système d'information d'une centrale ou d'exercer un chantage pouvant toucher des franges entières de la population.

Le manque de maturité dans la chaîne cyber peut toucher à la catastrophe. C'est ce qui est arrivé au Korea Hydro and Nuclear Power (KHNP), récemment victime d'une cyber-attaque. Les données personnelles de près de 11 000 employés et des plans de réacteurs et de leurs circuits de refroidissement ont partiellement été diffusés par les pirates sur des portails sud-coréens et sur Twitter. Les pirates ont ensuite menacé de divulguer d'autres informations si les réacteurs de deux centrales coréennes n'étaient pas arrêtés. A mettre en perspective avec les récentes attaques contre l'Ukraine…

(Guezo, 2021)

Le département principal du renseignement du ministère de la Défense de l'Ukraine (GURMO) a piraté et divulgué des documents qu'il prétendait avoir volés à la centrale nucléaire russe de Beloyarsk cette semaine. En somme, l'Ukraine divulgue la propriété intellectuelle russe comme acte de guerre.

(Uchill, March 10, 2022)

Comment la France peut assurer sa souveraineté dans le cyberespace ?

Commandement de la cyberdéfense

En 2007, l'Estonie subit une attaque cyber d'une ampleur inégalée, initiées par des hackeurs russes, sûrement soutenus par l'appareil d'État russe. À partir de cette attaque, les nations modifient leurs structures. En France, le Livre blanc de 2008 marque la volonté de changer la sécurité du numérique pour en faire un enjeu national. **En 2009, l'A.N.S.S.I. est créée, avec un effectif de 100 personnes, contre 675 d'ici fin 2022**. Rattachée au Premier ministre, elle n'est pas en concurrence avec la Défense puisqu'elle se situe au-dessus des militaires. En 2011 s'amorce la structuration de l'organisation militaire numérique, avec les premières opérations menées au niveau numérique et la création de l'Officier général à la Cyberdéfense.

Le Livre blanc de 2013 affiche l'ambition de la France dans ce secteur, puisque 17 pages sont consacrées à la cyberdéfense. Au sein du ministère de la Défense, un plan stratégique est mis en place, structurant la démarche des armées, accompagnant la création d'un pôle d'excellence et les efforts de formation et de rapprochement avec l'industrie.

En 2017, un grand commandement de la cyberdéfense (COMCYBER) est créé, il est composé, de l'ensemble des forces de cyberdéfense des armées, directions et services, sur lesquels il exerce une tutelle organique ou fonctionnelle.

(Douzet, Papaemmanuel, Abdalla, & Coustillière, 2017)

Un nouveau Livre Blanc avec 28 recommandations de la Présidence Française du Conseil de l'Union Européenne a été publié en septembre 2021, il constitue la boussole stratégique de l'Union.

« Dans l'Europe numérique de demain, la cybersécurité doit être à la fois une clé de voûte et un fer de lance. Une clé de voûte pour assurer la résilience collective dans le contexte de transformation numérique. Un fer de lance pour défendre et valoriser les intérêts européens, dans un monde marqué par le « retour des puissances » et par des stratégies globales dans lesquelles le cyberespace occupe une place grandissante. Si la puissance ne peut pas être uniquement numérique, il ne peut y avoir de puissance sans numérique. »

(ANSSI, LA CYBERSÉCURITÉ AU CŒUR DU NOUVEAU LIVRE BLANC SUR LA DÉFENSE ET LA SÉCURITÉ NATIONALE, September, 2021)

Mesures préventives prioritaires recommandées par l'ANSSI

Face à d'éventuels effets dans le cyberespace liés au conflit en cours entre l'Ukraine et la Russie, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) préconise la mise en œuvre de 5 mesures préventives prioritaires :

1. Renforcer l'authentification sur les systèmes d'information ;
2. Accroître la supervision de sécurité ;
3. Sauvegarder hors-ligne les données et les applications critiques ;
4. Etablir une liste priorisée des services numériques critiques de l'entité ;
5. S'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque.

Ces mesures prioritaires de cybersécurité sont essentielles et leur mise en œuvre à court terme permet de limiter la probabilité d'une cyberattaque ainsi que ses potentiels effets. Pour être pleinement efficaces, elles doivent cependant s'inscrire dans une démarche de cybersécurité globale et de long terme.

(ANSSI, MESURES CYBER PREVENTIVES PRIORITAIRES, February 26, 2022)

Dans un contexte de tensions internationales, l'ANSSI a publié son panorama des menaces informatiques en 2021. Pas de répit pour les cyberattaques qui progressent de 37% sur un an. L'agence alerte aussi sur la montée en puissance des campagnes d'espionnage et de sabotage.

(Cheminat, March 09, 2022)

Campus Cyber, lieu de rencontre des acteurs nationaux et internationaux

Ce projet de **Campus Cyber** a été initié par le Président de la République, c'est un lieu totem de la cybersécurité (Centre névralgique) qui rassemble les principaux acteurs nationaux et internationaux du domaine. Ce Campus a été inauguré en février 2022, il est basé Tour Eria à la Défense. Il permet en particulier d'accueillir sur un même site des entreprises (grands groupes, PME), des services de l'État, des organismes de la formation, des centres de recherche et des associations, soit au total 160 acteurs engagés. Ce Campus doit favoriser les échanges entre les industriels et les centres de recherche, servir de centre de formation et de centre événementiels Cyber, afin de renforcer et de maîtriser toutes les technologies de cybersécurité et de contribuer au développement de licornes françaises. *(Van Den Berghe, February 2022)*

Créé en 2014 par le ministère de la Défense et la Région Bretagne, le **Pôle d'excellence cyber** est une association qui fédère au niveau national des acteurs de la recherche, de la formation et de l'industrie pour contribuer à développer la filière cyber française et la promouvoir à l'international.

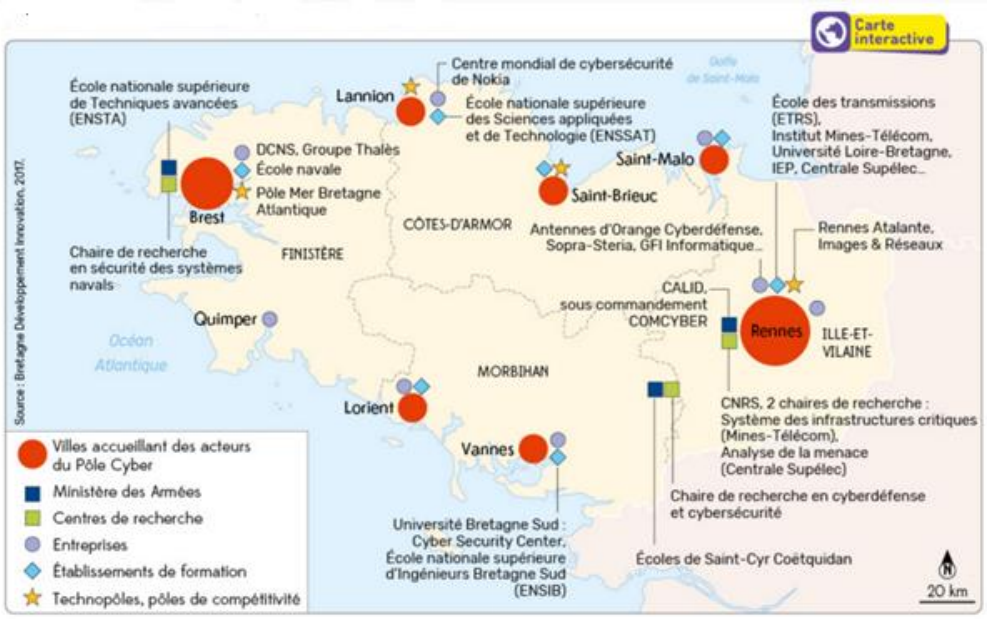

Figure 5 : Le pôle d'excellence Cyber en Bretagne (Cote, Godeau, Janin, & Le Quintrec, 2020)

Les profils de la cybersécurité en France

La cybersécurité est une filière d'avenir. Les entreprises du secteur emploient déjà en France 24.000 salariés et prévoient dans les trois ans de créer 1.400 postes (+ 6 %).

(Gless, October 11, 2018)

L'île de France, la Bretagne ainsi que la région Midi-Pyrénées présentent leur intérêt en matière de cybersécurité, les autres manquent encore de maturité, les besoins sont omniprésents.

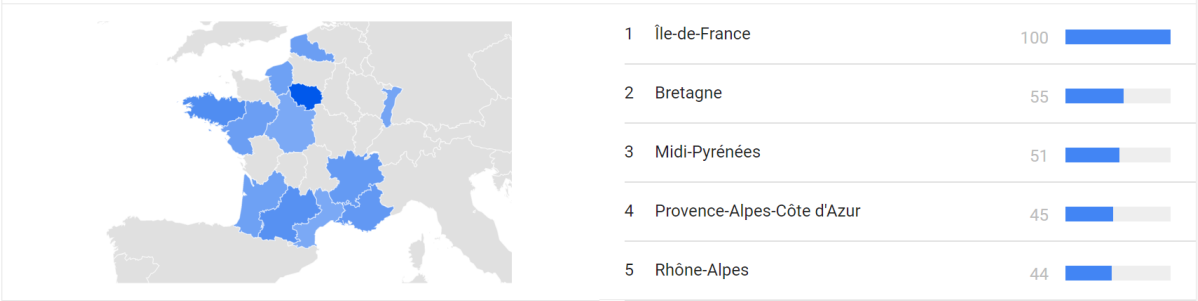

*Figure 6 : Source Google Trends sur les métiers RSSI**

*RSSI : Responsable en Sécurité des Systèmes d'Informations

Les données ci-dessous sont issues d'une analyse menée sur la base de 15 665 offres d'emploi en cybersécurité réparties sur toute la France en 2019 et d'une enquête en ligne à laquelle 2 381 professionnels de la cybersécurité ont répondu.

Les 5 principaux secteurs d'activités du métier RSSI représentent 49% des offres.

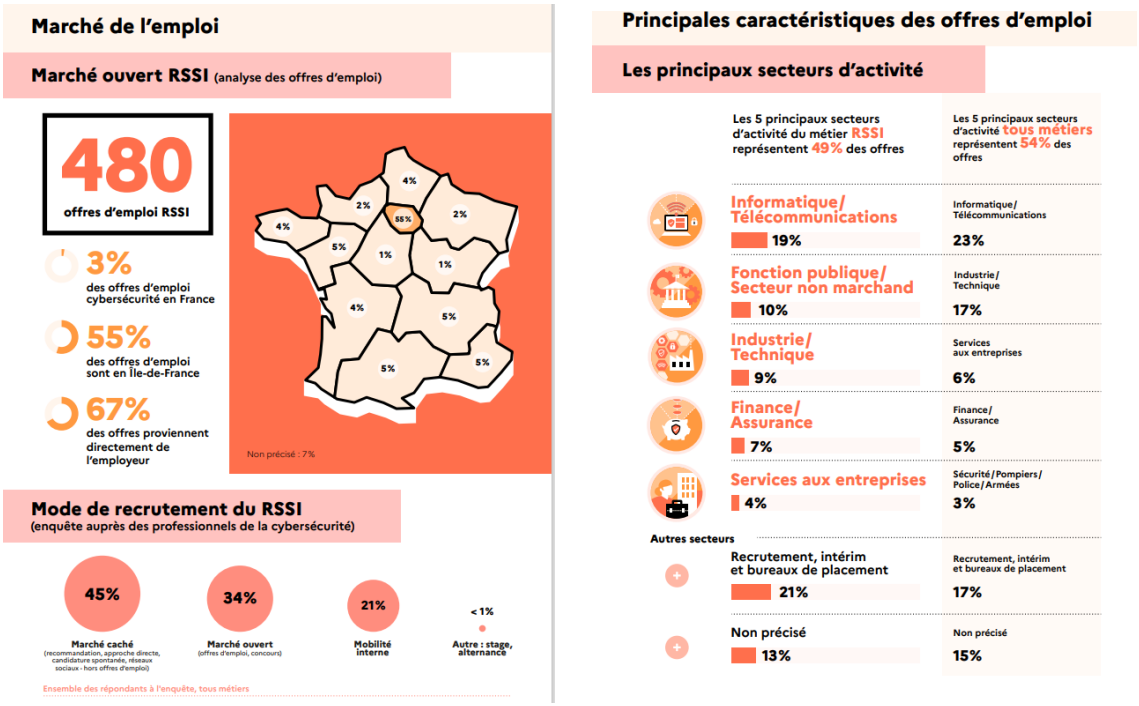

Figure 7 : Source ANSSI 2021 : Panorama des métiers de la cybersécurité

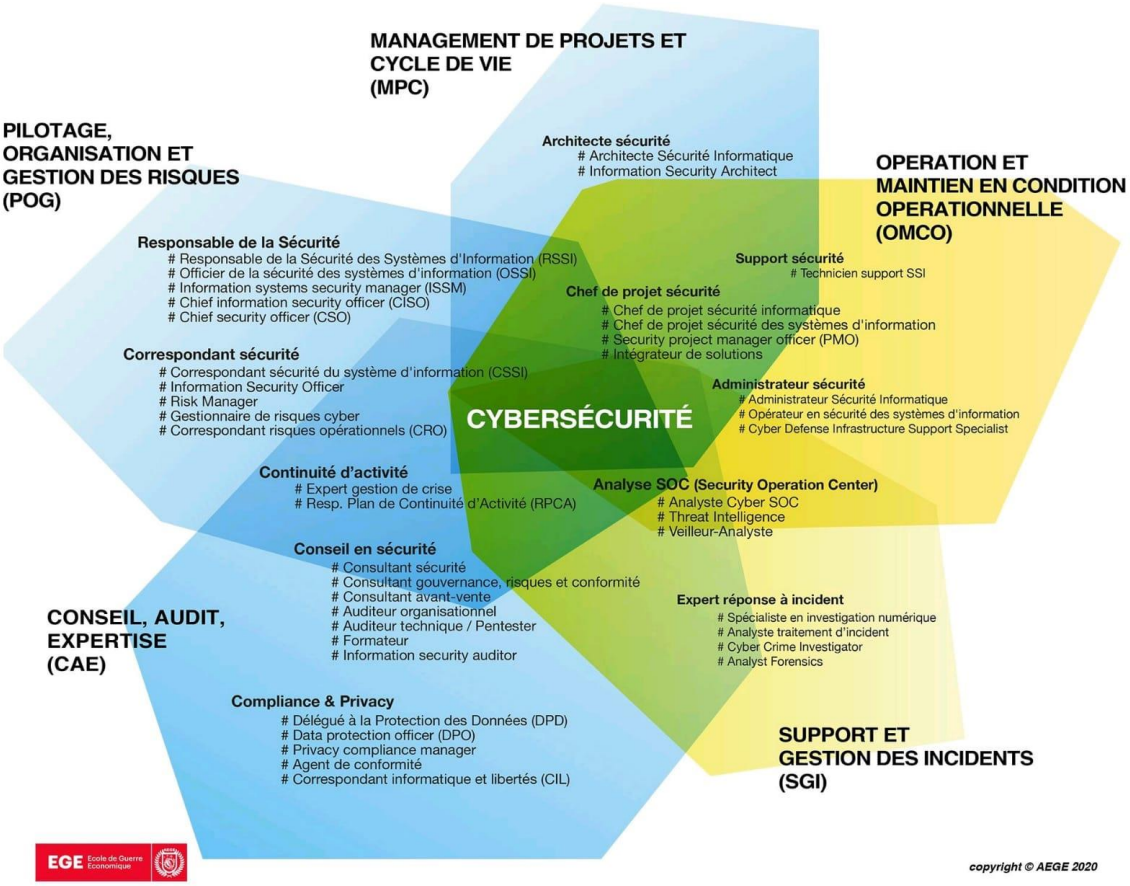

Figure 8 : Source EGE 2020 : Cartographie des métiers de la cybersécurité en 2020

Les zones bleues se rapportent à des familles de métiers Cyber typés management, alors que celles figurant en jaune sont plus orientés ingénierie et technique.

Conclusion

La cyberguerre s'appuie sur des cyberattaques comme moyens de propagande, de censure, de désinformation et d'espionnage, capables à l'extrême de paralyser les activités vitales d'un pays.

La cyberguerre n'est pas seulement une guerre virtuelle, les actes de cyberguerre peuvent impacter physiquement un pays.

Le cyberespace défie les frontières terrestres des États, cadres privilégiés du droit. Il s'appuie sur un réseau maillé qui permet aux Etats d'étendre leur territoire et leur souveraineté.

Dans un cyberespace sans frontière, le manque de maturité dans la chaîne cyber pourrait entraîner des catastrophes. Un groupe de hackers qui divulgue par exemple la propriété intellectuelle nucléaire d'un pays, comme acte de guerre, pourrait avoir des conséquences désastreuses et mettre en péril l'humanité.

En Europe, nos données partent massivement sur des plateformes américaines. Il est temps pour les Européens de rapatrier ces données, c'est un enjeu stratégique pour assurer leur souveraineté.

Le cyberespace oblige ainsi à repenser les normes internationales et la sécurité collective, avec la protection des libertés individuelles pour assurer l'avenir de la démocratie. Il nécessite un fort investissement dans la recherche et une collaboration entre chercheurs et industriels à l'heure où les algorithmes de chiffrement les plus avancés pourraient être cassés par l'ordinateur quantique.

Dans un monde où la croissance du volume des données devient exponentielle, le prochain défi pour les RSSI est d'adopter une cyberdéfense active, donc d'anticiper afin de réagir à tout moment de façon coordonnée et automatisée aux cyberattaques.

La cyberdéfense active passe par une attitude proactive facilitée suivant plusieurs approches, notamment :

- Mettre en œuvre les mesures préventives prioritaires rappelées par l'ANSSI,
- Faire de la veille intégrant les **activités dark web** afin de prendre connaissance de l'émergence de nouvelles menaces,
- Utiliser l'**I**ntelligence **A**rtificielle (**IA**, de type machine learning ou deep learning) permettant de traiter d'énormes volumes de données afin de faire une analyse comportementale des incidents.

L'IA devient un enjeu stratégique majeur pour la sécurité de nos Systèmes d'Information, elle ne remplacera pas l'humain mais devrait permettre aux analystes sécurité de répondre aux attaques en quasi-temps réel.

Bibliographie

ANSSI. (February 26, 2022). *MESURES CYBER PREVENTIVES PRIORITAIRES.*

ANSSI. (March 02, 2022). *Tensions internationales - Menaces cyber.* Paris.

ANSSI. (September, 2021). *LA CYBERSÉCURITÉ AU CŒUR DU NOUVEAU LIVRE BLANC SUR LA DÉFENSE ET LA SÉCURITÉ NATIONALE.*

Bousquet, R. (January, 2020). La 5G et la cybersécurité. *Globb Security.fr*.

Cheminat, J. (March 09, 2022). Ransomware, espionnage : l'Anssi dresse un bilan sombre des menaces IT en 2021. *Le Monde Informatique*.

Chol, E., & Fontaine, G. (2019). *Il est midi à Pékin.* fayard.

Cote, S., Godeau, E., Janin, E., & Le Quintrec, G. (2020). *Histoire-Géographie, Géopolitique, Sciences Politiques (HGGSP) Terminale.* Nathan.

Des milliers d'internautes en France et en Europe sans Internet à la suite d'une probable cyber-attaque. (March 05, 2022). *Le Parisien*.

Diwo, C., & Mariel, N. (s.d.). *Reportage TF1 Charles Diwo et Nathalie Mariel.*

Douzet, F., Papaemmanuel, A., Abdalla, M., & Coustillière, A. (2017). Du cyber au géopolitique. *Résumé de la conférence organisée le 4 avril 2017 en Sorbonne par Les Mardis de l'Innovation, Panthéon-Sorbonne Défense Sécurité & Citoyenneté et l'association ProECA Sorbonne.* Paris.

Gaudiaut, T. (October 18, 2021). *Les pays qui hébergent le plus de data centers.*

Gless, É. (October 11, 2018). Cybersécurité : profils experts recherchés. *L'étudiant*.

Guezo, L. (2021). *Cybersécurité du nucléaire? Où en est-on?*

(September 7, 2021). *La cybersécurité concerne-t-elle les réseaux d'eau ?*

Lakshmanan, R. (March 03, 2022). Russia Releases List of IPs, Domains Attacking Its Infrastructure with DDoS Attacks. *The Hacker News*.

Langlois, P. (June 2021). Sécurité des infrastructures 5G. *MISC - Magazine de la cybersécurité offensive et défensive*.

Le groupe de hackers Anonymous offre 52 000 $ en Bitcoin à tout soldat russe qui se livre avec son char. (March 04, 2022). *Cryptonaute*.

Les services de l'opérateur satellitaire Viasat en Ukraine freinés par une cyberattaque. (March 02, 2022). *ZDNet*.

Manaranche, M. (May 27, 2020). Yantar Shipyard Services "Oceanographic Research Vessel" Yantar. *Navalnews*.

Mariel, C. D. (March 02, 2022). VIDÉO - Les éoliennes de France menacées par les cyberattaques ?

Petitjean, O. (June 30, 2016). *L'eau, nouvelle frontière de la cybersécurité ?*

Pimenta, J. (July 19, 2021). Projet Pegasus : 3 points clés pour tout comprendre de cette massive affaire de cyber-espionnage. *SiecleDigital*.

Snowden, E. (2019). *Permanent Record.* New York: Metropolitan Books.

Stats, I. W. (2022). *Usage and Population Statistics - 2022 Year-Q1 Estimates.*

Uchill, J. (March 10, 2022). In a first, Ukraine leaks Russian intellectual property as act of war. *SC MEDIA*.

Untersinger, D. L. (July 18, 2021). « Projet Pegasus » : révélations sur un système mondial d'espionnage de téléphones. *Le Monde*.

Van Den Berghe, M. (February 2022). *UN CAMPUS DÉDIÉ À LA CYBERSÉCURITÉ.*

Vaughan-Nichols, S. (February 22, 2022). Les services de l'opérateur satellitaire Viasat en Ukraine freinés par une cyberattaque. *ZDNet*.

Vaughan-Nichols, S. (February 22, 2022). Ukraine : Elon Musk active Starlink pour aider à maintenir l'internet. *ZDNet*.

Wikipédia. (2020). *Empoisonnement du cache DNS.*

Wikipédia. (2022). *Les serveurs racine du DNS.*

Glossaire

Adresse IP : Une adresse IP (Internet Protocol) est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol.

ANSSI : L'Agence nationale de la sécurité des systèmes d'information est un service français créé par décret en juillet 2009. Ce service à compétence nationale est rattaché au secrétariat général de la Défense et de la Sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. L'ANSSI remplace la Direction centrale de la sécurité des systèmes d'information, créée par décret en juillet 2001.

Big Data : Le big data désigne les ressources d'informations dont les caractéristiques en termes de volume, de vélocité et de variété imposent l'utilisation de technologies et de méthodes analytiques particulières pour créer de la valeur, et qui dépassent en général les capacités d'une seule et unique machine et nécessitent des traitements parallélisés.

DDoS : Attaque par déni de service qui désignent toutes les actions ayant pour résultat la mise hors ligne d'un serveur.

DNS : Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaines Internet en adresse IP ou autres enregistrements.

GAFAM est l'acronyme des géants du Web — Google, Apple, Facebook, Amazon et Microsoft — qui sont les cinq grandes firmes américaines (fondées entre le dernier quart du XXe siècle et le début du XXIe siècle) qui dominent le marché du numérique, parfois également nommées les Big Five, ou encore « The Five ».

RIPE NCC : Le RIPE (Réseaux IP Européens - Network Coordination Centre) est un registre régional d'adresses IP. Il dessert l'Europe et une partie de l'Asie, notamment au Moyen-Orient. C'est une organisation à but non lucratif de droit néerlandais et son siège est à Amsterdam.

RGPD : Le règlement général sur la protection des données (ou encore **GDPR**, de l'anglais General Data Protection Regulation), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

RSSI : Le responsable de la sécurité des systèmes d'information (en anglais, Chief Information Security Officer ou CISO) d'une organisation (entreprise, association ou institution) est l'expert qui garantit la sécurité du système d'information et assure la disponibilité, l'intégrité et la confidentialité des données.