EGE Ecole de Guerre Economique

Militarisation de l'internet

Enjeux de la maitrise du cyberespace et de sa sécurisation pour les puissances

Karima DJOUADI
Marine LE DU
Adriano MISTRETTA
Georges SUMA
Biram TOURE

MACYB03 - Juin 2023

SOMMAIRE

ACRONYMES

- ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.
- APT : Advanced Persistent Threat.
- ARCOM : Autorité de Régulation de la Communication Audiovisuelle et Numérique.
- ARPA : Advanced Research Projects Agency.
- ARPANET : Advanced Research Projects Agency Network.
- ASAT : missile anti-satellite.
- BGP : Border Gateway Control.
- BRICS : Brésil, Russie, Chine, Inde, Afrique du sud.
- C2PO : Centre Cyber de Préparation Opérationnelle.
- CALID : Centre d'Analyse en Lutte Informatique Défensive.
- CASSI : Centre d'Audits de la Sécurité des Systèmes d'Information.
- CCDCOE : Cooperative Cyber Defense (Centre d'Excellence de l'OTAN).
- CERN : Conseil Européen pour la Recherche Nucléaire.
- CHPI : Centre des Homologations Principales Interarmées.
- CISA : Cybersecurity and Infrastructure Security Agency.
- CNDUM : convention des nations unies sur le droit à la mer.
- CSA : Cyber Security Agency.
- CSIRT : computer security incident response team.
- DARPA : Defense Advanced Research Projects Agency.
- DCSSI : Direction Centrale de la Sécurité des Services d'Information.
- DGSE : Direction Générale de la Sécurité Extérieure.
- DNS : domain name system.
- ETI : entreprise de taille intermédiaire.
- ETSI : institut européen des normes de télécommunications.
- FBI : Federal Bureau of Investigation.
- FCC : commission fédérale des communications.
- FSB : service fédéral de sécurité de la fédération de Russie.
- FTP : fil transfert protocol.
- GAFAM : Google, Apple, Facebook (Meta), Amazon et Microsoft.
- GCA : groupement de la cyberdéfense des armées.
- GEO : orbite terrestre geostationnaire.
- GRU : direction générale du renseignement.
- ICANN : Internet Corporation for Assigned Names and Numbers.
- INSEE : Institut National de la Statistique et des Etudes Economiques.
- IOT : internet of things.
- ISO : international organization for standardization.
- IUT : Union Internationale de Télécommunication.
- IXP : internet exchange point.
- L2I : lutte informatique d'influence.
- LEO : orbite terrestre basse.
- LID : lutte informatique défensive.
- LIO : lutte informatique offensive.
- LPM : loi de programmation militaire.
- M2M : machine to machine.
- MEO : orbite terrestre moyenne.
- MIE : mécanisme pour l'interconnexion en Europe.
- MIIT : ministère de l'Industrie, de l'Information et de la Technologie.
- NIS : network and information security.
- NIST : Ntional Institute of Standards and Technology.
- NSA : National Sécurity Agency.
- NSF : National Science Fondation.

- OIV : opérateur d'importance vitale.
- ONU : Organisation des Nations Unies.
- OSE : opérateurs de services essentiels.
- OTAN : Organisation du Traité de l'Atlantique Nord.
- PDIS : prestataire de détection d'incident de sécurité.
- PME : Petites et Moyennes Entreprises.
- PPC : posture permanente de cyberdéfense.
- PRISM : planning tool for resource, integration, synchronization and management.
- RGPD : règlement général sur la protection des données.
- RSSI : responsable de la sécurité des systèmes d'information ;
- SGDSN : Secrétariat Général de la Sécurité et de la Défense Nationale.
- SIGINT : signals intelligence.
- SOC : security operation center.
- SOC : security operations center.
- SWIFT : society for worldwide interbank financial telecommunications .
- TCP : transport control protocol.
- WWW : world wide web.
- RPC : République Populaire de Chine.
- BITC : base industrielle et technologique de cybersécurité.
- B2C : business to customer.
- B2B : business to business.
- B2G : business to government.
- GCHQ : Government Communications Headquarters.
- MDMC : multi domain multi champ.
- AS : systèmes autonomes.
- COMCYBER : Commandement de la Cyberdéfense.
- ONG : organisation non gouvernementale.
- OSINT : open-source intelligence.
- ML : machine learning.
- OMC : Organisation Mondiale du Commerce.

INTRODUCTION

« Une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts mathématiques... Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain ».

C'est ainsi que l'écrivain américain William Gibson a défini le terme cyberespace dans son roman de science-fiction Neuromancien, publié en 1984. La définition est imagée et littéraire, toutefois quarante ans plus tard le cyberespace ne relève plus de la science-fiction.

Les deux dernières décennies ont vu ainsi le monde changer avec comme bouleversement un développement accéléré des nouvelles technologies de l'information et de la communication *(NTIC).* L'expression "Autoroute de l'information" popularisée par le politicien Albert Gore dans les années 90 présageait le champ illimité du rôle joué par internet dans notre "société de l'information".

Cette sphère mondiale de diffusion des données qu'est le cyberespace révolutionna ainsi la notion d'échanges transnationaux. Début 2023, parmi les 8,1 milliards de personnes présentes sur Terre selon les Nations Unies, 5,1 milliards sont présentes sur internet, soit 64,4% de la population mondiale qui est interconnectée sur internet [1].

Nous, internautes, sommes devenus désormais des êtres cyber, prolongement d'un nombre considérable de flux de données. Notre ordinateur, nos téléphones, notre voiture connectée, nos montres, nos cartes de paiements et toutes sortes d'objets communiquent et communiqueront de plus en plus entre eux, sans même en avoir conscience.

D'un objet d'imagination nous sommes passés à une réalité, parfois difficile à appréhender tant les contours peuvent en être flous, omniprésente dans la société.

L'espace numérique s'est révélé un formidable moyen d'expansion commerciale, d'échanges d'information et de communication. De manière concomitante, cette mutation a conféré une direction stratégique à la protection des réseaux et des systèmes d'information. Les interconnexions et les interdépendances *(réseaux physiques etc.)* sont multiples sans être toujours comprises et maîtrisées.

L'une des anomalies de la richesse de cette société d'information et d'innovations technologiques est de générer des vulnérabilités au sein même de ses propres systèmes d'information. Le champ des opportunités mais aussi des risques liés à Internet ne cesse de s'étendre, comme en témoigne les actes de malveillances sur cet espace. En mentionnant le cyberespace à la fin des années 2010, on faisait référence à cette informatique en réseau, objet d'innovation et permettant de déceler des caractéristiques stratégiques pour les économies. Un basculement s'est opéré au cours de la décennie 2010.

Si on craignait le peu de prise de conscience des menaces dans le cyberespace, à date, on constate que celle-ci a eu lieu.

Au fil des années, on a oublié la notion de cyberespace pour passer à celles de cyberdéfense et de cybersécurité que recouvre aujourd'hui les organismes de sécurité et de défense en y ajoutant le préfixe cyber. On évoque surtout la conflictualité associée au cyberespace [2].

Selon le ministère de l'enseignement supérieur et de la recherche la définition de la cybersécurité est l'état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace. Quant à la définition de la cyberdéfense, c'est l'ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité.

Le cyberespace offre un cadre privilégié aux individus et aux groupes organisés animés d'intentions criminelles, échappant à toute contingence de lieu et de temporalité.

De manière logique, les Etats ne sont pas restés en marge de cette évolution sociétale. Selon la célèbre loi de Metcalfe, la valeur d'un réseau est proportionnelle au carré du nombre de ses utilisateurs [3]. Cela signifie que plus le réseau est employé *(c'est-à-dire plus il y a d'utilisateurs)*, plus il est jugé précieux. Plus de 64% de la population ayant accès à internet, l'accès à ces réseaux et leurs maîtrises sont en cela devenu un véritable enjeu pour les Etats. Face à ces différentes agressions informatiques certes dans un environnement virtuel, les organes de protection de la sécurité nationale des pays démocratiques ont deux responsabilités majeures :

- Garantir la sécurité des systèmes d'information de l'Etat tout en permettant le bon fonctionnement de l'administration et la protection des infrastructures critiques ;
- Etablir un environnement sécurisé favorisant l'instauration et la promotion de la confiance dans la société de l'information.

Les Etats doivent ainsi composer avec différents acteurs pour effectuer leur protection, ce large spectre de parties prenantes inclus la société civile et les entreprises publiques et privées. Considérant que leur souveraineté ne s'arrête pas à leur territoire traditionnel mais s'étend également au cyberespace. Celui-ci tant dans sa dimension physique technique que dans sa dimension « virtuelle » concentre et cristallise les enjeux de pouvoir des Etats. Ceux-ci ont investi le cyberespace sur plusieurs fronts : au niveau politique, économique, universitaire et militaire. Internet peut en effet servir des stratégies indirectes et des technologiques qui, même en temps de paix, visent à amoindrir ou abattre un secteur d'activité, une entreprise, un Etat et peut ainsi apporter des avantages concurrentiels à certains acteurs socio-politico-économiques.

L'expansion permanente de cet espace s'est accompagnée de la complexification des risques et menaces qui y sont liés. Le stratège chinois Sun Tzu recommandait une guerre brève, afin d'engager le moins de ressources possibles : « On ne saurait tenir les troupes longtemps en campagne, sans porter un très grand préjudice à l'État et sans donner une atteinte mortelle à sa propre réputation ». Quoi de mieux qu'une arme nouvelle et discrète pour surprendre et vaincre rapidement un adversaire.

Avec l'apparition de ce nouvel espace, une cinquième dimension est venue s'ajouter à la surface de protection et de confrontation traditionnelle : la terre, la mer, l'air, l'espace. A ce titre, le champ de bien commun et neutre est entré dans le champ militaire. Tel le Wyrd, symbole de la mythologie nordique, qui lie le destin à toute chose, à tout être, le cyberespace est transverse et affecte l'ensemble à la différence des autres dimensions.

La composante cyber doit ainsi être intégrée dans l'art de la guerre. Pour les forces étatiques, les logiques d'affrontements conventionnels des autres dimensions sont applicables mais doivent composer avec des domaines spécifiques de cette zone de conflits. Cette militarisation du cyberespace a eu des effets au niveau national et au niveau international : les stratégies et doctrines se sont adaptées et les Etats ont adoptés des mesures réglementaires protectrices. Ces enjeux seront détaillés dans la **première partie**.

Dans cet espace de conflits, une conception opérationnelle avec une métaphore géologique consiste à l'apparenter à plusieurs couches superposées. Le nombre de couches varient en fonction des auteurs allant de trois à cinq couches, voire pour certains à sept. Dans le cadre de ce mémoire, nous utiliserons la théorie des 3 couches par Daniel Ventre [4] que sont les couches physique, logique et sémantique car cela permet de bien appréhender comment cet espace peut être affecté par des cyberattaques.

La cyberattaque est l'ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité. Pour cela, on considérera le cyberconflit actuel comme une guerre par *(subversion)*, pour *(espionnage)* ou contre *(sabotage)* l'information [5]. Ainsi dans la **seconde partie** seront décrits les différentes couches et les risques et menaces les affectant.

Les cyberattaques tendent à se multiplier depuis une décennie et affectent de plus en plus les États. Dans ces confrontations sur ce domaine numérique, comment les puissances se positionnentelles ? Avec ces nouvelles armes cyber et le panel d'acteurs entrant en jeu, quelles stratégies peuventelles mettre en places autant défensives qu'offensives pour asseoir leur positionnement sur la scène internationale ? Quelles sont les perspectives à horizon 2030 de cette cyber conflictualité ? Nous nous concentrerons sur ces questions dans la **troisième partie**.

Etant donné l'étendue du sujet, nous avons décidé de délimiter notre approche aux cinq cyber puissances que sont les Etats Unis, la Chine, la Russie, Israël et la France. Les approches de ces pays sont bien documentées, dans les textes officiels ou dans les analyses du cyberespace. Pour mesurer le degré de puissance cyber d'un Etat, on peut se référer à des rapports produits par différents organismes, que sont des instituts de recherche ou des institutions internationales. A noter, que chaque étude a son schéma d'analyse propre, les approches et les conclusions peuvent donc différer d'une étude à l'autre. Si les trois premiers Etats font partis du top 3 du classement du Harvard Belfer center [6], Israël n'est pas dans le top 10, la France quant à elle n'est classée que 9ème. Nous avons toutefois décidé de les inclure dans cette étude, Israël étant un acteur incontournable de l'économie cyber, la France comme puissance économique européenne.

1 HISTORIQUE ET CADRE LÉGAL

Cette partie a vocation à rappeler et définir ce qu'est Internet et le cyberespace. Nous évoquerons également le cadre juridique applicable notamment dans le cas de conflits armés ou encore ce qui est fait en matière de prolifération des cyberarmes. Enfin, nous donnerons une vision synthétique des stratégies cyber de certains pays.

CRÉATION D'INTERNET ET CYBERESPACE

Création d'internet

Internet et le cyberespace tel que nous le connaissons aujourd'hui se sont construits petit à petit. D'une part, la mise en réseau a commencé au XIXème siècle avec des inventions comme le télégraphe qui ont révolutionné la façon de transmettre des informations. D'autre part, l'informatique électronique a débuté avec l'invention d'appareils pour aider le calcul mathématique [7]. C'est de là que vient le nom « computer », soit calculateur ou ordinateur en français. Plus tard, c'est la combinaison de la communication en réseau et de l'ordinateur qui ont déclenché une véritable révolution de notre société moderne.

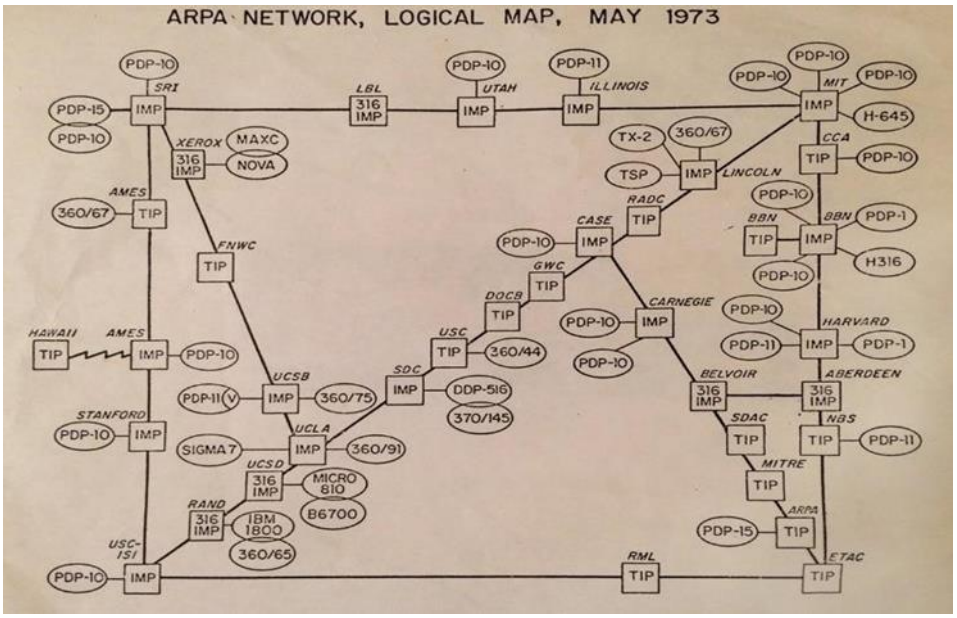
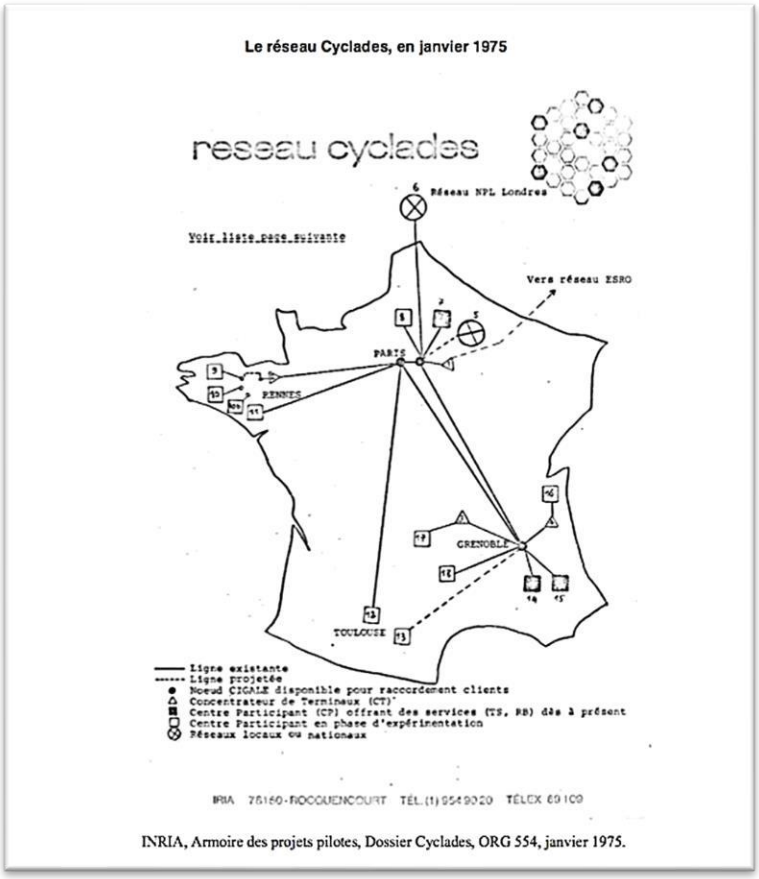


Figure 1 : Schéma logique du réseau ARPANET en 1973

Arpanet a été créé aux Etats-Unis sous l'impulsion de la DARPA. En 1969, la première connexion de réseau Arpanet est réalisée. Ce réseau avait pour but d'expérimenter les techniques d'échange de données par « paquets » et échanger des informations entre les universités et les militaires. Dans les années 70, les recherches se concentrent sur la manière de relier les ordinateurs et les réseaux même si leur architecture et constructeur sont différents. Durant cette même période, les réseaux locaux internes aux entreprises se

développent. Les protocoles TCP *(Transport Control Protocol)* et IP *(Internet Protocol)* sont développés. Ceux-ci sont adoptés par le réseau Arpanet au début des années 1980 et forment la base d'internet. A la même période, la partie militaire et la partie universitaire se séparent en deux réseaux distincts. Le réseau interne Milnet constitue le réseau réservé à l'usage militaire tandis que l'autre partie du réseau se concentrent sur les besoins universitaires et la recherche. Cette partie du réseau est placée sous la responsabilité de la National Science Foundation *(NSF)*. Sous l'impulsion de la NSF il est connecté à de puissants ordinateurs et s'ouvre rapidement à l'usage commercial. C'est cette partie du réseau qui constitue la base de l'internet actuel.

Un projet similaire a été mené en parallèle par le groupe RAND en 1964 aux Etats-Unis qui avait pour objectif de construire un réseau résistant aux attaques nucléaires. La similitude des deux projets a donné lieu à la fausse rumeur que cet objectif était fondateur d'ARPANET.

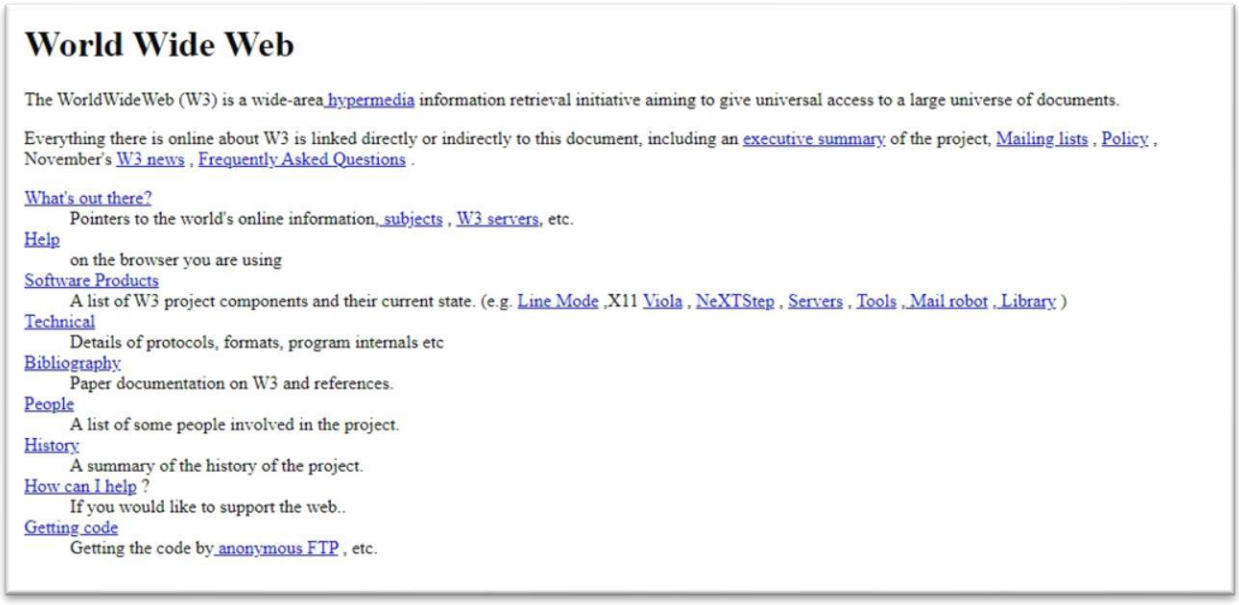


INRIA, Armoire des projets pilotes, Dossier Cyclades, ORG 554, janvier 1975.

Figure 2: Réseau Cyclades (janvier 1975)

La recherche française, en la personne de Louis Pouzin a également expérimenté un réseau à commutation de paquets entre 1972 et 1977 en écho à ARPANET[8]. Ce projet a été abandonné faute de moyens au profit du réseau Transpac en 1978.

D'autres innovations et transformations fondamentales ont permis de modeler l'Internet que nous connaissons aujourd'hui. Ces innovations sont aussi bien issues du monde universitaire et de la recherche que d'entreprises commerciales de la Silicon Valley. Certaines sont tombées en désuétude tandis que d'autres perdurent à tel point qu'elles sont devenues des noms communs dans le vocabulaire quotidien. C'est le cas du World Wide Web, une des nombreuses applications d'Internet qui a contribué à son expansion. Le World Wide Web est une application d'Internet, bien que le terme *Web* soit souvent utilisé par nombre d'internautes comme un synonyme d'Internet. Ce programme a été développé en 1989 par le chercheur britannique Tim Berners-Lee du CERN, l'Organisation Européenne pour la Recherche Nucléaire, dans le but de faciliter et permettre l'échange d'informations en instantané à travers le monde via Internet. Le système a été mis en fonctionnement en 1990 et mis à disposition dans le domaine public par le CERN en 1993 [9].



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

Figure 3 : Première page web de l'histoire

Ce bref rappel historique nous permet de mieux comprendre la définition d'internet de l'INSEE, selon laquelle internet est « un ensemble de réseaux mondiaux interconnectés qui permet à des ordinateurs et à des serveurs de communiquer efficacement au moyen d'un protocole de communication commun (IP). Ses principaux services sont le Web, le FTP, la messagerie et les groupes de discussion. » [10]

Développement et expansion

Le réseau Internet n'a cessé de se développer sous l'influence de plusieurs facteurs. Dans un premier temps l'expansion a été géographique. Du coté des grandes puissances, l'URSS est arrivée tardivement à se connecter à Internet. En 1982, le chercheur Anatole Klyosov à commencer à se connecter à Internet depuis un Modem, mais cela reste une exception jusqu'à la création d'un fournisseur d'accès internet par un autre chercheur, Andreï Soldatov à la fin des années 1980 [11].

L'Internet chinois a également été introduit par le milieu universitaire. La première communication se fait en 1988 entre l'université de Beijing et celle de Karlsruhe en Allemagne. Dès le début de la conception de l'internet chinois, une gouvernance a été mise en place pour accompagner le développement et le contrôle par l'Etat [12].

Les différentes avancées technologiques tant au niveau matériel *(démocratisation de l'ordinateur personnel et des smartphones, etc.)* qu'au niveau de la connectivité *(du bas débit au très haut débit avec la fibre optique)* ont permis une croissance importante des usages, du nombre d'utilisateurs et du volume de flux d'informations échangées.

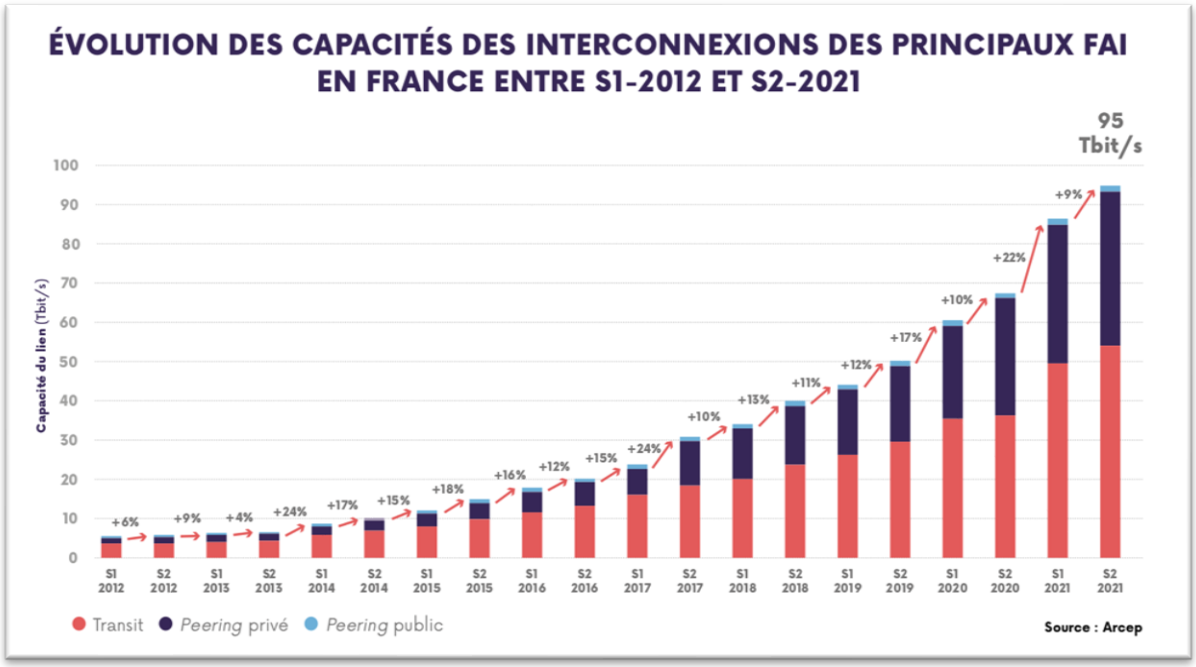


Figure 4 : Evolution des capacités des interconnexions entre FAI en France de 2012 à 2021

Enfin les années 2000 ont vu monter en puissance les grands acteurs privés d'internet, que sont Google *(Alphabet)*, Apple, Facebook *(Meta)*, Amazon et Microsoft plus souvent cités sous l'acronyme GAFAM. Internet se mondialise, le commerce électronique prend de l'ampleur. Les réseaux sociaux également vont apporter un changement de paradigme dans l'espace informationnel.

Qu'est-ce que le cyberespace ?

Avec le développement d'Internet et son utilisation par de plus en plus d'internautes, s'est posée la question de la définition du cyberespace. Les internautes se connectent et interagissent entre eux dans un nouveau lieu non pas physique mais virtuel. Définir ce nouvel espace n'est pas aisé et aucun consensus n'a été trouvé quant à sa définition.

Le cyberespace, d'un point de vue géographique, n'est pas considéré comme un territoire, il n'en reste pas moins un espace où interagissent des êtres humains. Il est « fondamentalement transfrontière » [13]. Paradoxalement, ce lieu virtuel et immatériel est pleinement ancré dans le monde tangible et physique par les infrastructures et le système technique qui sont nécessaires pour le faire fonctionner.

Il y a plusieurs définitions qui permettent d'appréhender ce qu'est le cyberespace. Pour le grand public, la définition la plus courante est celle d'un synonyme d'internet mais en ce qui concerne le domaine politique et militaire, il est désigné comme un environnement, un domaine, un théâtre d'opérations, un espace, un substrat, un milieu, ou un moyen. Certaines définitions restreignent le cyberespace à « *l'espace de l'internet et des mondes dit virtuels* » (*ENS Lyon*). De son côté, l'Agence Nationale de la Sécurité des Systèmes d'Information *(ANSSI)* définit le cyberespace comme *« l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitements automatisés de données numériques »*. La définition issue de la doctrine de défense française offre une conception large et plutôt détaillée du cyberespace comprenant l'ensemble des éléments qui constituent Internet

« 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 des services en ligne » (définition issue de la doctrine de défense française). Cette dernière définition a l'avantage d'évoquer le cyberespace sous la forme de 3 strates : la strate physique *(infrastructures physiques)*, la strate logique *(logiciels et protocoles)* ainsi que la strate cognitive *(contenu qui circule sur cet espace)*. C'est cette conception du cyberespace que nous retenons dans cette étude.

Il est difficile de donner une date exacte de naissance d'Internet. Certains retiennent la création d'Arpanet, d'autres se réfèrent à la création du World Wide Web. Cela reflète bien le fait qu'Internet s'est construit pas à pas et est le fruit d'innovations continues, qu'elles soient impulsées par des organisations étatiques publiques ou des entreprises commerciales. L'Internet du réseau Arpanet était très différent de ce que nous connaissons aujourd'hui. Le processus d'innovation et de transformation n'est pas figé à ce jour et Internet continue d'évoluer.

Initialement plutôt tourné comme un outil permettant de faire progresser la recherche dans un cadre universitaire, l'Internet s'est très vite répandu dans la société avec des finalités multiples. Le cyberespace représente un enjeu social, politique et commercial. De manière concomitante à son expansion, les questions de gouvernance de ce nouvel « objet » et d'application du cadre légal existant se sont posées.

CADRE LÉGAL ET GOUVERNANCE

Les utilisations liées au cyberespace sont multiples allant de la recherche, en passant par les usages commerciaux jusqu'à la cybercriminalité. Avec la montée en puissance du cyberespace, s'est naturellement posée la question de sa dimension juridique, des lois et des normes qui doivent l'encadrer. Il serait difficile de donner une vision exhaustive de tous les traités ou accords en lien avec le cyberespace, mais il est intéressant de mettre en perspective les débats autour de la gouvernance d'Internet et les différents courants de pensée qui s'opposent en ce qui concerne l'application du droit international et la manière dont l'espace numérique doit être appréhendé au niveau légal.

La gouvernance d'internet

La gouvernance d'Internet recouvre plusieurs aspects. D'une part, elle fait référence à la gouvernance « technique ». Il y a un écosystème d'organisations qui gère cette partie technique. Par exemple, l'Internet se base sur un schéma d'adressage commun. Une entité de gouvernance est donc nécessaire pour enregistrer et contrôler l'assignation des adresses. Le système des noms de domaine *(Domain Name System – DNS)* a été proposé par des chercheurs en 1982 aux Etats-Unis et a été totalement adopté par Internet en 1987. L'ICANN *(Internet Corporation for Assigned Names and Numbers)* a été créée aux Etats-Unis en 1998 sous la forme d'une association à but non lucratif basée en Californie. C'est l'institution qui a pour but de veiller à la coordination du système de nommage et d'adressage sur Internet. Cette mainmise étatsunienne sur Internet à travers l'ICANN a été beaucoup critiquée d'autant plus que l'ICANN était reliée au Département du Commerce des Etats-Unis.

« Les problèmes sont loin d'être résolus. La question du contrôle américain a été particulièrement aigue. Le débat devint public lors du Sommet mondial sur la société de l'information organisé par l'ONU. Lors de la deuxième phase, à Tunis en novembre 2005, environ 70 pays y pressèrent les Etats-Unis de renoncer à leur surveillance sur Internet au profit des Nations Unies. Ils refusèrent. » [7]

En 2016, l'institution a été réformée et devient indépendante. Une indépendance relative et formelle pour certains qui estiment qu'en pratique le gouvernement et les grands groupes américains sont toujours très présents.

La gouvernance d'internet ne se limite pas aux aspects techniques mais s'entend aussi comme la gouvernance sur les usages d'internet. Le système international se base sur le système westphalien, c'est-à-dire qu'il reconnaît la souveraineté des Etats sur un territoire clair et délimité par des frontières. Appliquer ce schéma de pensée au monde numérique est complexe du fait de la nature transfrontière du cyberespace. L'enjeu pour les gouvernements est de maintenir une forme de supervision ou de contrôle sur un cyberespace qui ne respecte pas les frontières étatiques.

De plus, concernant Internet, Julien Nocetti, chercheur associé au Centre Russie / Eurasie et au programme Géopolitique des technologies de l'Institut français des relations internationales (Ifri), évoque un *« centre de gravité mouvant »* [14]. Il y a un paradoxe entre les systèmes de coordination du réseau et de normalisation plutôt occidentale et le fait que 70% des internautes vivent en dehors du monde occidental. En 2017, on dénombrait 739 millions d'internautes en Chine contre 718 millions aux Etats-Unis et au sein de l'Union Européenne [14]. L'espace numérique est mondial et international, il est donc logique que sa gouvernance le soit également.

> *« Les tensions qui traversent la gouvernance de l'internet reflètent l'asymétrie entre la forte croissance de l'accès au Web dans les économies émergentes et le caractère intrinsèquement occidental des systèmes de coordination du réseau »* [15]

Les jeux de pouvoirs et les débats autour de la gouvernance d'internet s'inscrivent dans le cadre global des relations internationales. Pour comprendre cette gouvernance, il faut dépasser l'approche traditionnelle des Etats, c'est-à-dire une approche où la souveraineté numérique est un domaine supplémentaire de la souveraineté étatique et les questions s'y référant se discute uniquement entre les nations. La gouvernance d'internet est multi parties prenantes, elle ne se limite pas aux seuls Etats bien qu'ils soient des acteurs non négligeables. On y retrouve les tensions et rivalités « habituelles » entre nations : contestations de la position dominante étatsunienne, affirmation d'une position souverainiste pour certains Etats au premier rang desquels on peut citer la Russie ou la Chine, dépassement du cadre transatlantique pour y inclure les puissances émergentes notamment les BRICS *(Brésil, Russie, Inde, Chine, Afrique du Sud)*. Certains pays comme le Brésil se sont affirmés sur la scène internationale comme les promoteurs d'une gouvernance multipartite.

Par faute de véritable consensus international qui aboutirait à un traité sur Internet et qui poserait un cadre juridique clair auquel la majorité des Etats adhèreraient, ceux-ci s'appuient sur les institutions internationales existantes et les législations nationales *(droit de la protection des données, sécurité etc.)* pour exercer et établir leur gouvernance nationale sur l'espace numérique.

Comme le résume Julien Nocetti : *« la gouvernance d'internet est à la croisée des chemins. Entre une nécessaire évolution vers davantage de pluralisme et de transparence, et la prise en compte des*

mutations de la technologie et de ses usages, elle restera probablement un objet de conflictualité internationale » [14].

L'application du droit international : exemple du droit des conflits armés

Selon l'Organisation des Nations Unies *(ONU)*, on peut définir le droit international comme le droit qui *« définit les responsabilités juridiques des États dans leurs relations les uns avec les autres et les rapports que peuvent avoir ces États avec les individus qui vivent sur leur territoire »*.

Bien que certaines notions qui se rattachent au cyberespace comme le cyberterrorisme ou la cyberguerre ne sont pas définies dans des textes à valeur juridique [16], il n'y a pas de vide juridique dans le cyberespace, au contraire le droit de l'Internet est un « millefeuille législatif et réglementaire » [17]. Il est plutôt admis par les Etats que le droit international est applicable au cyberespace. Le débat se concentre sur les modalités d'application du droit existant et sur la nécessité ou non d'établir des nouvelles règles spécifiques au cyberespace. Ces questions sont régulièrement traitées dans le cadre de groupes en lien avec les institutions internationales (*Nations-Unies, Organisation de Coopération de Shanghai, etc.*). On peut également citer le Manuel de Tallinn *(2013)*, résultat du travail d'un groupe d'experts internationaux sur l'applicabilité du droit international à la cyberguerre. Une seconde édition est venue enrichir ces travaux en 2017. Cette étude, bien que ne représentant la doctrine d'aucune organisation internationale, est une étude approfondie du droit international existant. Toutefois, malgré les travaux universitaires et les débats récurrents, la communauté internationale est encore loin d'avoir un consensus sur ces questions.

Théoriquement, le droit des conflits armés est applicable à la dimension cyber si l'on considère que l'informatique est un moyen supplémentaire à disposition des Etats ou des groupes armés. Toutefois, le droit des conflits armés n'a pas été écrit avec cette dimension à l'esprit. Certaines dispositions sont inadaptées à l'univers informatique, ce qui le rend en pratique difficilement invocable. En effet, pour pouvoir qualifier d'« agression » un acte, il faut pouvoir prouver avec certitude qui est l'« agresseur ». Cette règle simple revêt une dimension complexe dans le cadre d'un écosystème cybercriminel toujours plus délicat à appréhender. Beaucoup de groupes APT *(Advanced Persistent Threat)* sont soupçonnés d'être affiliés à des Etats sans pour autant que l'on dispose de preuves directes les reliant à ceux-ci.

Le concept de frontière est également un obstacle. Le cyberespace a la particularité d'être plutôt pensé comme un espace transfrontière. La notion de frontière est importante dans le droit des conflits armés car elle délimite les territoires et donc les souverainetés et les responsabilités. A noter que l'aspect transfrontière est remis en cause par certain Etats comme la Chine ou la Russie avec l'idée d'un Internet interne.

De plus, la notion de seuil ou d'intensité pose question. Dans une attaque, il y a la notion d'agresseur et d'intensité. Afin de pouvoir invoquer le droit de légitime défense, l'agression doit avoir un certain niveau d'intensité. Quel est le seuil d'intensité pour qu'une cyberopération soit considérée comme un recours à la force envers un Etat et donc ouvrir le droit à l'invocation de la légitime défense pour ce dernier ? Les avis sont partagés sur cette question. Les cyberattaques causent peu de dommages matériels et humains. Ce qui est frein pour qu'un Etat invoque la légitime défense. Toutefois, la légitime défense n'est pas le seul moyen à disposition des Etats pour répondre à une cyberopération [18] :

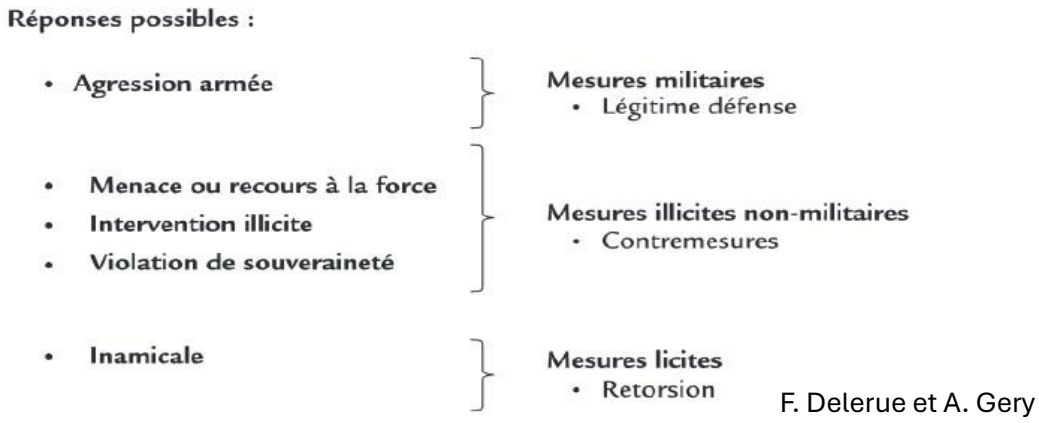


Figure 5 : Les réponses possibles à une cyberopération en droit international

Prolifération des cyberarmes

Le contrôle des exportations serait un moyen non négligeable de lutter contre le développement des cyberarmes. Au même titre que les traités et accords qui permettent d'encadrer et de contrôler la prolifération des armes classiques, il pourrait permettre de limiter la prolifération des outils numériques offensifs [19]. Toutefois, même si ce raisonnement semble facile, l'analogie a ses limites. Des mêmes lignes de code pouvant être utilisées dans un but illégitime et malveillant - comme une intrusion dans un système dans un but d'espionnage ou de destruction - aussi bien que dans un but légitime et inoffensif. L'usage initial peut être détourné pour une utilisation différente. Seule la finalité d'utilisation permet de faire la distinction entre un outil informatique et une cyberarme [16]. Le caractère dual des outils informatiques rend impossible la simple transposition des dispositions écrites pour les armes classiques. Il faut mener une réflexion à part entière qui prenne en compte les spécificités du code informatique.

Afin d'illustrer cette complexité, nous pouvons prendre l'exemple de l'Arrangement de Wassenaar. Créé en 1996, il compte aujourd'hui 42 membres, principalement européens, dont la dernière adhésion est celle de l'Inde en 2017 [20,21]. Son but est de « *contribuer à la sécurité et la stabilité régionale et internationale en promouvant la transparence ainsi qu'une plus grande responsabilité dans les transferts d'armes conventionnelles et de biens et technologies à double usage, pour, au final, en prévenir les accumulations excessives* ». Il s'agit donc de contrôle à l'exportation et de responsabilisation des Etats.

À la suite d'affaires ayant révélées l'implication d'entreprises européennes dans la vente de systèmes de surveillance et d'interception de communications, le Royaume-Uni et la France ont proposé de modifier la *Liste des biens et technologies à double usage* de l'Arrangement de Wassenaar. Les logiciels d'intrusion et systèmes de surveillance IP ont donc été ajoutés.

En 2017, ces nouvelles dispositions en vigueur ont été modifiées. Celles-ci sont en effet pensées autour des technologies et ne prennent pas en compte l'usage. Toutefois, lorsqu'il s'agit de technologies cyber il se révèle important de prendre en compte l'utilisation. Un certain nombre d'experts ont mis en évidence le fait que les dispositions telles qu'elles étaient posées dans l'Arrangement portaient atteintes au niveau de cybersécurité mondiale en imposant des restrictions sur des systèmes et outils

nécessaires à la recherche en cybersécurité et à l'amélioration de la sécurité des systèmes d'information [19].

D'autres traités et accords internationaux contiennent des mesures qui visent à empêcher la diffusion des outils numériques malveillants. C'est le cas de la Convention de Budapest contre la cybercriminalité, créée dans le cadre du Conseil de l'Europe. Le but est de favoriser la coopération internationale et créer une base juridique commune internationale permettant aux Etats parties de lutter plus efficacement contre la cybercriminalité. L'article 6 de la convention dispose que le transfert de certains codes malveillants constitue une infraction. Toutefois, pour que l'infraction soit effective il faut qu'il y ait une intention dans l'utilisation de l'outil à des fins malveillantes. L'élément intentionnel et la finalité de l'usage sont pleinement pris en compte.

Plusieurs limites existent actuellement en ce qui concerne la régulation des « cyberarmes ». La première, liée à l'exemple décrit est que l'Arrangement de Wassenaar ne concerne que 42 Etats dont beaucoup sont européens et donc soumis par ailleurs au régime européen de contrôle aux exportations des biens à double usage. Sa portée est de fait limité. Il en va de même avec la Convention de Budapest, à laquelle 68 Etats ont adhéré. Un enjeu important est donc l'uniformisation et « l'universalisation » des contrôles. Ces contrôles sont d'autant plus compliqués que la création et diffusion des cyberarmes sont plus aisées que celles des armes de destruction massive. De multiples acteurs peuvent être impliqués dans la diffusion d'outils numériques offensifs *(société civile, entreprises etc.)*. Une seconde limite, plus générale, est que pour aboutir à une législation sur l'encadrement de la prolifération des cyberarmes, l'étape essentielle et nécessaire serait d'avoir une définition universelle de ce qu'est une cyberarme. Or, à date aucune ne fait consensus entre Etats. Dans le cadre de l'Arrangement de Wassenaar il est fait mention de « logiciels d'intrusion ». Du côté des groupes d'experts gouvernementaux qui travaillent sur les questions d'informatique et de télécommunications en lien avec la sécurité internationale, ce sont les termes de « *techniques et outils informatiques malveillants* » qui sont utilisés. Là encore c'est une expression globale et peu précise. Le terme de cyberarme peut faire référence à un éventail large d'outils *(virus, rançongiciels etc.)* aux effets divers : espionnage et intrusion, vol de données, destruction de données etc. [19].

Des normes de conduites non contraignantes existent pour prévenir la prolifération des cyberarmes, comme le propose le rapport de 2015 du GEG (*groupe d'experts gouvernementaux réunis dans le cadre des Nations Unies pour traiter des sujets d'informatique et de sécurité internationale*) adopté par consensus par les Etats membres. Mais ces normes ne s'accompagnent pas d'une obligation de mise en place de contrôle aux exportations par exemple. Le traitement de la prolifération des cyberarmes est un sujet complexe à traiter au niveau international, les Etats sont cependant conscients des enjeux qui y sont liés notamment pour garantir la sécurité de l'espace numérique mondial.

> *« Les instruments juridiques adoptés par les Etats pour tenter de réguler les cyberarmes présentent quatre grandes caractéristiques : ils sont majoritairement non contraignants, leur portée n'est pas universelle, leur précision est variable et il n'existe pas d'articulation entre eux. »* [19]

S'il est possible de « gouverner » internet, il apparaît difficile de penser sa gouvernance avec un schéma de pensée traditionnelle. Notamment parce que le système international « westphalien » qui applique la souveraineté à un territoire délimité par des frontières claires est difficilement applicable au cyberespace. Le rôle des Etats dans cette gouvernance et leurs relations entre eux mais aussi avec les parties prenantes reste encore à préciser. L'espace numérique représente pour les Etats un domaine de

plus sur lequel leur souveraineté s'exerce, un enjeu de pouvoir, d'influence mais également un nouveau moyen offensif et défensif. Il est donc logique que les sujets de gouvernance d'Internet, de droit applicable dans le cyberespace notamment le droit des conflits armés, les questions de limitation de la prolifération des cyberarmes ou encore les réponses possibles en cas d'attaque de désinformation soient des sujets éminemment politiques pour lesquels il est difficile de trouver un consensus. Les stratégies et doctrines des Etats permettent de comprendre leurs prises de position au niveau international.

STRATEGIES CYBER

Les grandes puissances se sont dotées de stratégies ou doctrines de cybersécurité. Dans cette étude, nous avons pris le parti d'étudier les pays les plus en avance sur le plan cyber, à savoir : les EtatsUnis, la Russie, la Chine, la France et Israël. Pour autant d'autres pays comme par exemple le Canada, l'Australie, le Royaume-Uni, l'Estonie, la Nouvelle-Zélande, l'Indonésie, l'Iran, l'Inde, le Japon, la Corée du Nord ont également une certaine maturité cyber ou sont en train de se développer dans ce domaine [22].

Les doctrines sont publiées par les Etats. Ces documents publics ne sont qu'une partie visible de leur stratégie. Par définition, il n'est pas possible d'obtenir et de publier des documents secrets des Etats. Néanmoins les différentes stratégies sont complétées, quand c'est possible, par des discours de dirigeants, des recherches sur des attaques ou des fuites d'informations susceptibles d'apporter un angle différent ou complémentaire d'analyse. En effet, si publiquement la posture défensive est affirmée, il n'en est pas toujours de même pour le volet offensif.

Un évènement a servi d'accélérateur concernant la posture de cybersécurité des Etats et son intégration dans la stratégie de défense des Etats a été les cybers attaques de 2007 contre l'Estonie en provenance de la Russie. Les plus grandes puissances avait déjà pris en compte cet aspect cyber dans leur réflexion bien avant cette attaque, mais son ampleur a permis d'en matérialiser concrètement son pouvoir de nuisance. Cela conduira à la création dans plusieurs pays d'entités ou de stratégies de cyberdéfense autour des années 2009 et 2010.

Les Etats-Unis

Les Etats-Unis sont de loin le pays qui a investi le plus dans son armée. Au niveau militaire, les Etats-Unis ont une instance de commandement cyber dédié USCYBERCOM depuis 2010 avec la même direction que la National Security Agency (NSA)

Les Etats-Unis ont mis à jour leur stratégie concernant la cybersécurité en mars 2023. Cette version signée par le président Joe Biden reprend des éléments de la stratégie de 2018 publiée sous la présidence de Donald Trump et apporte des renforcements sur certains points comme l'amélioration de la sécurité des acteurs privés, la coopération public-privé ou la coopération internationale.

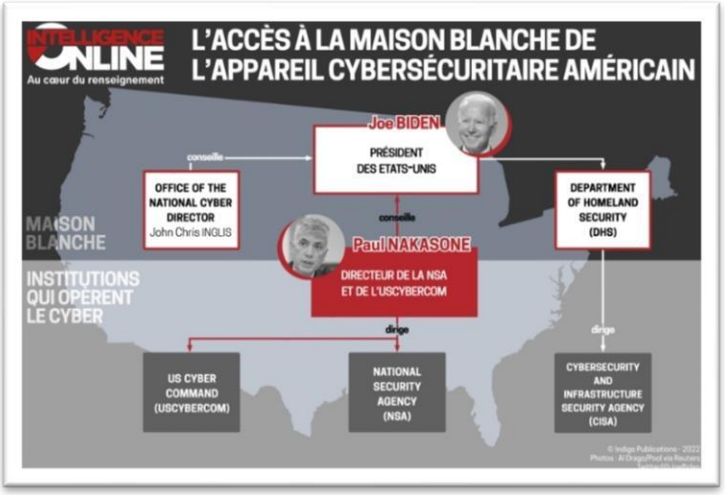


Figure 6: L'appareil de cybersécurité Américain

Les pays qui menacent les intérêts des Etats-Unis sont clairement nommés et leurs méthodes décrites. Ces pays sont, la Chine, la Russie, l'Iran, la Corée du Nord ou les autres pays autocratiques.

Les cinq piliers décrits dans la stratégie [23] de 2023

1. Protéger les infrastructures essentielles

Cela consiste à établir des exigences de sécurité pour un socle minimal de cybersécurité. Ces exigences sont réglementaires et les entreprises sont encouragées à aller plus loin.

Etablir une structure de coordination fédérale qui est interconnectée avec des services de soutien aux acteurs industriels privés.

Les agences principales en charge sont le CISA (Cybersecurity and Infrastructure Security Agency) qui s'appuie sur le NIST (National Institute of Standards and Technology) pour l'état de l'art normatif.

La partie sectorielle est gérée par le SRMA (Sector Risk Management Agencies).

La partie sectorielle comprends les activités suivantes :

- Secteur chimique.
- Secteur des installations commerciales.
- Secteur des communications.
- Secteur de la fabrication critique.
- Secteur des barrages.
- Secteur de la base industrielle de défense.
- Secteur des services d'urgence.
- Secteur de l'énergie.
- Secteur des services financiers.
- Secteur de l'alimentation et de l'agriculture.
- Secteur des installations gouvernementales.
- Secteur des soins de santé et de la santé publique.
- Secteur des technologies de l'information.
- Secteur des réacteurs nucléaires, des matières et des déchets.
- Secteur des systèmes de transport.
- Secteur des systèmes d'approvisionnement en eau et de traitement des eaux usées.

La NSA couvre la protection des données les plus sensibles de l'Etat. Au niveau national, chaque agence a également sa feuille de route [23].

2. Démanteler ou empêcher les acteurs de la menace

La lutte contre les rançongiciels est une priorité, notamment avec la participation du FBI (Federal Bureau of Investigation) en plus des acteurs cités dans le 1er pilier. Le but est de les démanteler les acteurs de la menace qu'il s'agisse de cybercriminels ou autres. Si le démantèlement n'est pas possible l'objectif est de rendre leur action difficile et remonter les flux de cryptomonnaie. En collaboration avec les acteurs de l'internet, protéger les infrastructures en nuage, les bureaux d'enregistrement de domaines, les hébergeurs ou autres services afin qu'ils ne puissent pas être exploité par les attaquants.

3. Orienter le marché vers la cybersécurité et la résilience

L'aspect fondamental de la protection des données personnelles et le développement sécurisé est mis en avant et notamment sur l'IOT. Le marché a tendance à favoriser le non-respect des règles élémentaires de sécurité, aussi la responsabilité des éditeurs ou fournisseurs de service doit être engagée.

4. L'investissement stratégique dans la résilience future

Les Etats-Unis continuent d'investir pour conserver et accroître leur puissance cyber. Les secteurs privilégiés en recherche et développement sont l'intelligence artificielle, les systèmes de contrôle industriels, l'infrastructure en nuage, les télécommunications, le cryptographie, la transparence des systèmes et l'analyse des données.

Internet a été bâti sur des standards et protocoles basés sur la confiance, aujourd'hui ces protocoles doivent tendre à être remplacés par des évolutions sécurisées.

Ces efforts doivent prendre en compte les enjeux futurs de l'ordinateur quantique et de la production d'énergie renouvelable.

Enfin le développement d'une identité numérique fiable pourrait rendre l'usurpation d'identité et la fraude beaucoup plus complexe ainsi que développer l'économie numérique.

5. La coopération internationale pour des objectifs communs

L'appui des partenaires internationaux pour la vision commune de l'internet et des échanges entre les CSIRT

Collaborer avec les alliés pour faire progresser leur niveau de sécurité

Apporter un soutien aux alliés et partenaires pour la réponse à incidents

Etablir des coalitions pour un comportement responsable des Etats et dans le cas contraire, pouvoir s'associer pour condamner les agissements et les réprimer significativement de manière diplomatique par tous les outils possible (l'isolement diplomatique, les coûts économiques, les opérations de lutte contre la cybercriminalité et d'application de la loi, ou les sanctions juridiques, entre autres)

Sécuriser la chaîne d'approvisionnement de l'économie des Etats-Unis. Pour les infrastructures les plus sensibles les développements doivent être américains ou alliés comme pour la 5G ou la nouvelle génération de réseaux sans fils.

D'un point de vue offensif, les Etats-Unis restent plutôt discrets. Malgré tout, quelques fuites d'attaques permettent de se faire une idée de la réalité. Une directive top secrète de Barak Obama d'octobre 2012 [24] parle de « Offensive Cyber Effects Operations (OCEO) » et précise de dresser une liste de cibles étrangères potentielles. Les actions offensives peuvent être des représailles, une anticipation d'une attaque ou des actions faisant avancer les objectifs des Etats-Unis. Si le premier cas se heurte seulement au problème de la vraisemblance de l'attribution, les deux suivants laissent le champ libre à beaucoup d'actions. Le texte contient toutefois quelques garde-fous comme la conformité au droit international et américain ainsi que l'approbation du président si l'opération est susceptible de graves conséquences.

L 'attaque cyber qui a marqué le monde est attribuée aux Etats-Unis et à Israël. Il s'agit de Stuxnet, un virus introduit dans le projet d'enrichissement d'Uranium Iranien destiné à saboter discrètement les machines industrielles.

La fuite d'information de la National Security Agency par le lanceur d'alerte Edward Snowden en 2013, a révélé l'espionnage à grande échelle des Etats-Unis, y compris de pays alliés. Une grande partie du trafic mondial à cette époque passaient par les Etats-Unis en raison d'un coût de transit plus faible. Le programme de surveillance PRISM

La NSA est liée à un groupe de très haut niveau, Equation Group[25], qui développe des cyber armes basé sur des failles qui ne sont pas publiquement connus appelé couramment 0days ou encore des attaques qui modifient les microcodes de disque dur afin d'être à la fois persistant et quasiment indétectable. L'exploit le plus puissant connu est EternalBlue qui leur a été dérobé par un groupe The Shadow Brokers et exploité notamment dans le rançongiciel WannaCry ou encore le wiper NotPetya.

Enfin les tissus économiques du numérique est un atout majeur des Etats-Unis. Les acteurs majeurs privé d'Internet sont tous des sociétés américaines. Les GAFAM en sont l'exemple le plus visible. Cette prédominance des acteurs de poids permet l'investissement dans la recherche et développement ou dans le rachat de startup innovantes.

La Russie

La position de la Russie est décrite dans les différentes stratégies de sécurité nationale dont la dernière mise à jour est l'oukase présidentiel n°400 publié par la chancellerie du Kremlin le 2 juillet 2021[26]. La cybersécurité n'y est abordée que très succinctement, mais on comprend que les risques globaux s'appliquent également au cyberespace qui n'est qu'un moyen de plus dans l'arsenal militaire russe.

Les Etats-Unis et leurs alliés, dont la France et Israël, sont clairement catégorisés comme des pays hostiles. Les tensions mondiales sont le risque à prendre en compte.

Un des points majeurs du texte concerne la sécurité informationnelle. La Russie aspire à la souveraineté sur ce point pour éviter les fausses informations propagées par des pays hostiles et réfute les accusations d'influence sur les élections de ces mêmes pays.

La protection des valeurs, de la tradition et de la culture du peuple russe doit être préservée des attaques occidentales.

La défense des intérêts de la Russie passe par le plan informationnel pour influer sur l'opinion dans le sens des valeurs défendues. Même si le Kremlin dément, d'autres sources indiquent que Evgueni Prigojine, proche de Vladimir Poutine, est le créateur de la compagnie militaire privée Wagner et de l'Internet Research Agency de St-Pétersbourg[27]. Cette agence qualifiée de « ferme à troll » par des journalistes a mené des campagnes de désinformation au profit du Kremlin.

Un autre point important est la volonté de ne pas être dépendant des autres pays pour le réseau internet. La Russie se fixe l'objectif d'être indépendant.

L'Etat a également beaucoup légiféré pour pouvoir protéger, surveiller et dissuader toute voix dissonante par rapport au discours officiel.

La loi de 2019 sur l'internet souverain permet de couper l'accès au réseau internet mondial. Ce principe de protection est communément appelé balkanisation d'internet dans les différentes études sur le sujet ou plus simplement « Splinternet » en anglais. Sa mise en place est plus complexe pour la Russie que les pays qui l'ont prévu dans la construction du réseau comme la Chine ou l'Iran. Malgré ces difficultés, la volonté de contrôle est un objectif à très court terme comme le reflète le Runet qui regroupe un

ensemble de systèmes et de services informatiques formant un certain niveau de souveraineté numérique [28].

Figure 7 : Ensemble de loi cybersécurité en Russie

Les documents publics de stratégie ne décrivent pas précisément l'implication des services étatiques dans les cyberattaques envers les pays étrangers. Néanmoins certains travaux de recherches ou des fuites de données motivées par l'opposition de certains russes à la guerre en Ukraine permettent de comprendre leur mise en œuvre. Les fuites les plus récentes concernent le groupe de rançongiciels russe Conti au début de l'année 2022 et les documents de la société Vulkan début 2023.

Les échanges de messagerie instantanée du groupe Conti mettent en évidence un lien probable avec le bureau du FSB de St-Pétersbourg qui leur passerait des commandes, des récompenses du Kremlin sur cibles spécifiques et l'alignement avec les intérêts Russes en évitant de piéger les entreprises russes ainsi que la Chine [29].

D'autres groupes russes sont impliqués dans des attaques de grande ampleur comme Sandworm en 2017 dépendant du GRU *(direction du renseignement militaire)*, qui a lancé NotPetya, un wiper destiné à saboter les systèmes informatiques, mais qui se fait passer pour un rançongiciel. La chronologie de la propagation débute en Ukraine avant de toucher le monde entier avec des dommages collatéraux y compris en Russie.

En plus des groupes d'attaquants, l'utilisation du secteur privé comme la société de conseil en cybersécurité Vulkan dirigée par deux anciens gradés de l'armée russe a été mise en lumière grâce à une fuite de documents. Ils montrent des liens avec la direction du renseignement militaire *(GRU)*, le service fédéral de sécurité *(FSB)* et le service de renseignement extérieur *(SVR)*. [30,31]

Pour autant les attaques en dehors de la période de guerre avec l'Ukraine sont plutôt réalisées en essayant de brouiller les pistes quant à l'attribution de l'attaque. Pour ce faire il est courant d'utiliser des techniques ou des infrastructures d'autres pays. Par exemple l'attaque de TV5 monde en 2015 est vraisemblablement réalisée par la Russie qui essaye de faire porter la responsabilité sur l'Etat Islamique [32].

Enfin le sujet de l'intelligence artificiel est abordé lors de la visite le 23 mars 2023 de Xi Jinping, président de la République Populaire de Chine, où Vladimir Poutine a déclaré :

> *La souveraineté technologique est la clé de la durabilité. Nous proposons d'améliorer encore les partenariats stratégiques dans des secteurs spécifiques. En combinant leurs capacités de recherche et leurs capacités industrielles, la Russie et la Chine peuvent devenir des leaders mondiaux dans les domaines des technologies de l'information, de la cybersécurité et de l'intelligence artificielle.*

Cette déclaration complète les orientations de la Russie sur l'intelligence artificielle qui n'étaient pas abordée dans la stratégie.

Plus concrètement, son utilisation dans des opérations de lutte informationnelle grâce à des *deepfake* est très probable même si les « canulars » de Vovan et Lexus, très orientés pro Kremlin qui visent à piéger des hommes politiques sont en général bien plus rudimentaire et utilisent plutôt la voix comme avec Christine Lagarde ou profitent de la barrière de la langue en se faisant passer pour un traducteur comme avec François Hollande. Il est ensuite assez simple comme cela a été fait avec les images de François Hollande de faire une fausse traduction dans les sous titres pour changer le message.

La Chine

La République Populaire de Chine veut s'affirmer comme une superpuissance mondiale dans tous les domaines. En ce qui concerne le domaine militaire et cyber, le pays a vite pris conscience, dans les années 1990 au moment de la guerre du Golfe de son infériorité par rapport aux Etats-Unis. Etant difficile de développer ses capacités militaires conventionnelles pour rivaliser avec les Américains, les penseurs de la doctrine chinoise se sont concentrés sur d'autres moyens : la guerre économique et la

guerre de l'information, autrement dit pour ce dernier aspect, devenir une cyberpuissance. Ceci explique le concept de « guerre asymétrique » qui ressort dans la doctrine chinoise. On retrouve l'objectif « d'informatisation » dans les Livres blancs depuis 2006. Au cours des années 2000, le cyberespace est devenu un champ de bataille essentiel.

Selon Ye Zheng et Zhao Baoxian, deux officiers de l'Académie des sciences militaires, *« un Internet libre [est] comme une menace pour le Parti-Etat »* [33]

L'idée de supériorité et de contrôle dans le domaine de l'information est donc un fondement de la stratégie chinoise. L'art de la guerre de Sun Tzu, qui date environ du IIIe siècle avant notre ère, fonde les principes de la guerre de l'information chinoise : « la guerre c'est l'art de duper », il s'agit là de « vaincre sans combattre ». La guerre de l'information vue par le gouvernement chinois est menée à l'extérieur comme à l'intérieur du pays, selon le principe que « l'intérieur et l'extérieur sont différents ». Pour soutenir ses ambitions, le parti a mis en place toute une organisation à laquelle participe de multiples acteurs. Par exemple, avec la réforme de l'Armée populaire de libération (APL) en 2015, la Force de soutien logistique a été créée dont dépend le Network System Department qui *« a pour mission la guerre cybernétique, les technologies de reconnaissance, la guerre électronique et la guerre psychologique »* [34]. Elle a également une *« armée bleue »*, ce sont des experts chargés de la sécurité de l'espace numérique chinois.

Le gouvernement n'hésite pas à s'appuyer sur des civils pour compléter les forces de l'armée traditionnelle pour des opérations. Des hackers civils peuvent donc participer à des opérations sur des réseaux jugés ennemis. Xi Jinping a créé en 2017 la commission pour l'intégration civile et militaire qui a pour but de permettre à l'armée d'avoir accès à toutes les ressources et innovations issues du secteur civil pour le domaine de la guerre de l'information. La même année a également été créé le Cyber Security Innovation Center dont la mission est d'aider l'armée à « remporter les guerres de demain ».

De plus, il faut relever les liens entre les entreprises privées chinoises et l'armée. Par exemple, le fondateur de Huawei est un ancien ingénieur militaire. L'intégration des moyens issus de la société civile permet à la Chine d'augmenter sa capacité d'action, à l'intérieur comme à l'extérieur de ses frontières.

Pour mettre en œuvre sa stratégie, l'Etat-parti a promulgué beaucoup de lois depuis les années 1990 qui lui permettent de contrôler le contenu et l'accès à Internet. Il a également mis en place le Great Firewall of China *(grand pare-feu)*, qui est issu du projet Bouclier doré lancé en 1998. Ce n'est pas un logiciel en particulier mais un ensemble de mesures qui permet au Parti de contrôler Internet en Chine. Parmi les dispositifs mis en place : filtrage des mots clés, surveillance de l'espace numérique par des policiers du web. Ce dispositif a une double vocation : il permet au régime de se protéger de l'extérieur tout autant qu'il lui permet de contrôler l'information à l'intérieur du territoire. L'effet direct de cette politique a été le développement de géants chinois qui avaient toute latitude pour se développer en l'absence des géants étatsuniens présents ailleurs : WeChat, Weibo, Tencent, Alibaba, Baidu, Xiaomi. Le développement de ces géants chinois n'est pas anodin et s'intègre dans la stratégie chinoise pour être une puissance sur tous les fronts. Le pays ne veut pas être dépendant d'autres puissances et veut garder le contrôle sur les technologies et domaines jugés stratégiques.

Sur le plan de la politique extérieure, la Chine est très présente au sein des organisations internationales sur tous les sujets en lien avec le cyber. La Chine s'appuie sur le principe de *« souveraineté de l'espace cyber »* [34]. Elle fait la promotion de ses standards et normes dans les instances de gouvernance

d'Internet, avec une volonté de limiter la « mainmise » occidentale sur le cyberespace *(via l'ICANN par exemple).*

> *« […] la maîtrise d'Internet constitue désormais l'un des enjeux centraux des rapports sino-américains, tout en représentant un attribut de leur puissance respective, ce qui irrite une Russie se percevant en superpuissance numérique »* [12]

Si certaines propositions n'aboutissent pas, comme ce fut le cas en 2006 avec la proposition du standard Wifi *(WAPI)* rejetée par l'ISO au profit du standard américain d'autres représentent une victoire pour la Chine comme l'attribution par l'ICANN en 2010 de noms de domaines en caractères chinois. « Un pas supplémentaire vers la sinisation du cyberespace » [33]

« Internet a certes contribué à changer la Chine mais la Chine entend aussi, pour sa part, changer le monde des nouvelles technologies de l'information en façonnant un cyberespace aux caractéristiques chinoises et en l'utilisant au profit de sa montée en puissance » [33]

Enfin, la Chine est très active sur le volet offensif. Plus d'une centaine de groupes d'APT qui sont présumés être liés à la Chine sont référencés par les sociétés de cybersécurité [35]. Même si les attaques sont globalement moins sophistiquées que celles d'autres pays, elles sont efficaces car nombreuses et touchant des sociétés dont le niveau de cybersécurité est bien souvent insuffisant. L'espace cyber est donc un moyen pour le gouvernement chinois de servir ses objectifs politiques et économiques comme en témoigne les multiples attaques et campagnes de désinformation dont Taiwan fait régulièrement l'objet.

La France

Consciente des enjeux de sécurité, en 1986, la France a mis en place une politique globale de sécurité des systèmes d'information (SI) et a créé une commission et une délégation interministérielle pour la sécurité des services d'information. 10 ans plus tard cette organisation est revue. Ainsi en 1996, la responsabilité de la surveillance et des risques des SI est transférée au secrétariat général de la défense nationale (SGDN). Toujours au sein du SGDSN, la direction centrale de la sécurité des services d'information (DCSSI) est créée en 2001 avec pour mission : d'évaluer et de vérifier la sécurité des SI des administrations, de leur apporter du conseil, d'agréer les chiffreurs pour la protection les données classifiées et de mettre en œuvre les conformément aux plans gouvernementaux Piranet ou Vigipirate [36]. Ces plans sont respectivement pour la réaction aux crises informatiques majeures et pour la lutte contre le terrorisme [37]. Le constat du rapport de Pierre Lasbordes en 2006 montre que les enjeux de sécurité des SI sont très loin d'être adressés : *« la France accuse un retard préoccupant face aux impératifs de sécurité des systèmes d'information, tant au niveau de l'Etat qu'au niveau des entreprises, quelques grands groupes mis à part »* [38]

Le livre blanc sur la défense et la sécurité national dans version de 2008 sous la présidence de Nicolas Sarkozy va définir les axes stratégiques et créer une structure dédiée pour traiter la sécurité des Systèmes d'information. La France a créé l'Agence Nationale de la Sécurité des Systèmes d'Information *(ANSSI)* en 2009. Elle est rattachée au secrétariat général de la défense et de la sécurité nationale

L'ANSSI a pour mission la réalisation de quatre objectifs stratégiques [39] :

- Être une puissance mondiale de cyberdéfense.
- Garantir la liberté de décision de la France par la protection de l'information de souveraineté.
- Renforcer la cybersécurité des infrastructures vitales nationales.
- Assurer la sécurité dans le cyberespace.

Pour la protection des actifs les plus critiques pour le bon fonctionnement de la nation, la stratégie de la France a contraint les Organismes d'Importance Vitale (OIV) à appliquer les recommandations de l'ANSSI par la loi. L'article 22 de la loi de programmation militaire (LPM) de 2013 et le livre blanc sur la défense et la sécurité national dans version de 2013 pose le cadre de sécurité exigé pour les OIV qui ont l'obligation de protéger leur les systèmes d'information d'importance vitale (SIIV). L'ANSSI maintient une liste d'environ 250 OIV qui n'est pas publique [40]. Elle inclut des entreprises dans les 12 secteurs d'activité d'importance vitale (voir figure 6).

Dans un second temps, elle a créé le commandement de la cyber défense (COMCYBER) en 2017. Il est sous la direction du chef d'état-major des armées [41].

Le COMCYBER est constitué de 3600 cybers combattants. Ce chiffre est amené croitre rapidement puisque la cible est de 5200 à l'horizon 2025. Il est constitué de différents centres de compétences :

- Le GCA : Groupement de la cyberdéfense des Armées
- Le CALID : Centre d'analyse en lutte informatique défensive
- Le CASSI : Centre d'audits de la sécurité des systèmes d'information
- Le C2PO : Centre cyber de préparation opérationnelle
- Le CHPI : Centre des homologations principales interarmées

La France a publié des doctrines sous la responsabilité de COMCYBER selon plusieurs axes qui sont:

- La Lutte Informatique Défensive LID[42]
- La Lutte Informatique Offensive : LIO[43]
- La lutte d'influence[44]

La France a bien séparé ces 3 axes en termes d'organisation et fait la distinction entre les temps de paix ou les temps de guerre.

La lutte informatique défensive est nécessaire pour se prémunir de l'espionnage, du sabotage ou des attaques informationnelles.

Les principes de défense sont déclinés en 6 missions :

- Prévenir : Cela consiste à sensibiliser les utilisateurs aux risques cyber.
- Anticiper : Cela consiste à évaluer l'état de la menace et prendre des mesures préventives si la vraisemblance de l'attaque est élevée.
- Protéger : Cette protection consiste à diminuer le nombre des vulnérabilités, le but étant de rendre le travail des attaquants plus complexe et de faciliter la détection.
- Détecter : Cela consiste à rechercher les éléments d'une cyberattaque en cours en faisant appel au besoin aux partenaires nationaux et internationaux.
- Réagir : Cela consiste à gérer la continuité de l'activité en résistant à la cyberattaque. Les moyens peuvent être conventionnels *(justice, diplomatie, sanction économique, ...)*.
- Attribuer : Cela consiste pour les hauts responsables politiques de préciser l'auteur d'une cyberattaque sur cyberdéfense (PPC) qui est définie par 4 niveaux de

menaces à l'encontre des systèmes informatiques du ministère en écho au classement des attaques informatiques de la revue stratégique de cyberdéfense de 2018.

Ces niveaux sont associés à des stades d'alerte (voir figure 9) :

- Jaune et orange => risques potentiels plus ou moins importants. => vigilance
- Rouge => risques hostiles jugés plausibles => renforcé
- Écarlate => risques majeurs et simultanés => crise

Echelle de gravité	Equivalence avec l'échelle CISS USA	Caractérisation de l'impact	Caractérisation comme agression armée au sens de l'article 51 de la Charte des Nations-Unies
Niveau 5 - Situation d'urgence extrême	Level 5 Emergency (Black)	Impact extrême	Probablement possible : à examiner au cas par cas.
Niveau 4 - Crise majeure	Level 4 Severe (Red)	Impact majeur	Probablement impossible : les actions correspondant à ces niveaux pourraient néanmoins constituer d'autres faits internationaux illicites (intervention, violation de la souveraineté, usage de la force, etc.).
Niveau 3 - Crise	Level 3 High (Orange)	Impact fort et étendu	
Niveau 2 - Incident grave	Level 2 Medium (Yellow)	Impact fort et circonscrit	
Niveau 1B - Incident	Level 1 Low (Green)	Impact significatif et circonscrit	
Niveau 1A - Evénement significatif		Impact faible	
Niveau 0 - Evénement	Level 0 Baseline (White)	Impact négligeable	

Figure 9 : Schéma national français de classement des attaques

Concernant les ingérences numériques étrangères, la France a créé le 13 juillet 2021, toujours à la DGDSN, l'entité VIGINUM dont le rôle est de *« préserver le débat public des manipulations de l'information provenant de l'étranger sur les plateformes numériques. »* [45]. Sa taille est rapidement passé a 42 collaborateurs en septembre 2022 pour une cible à 65 [46].

La définition de l'ingérence étrangère telle que définie pars VIGINUM est la combinaison des 4 points suivants :

- Une atteinte potentielle aux intérêts fondamentaux de la Nation.
- Un contenu manifestement inexact ou trompeur.
- Une diffusion artificielle ou automatisée, massive et délibérée.
- L'implication, directe ou indirecte d'un acteur étranger (étatique, paraétatique ou nonétatique).

La France a beaucoup légiféré et a organisé et fait évoluer ses doctrines de sécurité et son organisation de cyberdéfense. La guerre en Ukraine a pu précipiter des textes, ainsi la version 20242030 de la LPM, présentée le 11 avril 2023 a été rejetée à l'Assemblée nationale en raison de la faiblesse de l'étude d'impact [47,48]. Malgré ce contretemps qui va retarder son application, les budgets octroyés sont considérables puisqu'on parle de 413 milliards d'euros sur 7 ans.

Concernant le sujet de la formation l'ANSSI a adopté un système assez semblable à celui de l'unité 8200 en Israël. Cela consiste à former des personnels aux méthodes de l'agence et à les garder en contrat à durée déterminé pendant 3 à 6 ans pour les voir ensuite rejoindre les entreprises privées pour transmettre les bonnes pratiques de cybersécurité ou fonder des startups [49,50]. Cette méthode d'essaimage a par exemple permis de fonder la société Alsid en 2016, spécialiste de la protection des Active Directory qui est le système clef de beaucoup d'entreprises pour gérer les authentifications et des droits d'accès [51]. La limite de ce système réside dans la capacité pour la France de conserver ses pépites puisque la société américaine Tenable a racheté Alsid en 2021 [52].

Figure 10: Dates clef de la cyberdéfense française depuis 2009

La réponse à incident a été traité en 2021 dans le cadre du plan France Relance où 12 CSIRT régionaux ont été ouverts pour pouvoir traiter les demandes des PME, ETI, collectivités territoriales et associations. Ils ont également un rôle de sensibilisation et de conseil au niveau local.[53]

Il y a peu d'attribution d'attaques, mais en 2009, un outil d'espionnage appelé Babar a été attribué à la DGSE [54]. Un rapport des services canadiens a étudié cette opération de cyber espionnage nommée « Snowglobe ». Ce rapport classifié Top Secret fait partie des la fuite de données Snowden.[55]

La stratégie d'influence se voit dans l'espace européen où la France apporte son savoir-faire et ses méthodes. Quelques exemples illustrent cet état de fait, comme le référentiel PDIS (Prestataire de Détection d'incident de Sécurité) qui inspire le guide pour la mise en place et l'exploitation d'un centre d'opérations de sécurité [56] de l'ETSI. De la même façon, la directive NIS pour les OSE (Opérateur de Services Essentiels) est dérivée des exigences de la Loi de Programmation Militaire (LPM) pour les OIV.

Il est important de garder à l'esprit que la stratégie française s'inscrit également dans le cadre de la stratégie de l'Union européenne.

Israël

Israël a mis en place depuis 2011 une stratégie concernant la cybersécurité. La dernière version date de 2021. Le premier directeur du Bureau National du Cyber israélien, Eviatar Matania, a exposé la genèse de la doctrine [57] de la manière suivante :

Concernant le secteur privé, le premier axe utilisé est le côté réglementaire pour obliger les entreprises à appliquer les bonnes pratiques de cybersécurité. Le second axe porte sur la dimension opérationnelle au travers des guides de bonnes pratiques de cybersécurité que fourni l'Etat.

La doctrine défensive comporte trois strates : la robustesse, la résilience et la protection nationale. La première strate couvre la mise en place des mesures de protection organisationnelles et techniques, la sensibilisation des utilisateurs et le pilotage de la sécurité par la gestion des risques. La seconde strate sur la résilience traite de la capacité de réponse à incident. Dans ce cas, l'Etat peut aider les organisations à recruter les experts nécessaires. En effet, l'Etat intervient en priorité pour traiter les attaques d'autres nations qui visent des infrastructures critiques ou des attaques dont l'ampleur ou le potentiel destructeur sont craints.

La version 2021 de la stratégie de cybersécurité israélienne à l'instar de la doctrine de l'allié Américain documente l'importance de la collaboration avec les autres pays alliés dans la lutte défensive.

La partie opérationnelle y est nettement plus détaillée.

En dehors de la doctrine officielle de défense, de nombreuses actions offensives ou de hack back ont été attribuée à Israël. Il y a par ailleurs également eu un exemple de réponse militaire conventionnelle par un tir de missile sur le bâtiment, dans la bande de Gaza duquel le Hamas menait l'attaque en réponse à une cyber attaque [58]. En dehors de la doctrine officielle de défense, de nombreuses actions offensives ou de hack back ont été attribuées à Israël. Serait attribuée à Israël, la seule réponse militaire conventionnelle *(tir de missile sur un bâtiment sur la Bande de Gaza)* à une cyberattaque du Hamas. [58].

Israël développe sa stratégie de dissuasion par des accords juridiques ou du Hack Back.

La cyberpuissance a été vraiment poussée par l'État qui a encouragé la création de startup dans le domaine de la cybersécurité, la formation, les pôles d'attractivité comme Beer-Shev'a présenté comme la Silicon Valley israélienne. Dans les faits, le pôle principale reste Tel Aviv.

La stratégie pensée en 2012 pour booster les investissements dans le cyber a été un succès. L'Etat a priorisé les investissements dans les startups liées à la cybersécurité.

En investissant 22,5 millions de dollars sur deux ans sur une dizaine d'entreprises, l'impulsion était donnée [57]. Cette dynamique a également attiré les capitaux étrangers dont l'allié Américain qui voit d'un mauvais œil les capitaux chinois arriver également en Israël.

L'unité de renseignement militaire cyber est l'unité 8200. Elle est suspectée par plusieurs médias d'activités de sabotages ou d'espionnage du projet de nucléaire iranien.

Le tissu de startup en Israël bénéficie de la stratégie de formation du pays, d'une part par les universités, notamment l'université Ben Gourion de Beer-Shev'a et d'autre part via le service militaire obligatoire notamment dans l'unité 8200 où les cybers combattants formés se retrouvent dans les startup [59]. La particularité est que contrairement au service national qui est de 3 ans, dans l'unité 8200, il est de 5 ans.

Les autres pays

Depuis au moins une quinzaine d'années, beaucoup de pays ont intégré l'importance d'établir une stratégie ou un modèle de défense cyber. Ce sous-chapitre évoque de manière très succincte les principales directions prises par ces pays.

Deux pays sont dans la même optique de contrôle et de fermeture de l'internet, il s'agit de l'Iran et de la Corée du Nord. L'Iran est aguerrie au conflit cyber avec dans la région, le conflit avec Israël. La Corée du Nord est plutôt connue pour ses attaques cybercriminelles ayant permis de rançonner ou de voler des cryptomonnaies.

Dans les lignées des Etats-Unis, l'Australie, le Canada, le Royaume-Uni et la Nouvelle-Zélande constitue les « Five Eyes » qui sont un accord entre service de renseignement concernant la collecte de renseignements électromagnétiques appelé SIGINT. En dehors de cet accord de partage de renseignements chaque pays a une stratégie qui lui est propre.

L'Inde mise sur Internet pour sa croissance économique, le développement de sa puissance cyber est donc mise au premier plan. Elle partage des objectifs communs avec la France par le biais d'une feuille de route commune sur la cybersécurité et le numérique [60].

L'Estonie est un pays qui a subi plusieurs attaques, en 1995 pour un vol de données et en 2007 par du déni de service. Le pays s'est donc mis en position de pouvoir se protéger des attaques redoutées de groupes pro-russes. Il est décrit comme un pionnier de la cybersécurité *(ce sujet sera développé dans la troisième partie)* [61].

L'Union européenne a une stratégie supranationale. Celle-ci porte sur trois domaines :

- Résilience, souveraineté technologique et leadership ;
- Capacité opérationnelle de prévenir, de dissuader et d'intervenir ; Coopération pour promouvoir un cyberespace mondial et ouvert.

Cette stratégie est soutenue par un budget qui a quadruplé par rapport au précèdent [62].

L'Europe a également contraint les acteurs du numérique à faire monter leur niveau de sécurité, notamment par :

- Le Règlement Général sur la Protection des Donnée (RGPD) de 2016 qui s'applique à toutes les sociétés qui traitent des données personnelles de citoyens européens.
- La directive Network and Information Security (NIS) qui doit être transposée dans le droit local des pays membres.

LES RISQUES DU CYBERESPACE

Les différentes stratégies et les procédés militaires traditionnels ne sont pas mis en opposition aux affrontements possibles dans le cyberespace mais il est question d'en appréhender leur complémentarité. Le cyberespace est devenu ces dernières années un espace de lutte et de rapports de force entre nations. De quoi est-il composé et quelles sont les menaces possibles ?

Depuis les années 2000, le terme cyberespace est réapparu dans beaucoup de discours des Etats. On le retrouve dans les doctrines militaires *(comme précisé en partie I)* ou dans les négociations internationales. Considéré comme un territoire, il est devenu un espace à conquérir, à contrôler ou à surveiller.

Cet espace même s'il évoque un monde « virtuel », est composé de trois « macro-couches interdépendantes » dont la première est considérée comme la couche physique : des matériels tangibles.

Elle s'articule autour d'infrastructures permettant d'établir un réseau de connectivité :

- Les câbles sous-marins et terrestres.
- Les satellites.
- Les datacenters.
- Les points d'échanges.
- Les objets connectés.
- Les serveurs.
- Les ordinateurs.

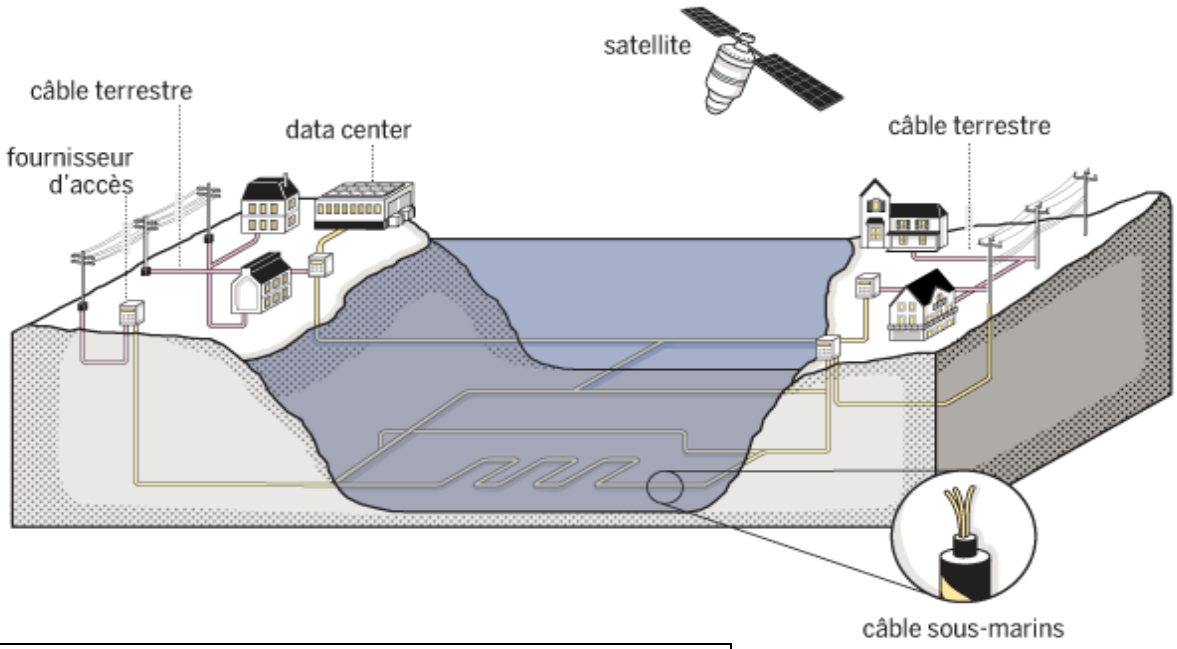
La seconde est la couche logique : ce sont les protocoles, langages, systèmes d'information, etc.

La troisième représente la couche sémantique (psycho-cognitive), correspondant à l'ensemble des applications en contact avec les utilisateurs. C'est la couche des dimensions sociale et informationnelle.

Cet espace est ainsi devenu une dimension supplémentaire de la guerre conventionnelle et est devenue une cible, avec les risques qui en découlent. La guerre en Ukraine en est un exemple : les 3 macros-couches du cyberespace sont devenues des angles d'attaque pour les stratégies militaires des Etats. Avant de débuter les affrontements conventionnels contre l'Ukraine, la Russie s'est attaquée aux infrastructures (couche basse physique) pour couper la connectivité ou au moins la rendre plus difficile.

La seconde couche - la couche logique - aurait été également touchée avec le changement de direction du réseau Ukrainien vers la Russie sur son propre réseau pour récupérer l'ensemble des données [63]. Cette méthode utilisée est le reroutage des données. La dernière couche - la couche sémantique - a été altérée avec la diffusion par le gouvernement russe d'informations pour justifier son invasion. Ces différents cas seront détaillés par la suite.

INFRASTRUCTURES PHYSIQUES DU CYBERESPACE A MAITRISER



Source : Monde la Guerre mondiale des données colloque international « cartographie du cyberespace », organisé en mars

Figure 11: Réseau physique du cyberespace

Les câbles sous-marins de communication

Les Etats sont de plus en plus gourmands en bande passante : réseaux 5G, streaming vidéo en ultra-haute définition, objets connectés, « machine to machine » (M2M), transactions financières à haute fréquence. Cela devrait avoir une tendance à la hausse avec toutes les nouvelles applications en temps réel : la réalité virtuelle, la réalité augmentée ou les voitures autonomes etc. Pour la période 2018-2022, la capacité de transmission des fibres sous-marine a augmenté de 13,3% sur les axes majeurs. Sur la base des données communiquées et des estimations futures, la capacité mondiale devrait augmenter de 75,4% d'ici la fin 2025 [64].

Cette dépendance au réseau international est en majorité liée aux câbles sous-marin, support de l'interconnexion.

Le réseau internet est composé par les câbles sous-marin de communication et sont une cible de choix d'actions hostiles depuis leur construction et mise en service.

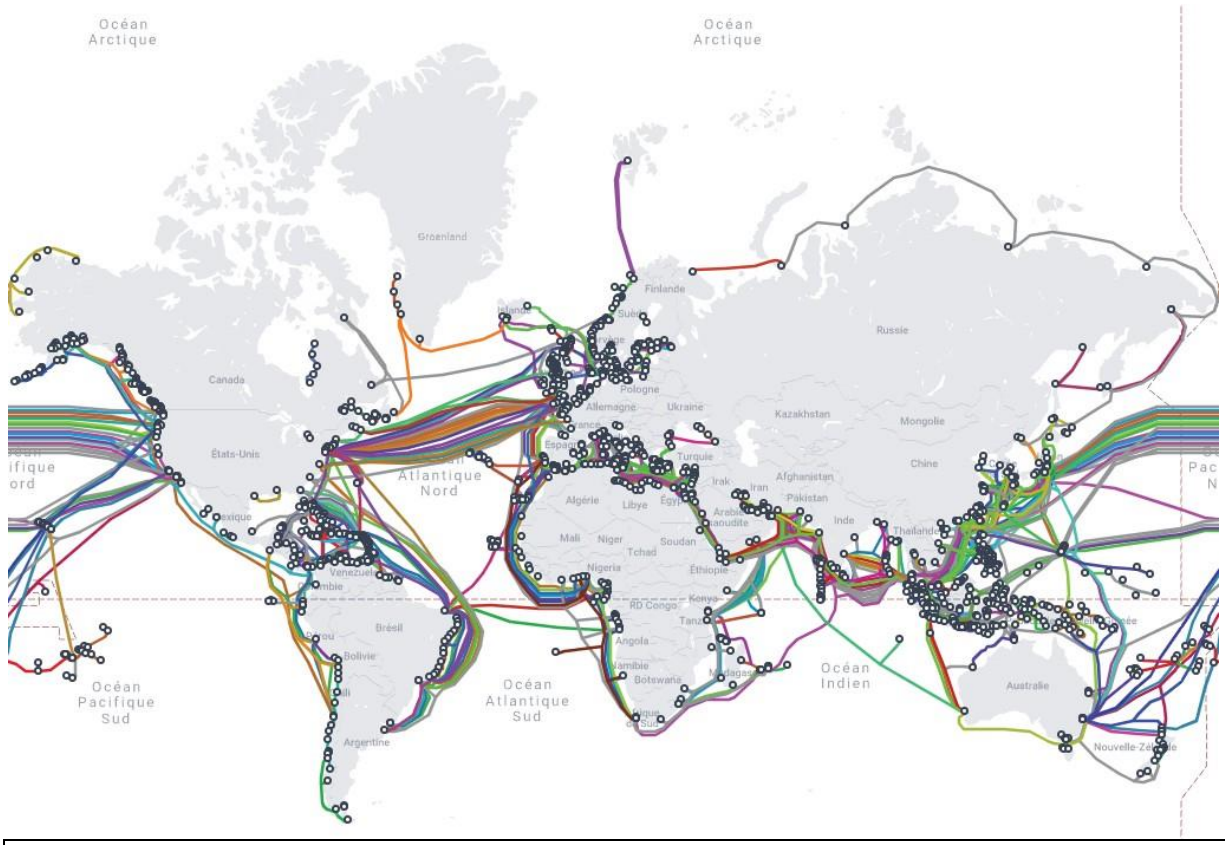
Le numérique sous mers et océans

Figure 12 : La huitième merveille du monde : Le câble de l'Atlantique.

Le câble sous-marin se définit selon l'Union internationale de Télécommunication (IUT) est l'Organisation des Nations Unies en charge des technologies de l'Information et de la Communication) comme "un câble posé dans le fond marin, ou ensouillé à faible profondeur, destiné à acheminer des communications". Ces infrastructures ne sont pas récentes. Le premier câble télégraphique sous-marin a été posé en 1850 dans la Manche [65]. Huit ans plus tard, apparaitra le premier câble transatlantique. Il sert depuis ses origines à la transmission d'information entre des territoires séparés par les eaux. La technologie utilisée à date est la fibre optique et permet la transmission de données internet ("la data") et les appels téléphoniques. En effet, dans les années 1980, le coaxial a atteint ses limites, or les demandes ne cessent de croître ; on assiste alors au développement des câbles à fibre optique dont le conducteur est du verre très pur *(appelé silice)*, c'est la nouvelle génération de câble. Le 1er câble transatlantique de ce type fût posé en 1988. Le signal qui parcourt la fibre optique, la lumière, perd de sa force et doit régulièrement être restauré à intervalles de 50 à 80 kilomètres. Cela nécessite l'installation de répéteurs qui doivent être alimentés par de l'électricité à haute tension.

Des composants terrestres qui sont la station d'atterrissement, la chambre plage et la partie terrestre du câble sont indispensables également pour la circulation et la distribution des données internationales. Un câble n'est pas plus gros qu'un tuyau d'arrosage selon Geoffroy De Dinechin, directeur opérationnel d'Orange Marine.

En avril 2023, plus de 98% des flux de données intercontinentales sont transportés par les mers et les océans via les câbles sous-marins. Début 2023, il y a environ 553 câbles sous-marins de fibres optiques et 1 306 atterrissages en service ou en cours de construction [66]. Cela représente plus de 1,3 millions de kilomètres de réseau de câbles. Le plus long câble "2africa" avec ses 45 000 km *(taille de la circonférence de la Terre)* est en cours de déploiement. Sa mise en ligne est prévue en 2024 [67]. Ils sont repartis sur l'ensemble de la Terre de manière hétérogène, cette immense toile permet d'avoir un réseau de communication mondiale en connectant plus de 4 milliards de personnes. La localisation de ces autoroutes de l'information peut être connue si les propriétaires en ont donné le trajet exact en sources ouvertes. Si ce n'est pas le cas, les sites qui répertorient l'ensemble des câbles estiment le parcours effectué entre chaque zone d'atterrissage. Seules les entités détenant les systèmes d'exploitation, de surveillance et de maintenance ont une vision globale de l'emplacement de ces infrastructures et possèdent ainsi la cartographie complète et précise [68].



source : www.submarinecablemap.com

Figure 13: Carte des câbles sous-marins 2023

Actifs stratégiques primordiaux

Le réseau internet est essentiel à l'organisation sociale mondiale. La majorité de nos activités quotidiennes, que ce soient nos transactions financières, nos envois de courriel professionnels, nos communications personnelles ou l'accès au stockage de nos informations dans le cloud nécessitent internet. Plusieurs serveurs situés dans différents pays sont en communication pour ces échanges de données. Que ces pays soient séparés ou non par une mer ou un océan, il y a une très grande **.** probabilité que le chemin utilisé transite par un câble sous-marin. L'évaluation la plus récente par des représentants de la Commission Fédérale des Communications américaines *(FCC)* chiffrait à environ 10 000 milliards de dollars de valeurs transactionnelles globales du trafic en 2016 circulant sur le réseau des câbles sous-marin [69]. Ce montant est revu à la hausse chaque année mais il est difficilement quantifiable car aucun organisme n'est dans la possibilité de compiler l'ensemble des données et la valeur des transactions. Seules des estimations sont données. Ces infrastructures sont des actifs indispensables à différents secteurs stratégiques tel que la finance internationale ou le monde militaire. Le secteur bancaire, pierre angulaire de nos économies, est l'un des principaux clients des opérateurs de câbles. C'est par exemple le cas du principal système d'échanges de la finance mondiale de la Society for Worldwide Interbank Financial Télécommunications *(SWIFT)* qui dépend de la vitesse de ces câbles à fibre optique. Le volume de données transporté d'ici 2025 devrait ainsi être multiplié par 60, avec pour objectif d'améliorer le niveau de sécurisation (redondance et chiffrage des données selon les

demandes) et de résilience des réseaux [70]. Par ailleurs, les câbles sous-marins sont des instruments de développement économique. L'arrivée des bandes passantes internationales dans les pays d'Afrique subsaharienne a permis par exemple de réduire la fracture numérique de la région et accompagner le développement économique et sociale. En effet, les usages des TIC par les individus et les entreprises croissent et favorisent la productivité et l'arrivée d'investisseurs étrangers.

Acteurs de l'écosystème

Ces actifs sont stratégiques et des enjeux économiques majeurs sont associés à la fabrication, la pose, le contrôle et la maintenance de ces câbles. Une multitude d'acteurs sont impliqués dans les câbles sous-marins de communication.
Il existe plusieurs parties prenantes toutefois le nombre est réduit :

Les fabricants ;

Ce sont les acteurs les plus critiques, ils possèdent un savoir-faire essentiel au système de fonctionnement des câbles sous-marins. Les acteurs principaux sur ce marché [64] sont TE SUBCOM (Etats Unis), Alcatel Submarine Network (ASN, sous le bastion Finlandais depuis 2015 mais basé en France), NEC(Japon), et HMN technologies (Chine). Le secteur est ainsi détenu par quelques acteurs, et de fait en par quelques Etats. Les trois premiers sont issus d'entreprises historiques, la Chine est en plein essor sur le marché [71]. Sur les quatre dernières années (2018-2022), le chinois HMN technologies a produit autant de câbles que l'américain (13) mais reste loin derrière l'européen ASN (22) [64]. TE SUBCOM reste l'acteur principal en nombre de kilomètres déployés.

La croissance de ce nouvel acteur chinois dans le paysage des câbles n'est pas vu par les Britanniques et les Etasuniens d'un bon œil. Le moyen le plus simple d'espionner l'ensemble des flux de donnés transitant par les câbles sous-marins est lors de leur fabrication en posant du matériel complémentaire.

Les poseurs et maintenance

Des navires propres à ce savoir technique doivent être détenus pour effectuer cette activité. Il s'agit donc d'armateurs qui sont également en nombre réduit sur ce secteur [68], les principaux sont :TE SUBCOM *(Etats Unis),* Alcatel Submarine Networks Marine *(actionnaire Finlandais mais basé en France),* Orange Marine *(France),* Global Marine Systems Ltd *(UK),*E marine *(France)…*

Les propriétaires détenteur du contrôle des câbles

Ils sont traditionnellement des opérateurs de télécommunications *(internet backbone providers)* qui se regroupent en consortium pour effectuer un investissement en commun dans un câble sous-marin et ainsi répartir les coûts de construction et d'exploitation. Ils disposent ainsi de la copropriété. Parmi les principaux opérateurs on peut citer les Américains AT&T et Verizon, les Britanniques Vodafone & BT groupe, le français Orange, l'indien Tata & communication et les Chinois Chine Télécom & PCCW.

Nouveaux acteurs du marché : entrée des "GAFAM"

Cette infrastructure physique est en cours de changement de main. En effet, depuis 2010, les "géants d'internet", autres noms donnés pour les GAFAM, sont entrés sur le marché. L'objectif premier de ces

entités pour l'entrée dans des consortiums de copropriété de construction de câbles sous-marins est purement économique. Leur besoin grandissant de capacité de transmission *(multiplié par 9 entre 2015 et 2019)* a changé leur modèle économique [71]. Ils sont passés d'acheteur de capacité à propriétaire de câble. "Bientôt, 95 % des capacités de communication transatlantiques seront contrôlées par les GAFAM ", soulignait Jean-Luc Vuillemin, vice-président exécutif d'Orange International Networks, Infrastructures & Services lors de notre entretien. Ils obtiennent ainsi une maîtrise complète du processus de transmission : relier le plus directement et rapidement possible leurs datas centers et choisir la route des flux. Ils cherchent également une redondance systématique dans leur capacité de transmission ce qui les pousse à investir dans de nombreux câbles avec des trajets qui ne sont pas forcément ceux suivis habituellement. Cette résilience leur permettra d'effectuer le reroutage du trafic en cas de panne d'un câble. Ils pourront ainsi ne pas demander une maintenance express aux navires câbliers.

« Avec la prédominance des acteurs privés, peut-on aboutir à une forme de monopole des GAFAM sur les câbles sous-marins ? Ils ont des moyens financiers considérables pour façonner l'Internet », s'inquiétait pour sa part Camille Morel, chercheuse au Centre lyonnais d'études de sécurité internationale et de défense *(CLESID)*, lors d'un rendez-vous inCyber en janvier 2021. Internet à travers les câbles sous-marins est le prolongement des luttes de pouvoirs existantes de l'impérialisme américain

Internet est le prolongement des luttes de pouvoir existantes, dans une autre dimension.

Vulnérabilité & Résilience

Les câbles sous-marins ont été conçus pour être résilients mais se révèlent avoir des vulnérabilités. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.

Deux types d'attaques peuvent être effectuées sur les câbles sous-marins de communication :

Le sabotage

Pour effectuer un acte de sabotage sur un câble sous-marins, il faut le sectionner de manière volontaire afin d'empêcher les communications. Cette menace n'est pas récente. En effet, depuis la première pose de cette infrastructure le risque est présent. Pendant la Guerre américano-espagnole de 1898, les Américains coupèrent les câbles télégraphiques entre l'Espagne et ses territoires transatlantiques. Pendant la Première Guerre mondiale, une des premières décisions de la GrandeBretagne fut de couper les câbles allemands, privant l'Allemagne de communication. Une guerre des câbles s'en est suivie car l'Allemagne a répliqué en s'attaquant aux stations télégraphiques britanniques dans les océans Pacifique et Indien.

Aujourd'hui, en plus des aspects stratégiques et militaires de la circulation de l'information, il y aurait surtout un impact économique majeur.

A date, le réseau internet sous les mers connait en moyenne une centaine de coupures *(câbles sectionnés)* par an [72].

Cela est dû pour plus de la moitié des cas à des accrochages d'encre ou de filets de pêche. La nature peut également être responsable de coupures comme les séismes sous-marins, les tsunamis et les éruptions volcaniques [73]. Les changements climatiques entraîneront des conséquences dans le futur dû à la hausse du niveau de la mer et donc aux risques de submersions des zones d'atterrissage des câbles sur les littoraux mais ici on se concentrera sur les menaces liées aux actes malveillants.

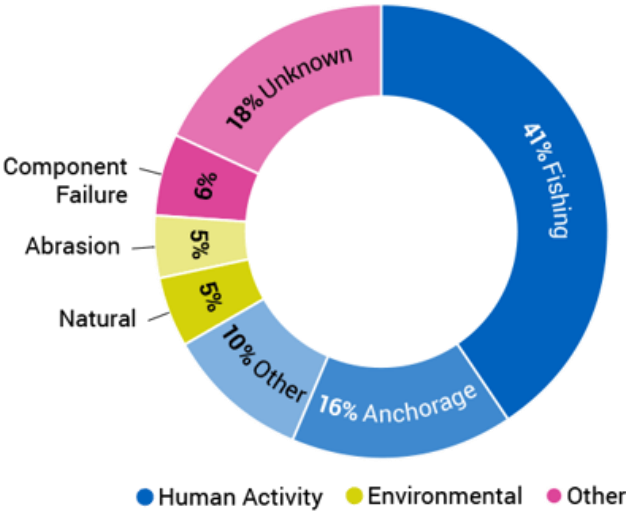


Figure 14: Origine des dommages causés sur les câbles sous-marins

Si dans la majorité des cas les coupures sont involontaires, des actes de malveillances peuvent être commis. Comme constaté sur le graphique de la figure n°14 ci-dessus, 18% des actes sont d'origine inconnue, dont on n'a pas pu déterminer la cause.

Le plus simple pour effectuer un acte de sabotage sur un câble sous-marins est d'effectuer un acte de malveillance près du littoral, certes la partie la plus protégée et en visibilité car proche des côtes mais la plus facile à atteindre, la moins immergée. Trois plongeurs ont été accusés d'avoir coupé un câble sous-marin SMW-4 au large d'Alexandrie reliant Marseille à Singapour [74]. Plusieurs pays qui sont dans le consortium de ce câble auraient été touchés par cette coupure et ont subi des impacts financiers.

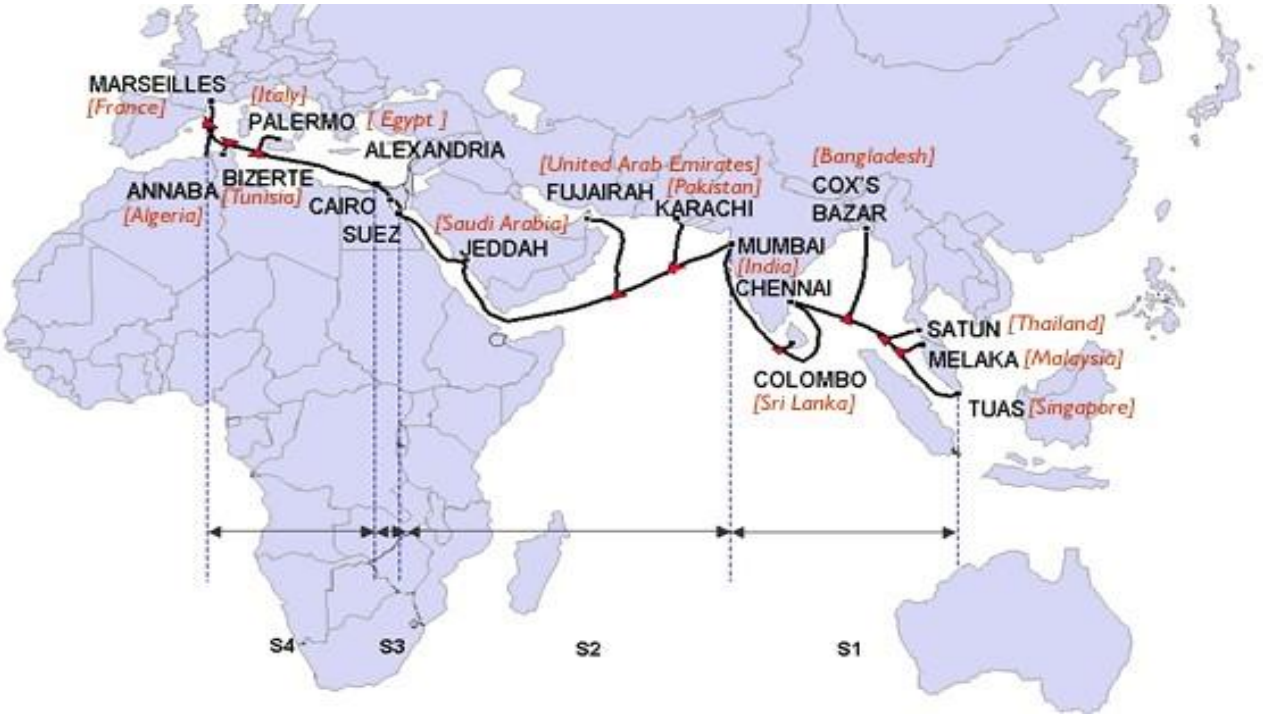


Figure 15 : du tracé du câble sous-marins SMW-4 reliant Marseille à Singapour

Selon Geoffroy de Dinechin, directeur opérationnel d'Orange Marine, les actes de sabotage en grandes profondeurs s'avèrent être une opération complexe à mettre en œuvre et il faut disposer de l'équipement nécessaire.

L'impact d'une coupure de câble n'est pas le même d'un pays à l'autre. La résilience dépendra ainsi de la capacité à dévier le trafic sur d'autres câbles sous-marins ou d'utiliser d'autres moyens de transfert du trafic comme les satellites ou les interconnections terrestres. Les méthodes et les délais de réparation en cas d'entaille des câbles et la technologie utilisée pour limiter les dommages se sont raccourcis au cours du temps [64] .

Ainsi plus un Etat est relié à des câbles sous-marins, moins sont les risques de placer tout le pays dans le noir numérique. A titre d'exemple, pour rendre très difficile la connectivité sur le territoire français, il faudrait en simultané la coupure d'au moins trois de ces câbles atterrissant sur ces côtes, manœuvre possible mais à effectuer. Pour déstabiliser le territoire français, il faudrait s'attaquer à ses territoires plus isolés qu'est l'île de la Réunion par exemple. Elle ne dispose que deux câbles sous-marins pour sa connectivité internationale. Les actes de sabotage en concomitance sur cette infrastructure physique *(plus aucune lumière)* rentreraient dans le spectre de la guerre conventionnelle et les intentions seraient connues ainsi que le belligérant. On pourrait immédiatement repérer le lieu de la coupure et on connaitrait facilement la nationalité du bâtiment impliqué [75].

Les craintes sur les coupures ont été amplifiées après le sabotage des gazoducs Nord Stream 1 & 2 le 16 septembre 2022 en mer baltique [76]. Les impacts sur cette infrastructure gazière certes en mer ne sont pas les mêmes. En effet, le temps de réparation ne se compte pas en jour mais en années pour une remise en marche. La prospective de sabotage réalisée sur cette infrastructure doit être relativisée : les atteintes volontaires au réseau sous-marin restent rares, si l'on regarde l'ensemble des dommages causés au quotidien. [68,70,75].

Si des actions traditionnelles peuvent encore avoir *lieu (coupure de câble, bombardement de stations, actions de renseignements, censures...)*, le système de contrôle et de gestion des réseaux des câbles sous-marins à distance peut être piraté.

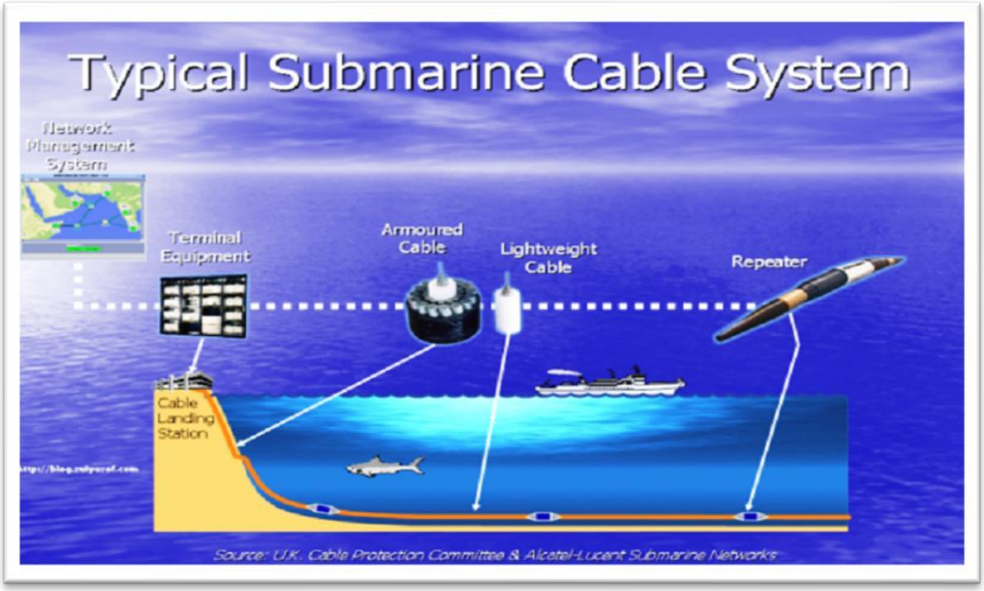


Figure 16: Schéma du système de gestion des câbles sous-marin de communication.

En raison de leur longueur, la majorité des câbles sont équipés de systèmes de surveillance des défaillances et de trafic qui peuvent détecter les ruptures de câble ou les points d'endommagement en vue d'une réparation *(ralentissement de la vitesse du trafic, arrêt de la lumière, problème sur les répéteurs)* comme indiqué sur la figure ci-dessus.

Cette interface d'administration peut être piratée et ainsi aboutir à une perturbation des flux de données, un arrêt du trafic ou un dysfonctionnement dans la détection des dommages.

La gestion du management des câbles est effectuée par plusieurs acteurs sur la majorité des infrastructures. En effet, ces derniers peuvent transiter sur plusieurs stations d'atterrissement. Plusieurs unités de branchement peuvent donc être présentes et la gestion de l'exploitation partagée avec tous les acteurs des consortiums. Cela multiplie ainsi les risques de piratage car les politiques de sécurité ne sont pas identiques pour l'ensemble des exploitants.

L'espionnage

Sur cette infrastructure matérielle pèse le risque immatériel de la captation de données. L'espionnage désigne la collecte clandestine d'informations secrètes, activité relevant du domaine du renseignement.

Ce type d'attaque n'est pas nouveau, il a été mis sur le devant de la scène avec les révélations d'Edward Snowden. Cet ex-consultant de la CIA, a rapporté dans la presse en juin 2013 [77], les moyens déployés en cybersurveillance à grande échelle par les agences gouvernementales américaines, que sont la CIA et la NSA, et le service de renseignement britannique CGHQ. Deux programmes ont été révélés, PRISM *(Planning tool for Resource, Integration, Synchronization and Management)*, aux Etats Unis et Tempora, au Royaume-Uni.

Ces derniers ont eu pour objectif, conjointement entre les deux pays, de collecter massivement des données en se « branchant » sur les câbles sous-marins à partir des stations d'atterrissement sur le territoire britannique. Cela comprenait plus de deux-cents câbles [78].

L'espionnage tiré de l'ensemble des câbles sous-marins mondiaux est un atout énorme, l'accès à toutes ces métadonnées [79], fait de la donnée, une donnée rare et stratégique.

Les dispositifs installés sur les câbles ont été faits sur les stations de contrôle où atterrissent les câbles sous-marins, passage obligatoire du flux de communication. La méthode utilisée sur les câbles est la méthode « Upsteam », c'est à dire lors du transit des données à la différence de la méthode « Downstream » dont la captation se faire sur les serveurs de stockage des entreprises [78].

Cette captation de la donnée sur les câbles sous-marins peut se faire aisément, il est très difficile d'être détecté par des tiers si la station est située sur le territoire nationale mais encore faut-il disposer de moyens de stockage et de traitements des métadonnées. Certains pays permettent cet espionnage avec l'aide des exploitants des câbles ou non dans le cadre du renseignement de la sécurité intérieure. Les Américains et les Britanniques, ne sont pas les seuls à opérer sur ces infrastructures pour du renseignement et sous couvert de la sécurité intérieure, la France [80] ou encore la Nouvelle-Zélande [81] y ont également procédé.

Cette opération de renseignement est beaucoup moins aisée à effectuer avec un espionnage en pleine mer et fait souvent l'objet de beaucoup de fantasmes dans les médias. Plus discret car les moyens sont sous-marins et avec un cadre juridique plus permissif car dans les eaux internationales mais sa mise en œuvre est complexe. Des drones sous-marins ou des navires sous-marins sont nécessaires et dans la

capacité de stocker un nombre conséquent de données captées. L'ensemble des flux présents dans la lumière de la fibre sera récupéré, aucun filtre n'est possible à ce stade. La coupure d'un câble en plein mer peut être effectuée par beaucoup d'acteurs mais l'espionnage n'est pas l'apanage de tous. Il faut disposer des moyens nécessaires exigés : une technologie et un savoir-faire élevés. Seul un Etat puissant peut avoir cette capacité.

L'ensemble de ces risques sur les câbles sont possible sur n'importe quelles zones de l'immense toile de ce réseau. D'autres éléments peuvent rentrer également en jeu : Le pays de provenance de l'exploitant et les lieux des zones d'atterrissement sur les risques probables sur ce secteur en croissance.

Conflits sur cet espace

Depuis l'ère de la télégraphie, les Etats ont pour ambition d'installer des lignes sous-marines propres, de surveiller le contenu qui y transite, de les cibler d'un point de vue militaire ou de les réguler. Les câbles sous-marins sont assujettis à une protection du droit international insatisfaisante. Ils sont encadrés par la convention des Nations Unies sur le droit à la Mer (CNDUM) de 1982.

Ce texte est basé en partie sur des éléments de plusieurs autres textes dont la convention internationale sur la protection des câbles sous-marins de 1884 et des conventions de Genève de 1958 sur le droit de la mer. Si tous les Etats peuvent immerger des câbles sous-marins librement sur le lit de la haute mer, des demandes d'autorisations doivent être effectuées pour la mer territoriale, régies par les lois nationales pays d'atterrissement.

- Le sujet des câbles sous-marins est ainsi discuté dans diverses organisations multilatérales. Ainsi les perspectives de défense ont été évoquées par les pays membres de l'OTAN *(Organisation du Traité de l'Atlantique Nord)*. En 2010, elle publiait un document de prospective indiquant que la prochaine attaque significative contre l'alliance serait sur un câble sous-marin de communication à fibre optique [82]. Depuis 2017, les déclarations et textes se sont multipliés :
- 2018 : Renforcement du commandement allié sur les voies de communications maritimes transatlantiques [83]
- 2019 : Lors d'une conférence de presse, le secrétaire général de l'OTAN, Jean Stoltenberg soulignait le besoin de renforcer la résilience des infrastructures critiques que sont les câbles sous-marins, les satellites et la 5G. La CCDCOE *(Cooperative Cyber Defense Centre of Excellence de l'OTAN)* publiait une étude sur l'importance stratégique et la dépendance aux câbles sousmarins de communication [84]
- 2020 : Le conseil de l'OTAN en octobre, réuni avec l'ensemble des ministres de la défense des pays membres a mis à l'agenda la question de la protection des infrastructures
- 2023 : Le secrétaire général, M. Jens Stoltenberg, a annoncé le 15 février 2023, la création d'une cellule de coordination des infrastructures sous-marines critiques au siège de l'OTAN [85]

Au niveau de l'Union Européenne, c'est sous l'angle de la souveraineté numérique et de résilience des infrastructures critiques que le sujet a été porté. Que ce soit lors de la présidence portugaise en 2021, avec la signature de la déclaration commune pour l'amélioration de la connectivité globale en Europe *("Data Gateway")* ou sous la présidence française en 2022 avec la discussion sur la résilience des

infrastructures critiques et réseaux de communications en Europe, que le sujet concernant les risques portés par les câbles sous-marins a été traité.

C'est surtout sur le plan national que les Etats ont pour objectif de renforcer la protection des câbles sous-marins et ainsi à améliorer leur résilience numérique.

Divers leviers peuvent être activés :

- Nouvelles réglementations et procédures administratives relatives à la technologie sous-marine.
- Soutien financier des entreprises dans le secteur d'activité.
- Augmenter les échanges avec l'industrie.
- Développer des capacités d'action sur le réseau et le contenu.
- Coopération avec d'autres Etats.

Une guerre hybride sino-étasunienne [86]

Les Etats Unis sont les pionniers pour activer les leviers précisés ci-dessus. La coupure en 2008, de plusieurs câbles au large de l'Egypte a été un élément déclencheur. En effet, cet événement a eu un impact sur les transmissions d'informations militaires depuis des points d'opérations américains [87]. Différents outils sont ainsi mis en place. En 2008, il y a la mise en place d'un groupe de travail appelé "Team Telecom" qui étudie sous l'angle de la sécurité nationale, l'ensemble des demandes de licences déposées par des acteurs étrangers pour l'exploitation des câbles sous-marins sur les territoires américains par la FCC (Commission Fédérale des communications). Comme pour la partie mobile des télécommunications, la 5G [86], les Etats unis se sont alarmés du développement du rôle joué par des entreprises chinoises dans le secteur des câbles sous-marins [88]. Concernant la Chine, c'est le ministère de l'Industrie, de l'Information et de la Technologie (MIIT) qui régule les activités numériques chinoises mais ne joue pas dans la même cour que la FCC.

La Chine a récemment reconnu le rôle important des câbles sous-marins pour le développement de son économie nationale. Le rôle stratégique du numérique et des câbles sous-marins sont évoqués dans les documents de la stratégie chinoise sur les nouvelles routes de la soie (BRI, Belt and Road Initiative). Comme le résume Jean-Luc Vuillemin « Si demain matin tous les câbles sous-marins qui relient la Chine au reste du monde sont coupés, pour 99% de la population chinoise, il ne se passera rien du tout ». Dans la poursuite de cette guerre économique et technologique contre les Etats-Unis sur ce secteur, le déploiement d'un nouveau câble sous-marin est en projet reliant l'Asie, l'Afrique et l'Europe, 100% chinois (fabricants & poseurs et exploitants). Cette aspiration est apparue après l'éviction d'acteurs chinois d'un projet similaire par les Etats-Unis [89].

Les Routes de la Soie

Théâtre des tensions diplomatiques entre la Chine & les Etats-Unis

La chine a pour objectif de se (re)tourner vers l'Ouest en restructurant des liaisons eurasiatiques en passant par le cœur du continent. Ces routes sont terrestres (routiers, ferroviaires), maritimes et également numériques, elles veulent bousculer l'ordre établi. Ses ambitions d'investissements pour l'écriture d'une nouvelle histoire du monde et le storytelling orchestré par l'empire du Milieu est en parfait accord avec la notion de connectivité mais également avec sa stratégie économique et commerciale actuelle.

Cette politique numérique répond à plusieurs objectifs :

- Être le leader mondial dans le secteur des équipements des infrastructures numériques (câbles sous-marins, 5G …)
- Centralisation des infrastructures numériques asiatiques et mondiales davantage sur la Chine (pierre angulaire)
- S'imposer en influençant sur les standards et normes technologiques et notamment ceux du cyberespace
- Influence sur le discours mondial
- Développement du e-commerce et des technologies
- financières
- Accès aux données étrangères par le biais de ses grandes entreprises internationales

Sur le plan intérieur, le rêve des Chinois est de dominer les technologies du futur avec leur programme « ***Made in China 2025*** » (quantiques, les voitures sans conducteur et l'intelligence artificielle...).

Il est donc incontournable que ce projet représente, entre autres, un instrument d'opposition à l'impérialisme étasunien, toujours plus important dans la région et dans le monde.

Le gouvernement américain identifie trois risques avec cette nouvelle stratégie chinoise :

Cybersécurité

En étant acteur dans la construction et l'opération des câbles sous-marins, cela faciliterait la captation et la surveillance des flux d'information transitant par ces derniers ainsi que le risque de DDOS, le déni d'accès au service. Comme vu précédemment, c'est lors du processus de fabrication ou d'installation que des équipements permettant le piratage de ces câbles peuvent être installés. Une coupure des flux est également possible par l'exploitant.

A ce jour, il n'y a aucun cas documenté à la connaissance du grand public de mise en place d'équipement espion ou de futur sabotage dans les équipements de communication des entreprises chinoises. Le risque porté en prenant comme fabricants ou poseurs de câbles les Chinois n'est pas plus grand que le choix se portant pour les Etats Unis.

Dépendance

Le développement de la Chine sur le secteur en tant que propriétaire des câbles peut aboutir à la dépendance de certains Etats pour le transfert de certains flux de données sensibles et stratégiques et remettre en question la sécurité intérieure des Etats européens.

Double usage

Ces autoroutes sous-marines présentes dans de nombreuses mers et océans donnent la possibilité de placer des capteurs autres qu'à usage de communication. Le déploiement de ces outils complémentaires permettrait une observation des fonds marins au profit du gouvernement chinois.

Ces inquiétudes sont amplifiées par les relations entre l'armée, l'Etat et les sociétés privées du secteur. Ces risques ne sont pas différents de ceux rencontrés par le poids des Etats Unis dans cette industrie. Prenant pleinement conscience du risque de remise en cause de sa suprématie dans ce secteur, les Etats Unis déploient une politique de sécurisation des réseaux sous-marins :

- Restriction de l'accès aux entreprises chinoises à leur territoire pour les nouveaux projets commerciaux comme vu précédemment avec la FCC.
- Influence sur leurs alliés pour les sensibiliser aux risques identifiés par le gouvernement à recourir aux sociétés chinoises en établissant des rapports officiels publiés *(France, Japon, Royaume Unis, Australie...)* [71].
- Financement de projets alternatifs pour contrer l'influence chinoise [90]
- Acquisition d'actifs et d'entreprises dans le secteur du numérique en Europe [91]

Menace ou psychose russe ?

La Russie est revenue souvent dans les discussions au sein de l'OTAN depuis 2014, sur les risques qu'elle pourrait porter aux infrastructures numériques et plus particulièrement aux câbles sous-marins. "Nous constatons aujourd'hui une activité sous-marine russe à proximité des câbles sous-marins que nous n'avons, je crois, jamais vue", a déclaré au Washington Post le contre-amiral Andrew Lennon, commandant des forces sous-marines de l'OTAN. « La Russie s'intéresse clairement à l'infrastructure sous-marine de l'OTAN et des pays de l'OTAN » [92]. Il mentionne la présence répétée de bâtiments à proximité des câbles, et plus particulièrement le navire océanographique Yantar, exploité par le ministère de la Défense russe. Ce pavillon a été repéré dans l'atlantique Nord, près du Golfe de

Gascogne et le long des côtes américaines en 2015, à proximité des zones de passage de câble reliant la Syrie sans en identifier la cause en 2016. Ces dernières années, il a été identifié à plusieurs reprises au large des côtes françaises et irlandaises.

La Russie est reliée par un nombre faible de câbles sous-marins et n'est pas représentée dans l'industrie. Alors que, comme souligné dans différents discours du président Vladimir Poutine et de ses généraux, le contrôle des flux d'information est un enjeu important dans la maîtrise des conflits [93]. Lors de l'annexion de la région de la Crimée en mars 2014, la Russie a procédé à la coupure des communications internationales de cette zone ukrainienne [94]. La Russie a par ailleurs réitéré l'opération dans l'espace numérique lors de l'invasion en Ukraine en mars 2022 et mis à mal ainsi les communications internationales des occidentaux.

Ces actions offensives sont couplées avec des actions défensives. Comme décrit en partie 1 de ce mémoire, une loi votée en 2019 a pour objectif de tout mettre en œuvre pour isoler l'Etat russe de l'internet mondial et parvenir à entrer dans une souveraineté numérique. Cela leur permettrait d'agir sur les câbles sans crainte d'être impacté en cas de conflit et ne plus être dépendant de ce système numérique transnational. Cela pourrait présager des actions au long court sur les câbles sous-marins avec les repérages actuels. La crainte de certains exploitants ce serait la pause d'objets permettant la dégradation simultanée de plusieurs routes à distance.

Position de la France

Ce conflit sino-américain a mis en lumière la vulnérabilité de l'Europe et par conséquent de la France qui est prise entre ces deux forces, engagée dans une rivalité économique, technologique et géostratégique pour le leadership mondial.

Pour l'Europe et la France, 70 à 80 % des flux d'information échangés par les européens sur internet transitent par des serveurs et datas centers aux Etats Unis. Une interruption des liaisons sous-marines entre l'Europe et les Etats-Unis peut éteindre la lumière et générer un blackout temporaire jusqu'à réparation des câbles. Cette situation est donc propre à cette zone car les impacts pour la Chine, la Russie et les Etats Unis ne sont pas critiques [95].

Le secteur des câbles de télécoms est cependant un des rares secteurs dans le domaine du cyberespace où la France dispose d'une souveraineté industrielle quasi complète. Les années futures seront primordiales pour essayer de récupérer dans son fleuron le constructeur finlandais ASN (Alcatel Submarine Network) mais qui reste une entreprise localisée en France.

La France s'est positionnée sur plusieurs fronts. La première étape a été juridique. La loi 2019810 du 1er août 2019, a augmenté les sanctions pénales aux dommages causés aux câbles sous-marins [96].
Pour accroitre la résilience, un décret a été publié en 2017, relatif à la mobilisation de la flotte stratégique [97]. Les navires câbliers sont ainsi des bâtiments aptes à assurer la sécurité des moyens de communication et peuvent être réquisitionnés si besoin en temps de crise pour compléter les moyens des forces armées [98].

Enfin, en février 2022, prenant pleinement conscience du retard de la maîtrise des fonds marins et du besoin de protection des câbles, la stratégie ministérielle officialise la nécessité pour le ministère des armées de se doter d'équipements de sécurité des infrastructures maritimes, à la hauteur des Etats Unis, de la Chine et de la Russie [99].

Une initiative européenne a été mise en place avec le programme Mécanisme pour l'interconnexion en Europe — MIE numérique [100]. Elle a pour but d'accroître la capacité et la résilience de la dorsale

numérique internationale, les câbles sous-marins. C'est dans la continuité de l'Europe de devenir souveraine et indépendante sur le plan numérique. Ce projet participe ainsi pleinement à la stratégie « Global Gateway ». Des fonds sont octroyés par ce programme sur des projets de déploiement de câbles en particulièrement à un de ses représentants sur le secteur la société française Orange. Par exemple, un co-financement a été mis en place pour la construction d'un câble sous-marin entre le continent européen (Marseille en France) et africain (Bizerte en Tunisie). La société en restera l'unique propriétaire [101].

La cartographie des câbles sous-marins est le reflet des logiques stratégiques, économiques et politiques de notre monde actuel et de ses déséquilibres. Les câbles sont des infrastructures aussi essentielles que vulnérables. La conquête, le contrôle et la surveillance sont devenus « puissamment » stratégiques dans les guerres d'influence [102].

Tous les Etats se dotent de service de cybersécurité qui seront décrits par la suite, l'ensemble des acteurs doivent prendre pleinement conscience de la vulnérabilité des câbles sous-marins et resteront des cibles de guerre qu'elles soient traditionnelles ou cyber, un outil d'espionnage à grande échelle ainsi qu'un enjeu économique et politique.

Les satellites

En 1945, l'écrivain et chercheur Arthur C. Clarke a imaginé la communication par satellite géostationnaire. Dans un article publié, il énonça comment un satellite apparaissant comme un point fixe dans l'espace à des milliers de kilomètres pouvait permettre à l'homme de communiquer grâce à des ondes radio [103].

A la fin des années 601960, soit vingt ans plus tard, débuta l'ère satellitaire soit vingt ans plus tard. Au 1er mai 2022, 5465 satellites étaient en service autour de la Terre [104].

L'espace où se situent les satellites en orbite est d'abord un domaine de passage d'objets. Il est un enjeu majeur militaire dans un premier temps. Toute puissance qui a dans son arsenal des missiles balistiques utilise cette zone exoatmosphérique. Après le transit, cet espace peut être un lieu de placement des objets de nature militaire et également un lieu d'arsenalisation d'armes pour visée terrestre, maritime ou bien dans l'espace. La militarisation de l'espace n'est pas nouvelle mais la démocratisation de cette zone avec le risque cyber pose question dans les nouvelles stratégies militaires [105].

Si dans l'imaginaire, toutes les communications à l'international sont gérées par le satellite, ce n'est plus le cas depuis l'avènement de la technologie de la fibre optique depuis la fin des années 1980. Les câbles sous-marins sont les infrastructures utilisées pour les communications internationales en grande majorité comme décrit précédemment. La qualité et le temps de latence de la transmission de l'information sont de meilleure qualité et le coût moins élevé. L'usage des satellites est différent. Dans nos sociétés contemporaines en plus des télécommunications, ils sont utilisés pour le positionnement et la localisation géographique, la météorologie, la science ou pour la finance *(trading haute fréquence synchronisation temporelle très fine)*. Ils sont essentiels en ce qui concerne la connexion des opérations en mouvement, des zones mal reliées entre elles et qui ne disposent pas d'infrastructures de connexion terrestre, ils permettent également la résilience des autres infrastructures en cas de déconnexion.
On constate que les satellites sont en majorité exploités à des fins commerciales *(plus de 75% à mai 2022).* Ces dernières années, le nombre de données en orbite a fortement augmenté. Selon le rapport space tech de Sifted de janvier 2023, d'ici 2040 [106], le marché de l'industrie spatiale est estimé à plus

de 1 000 milliards de dollars. L'intelligence qui permet de percer les secrets de la surface de la Terre a un impact sur de nombreuses industries avec les données d'observation, par exemple l'agriculture, la pêche, les assurances, le climat.

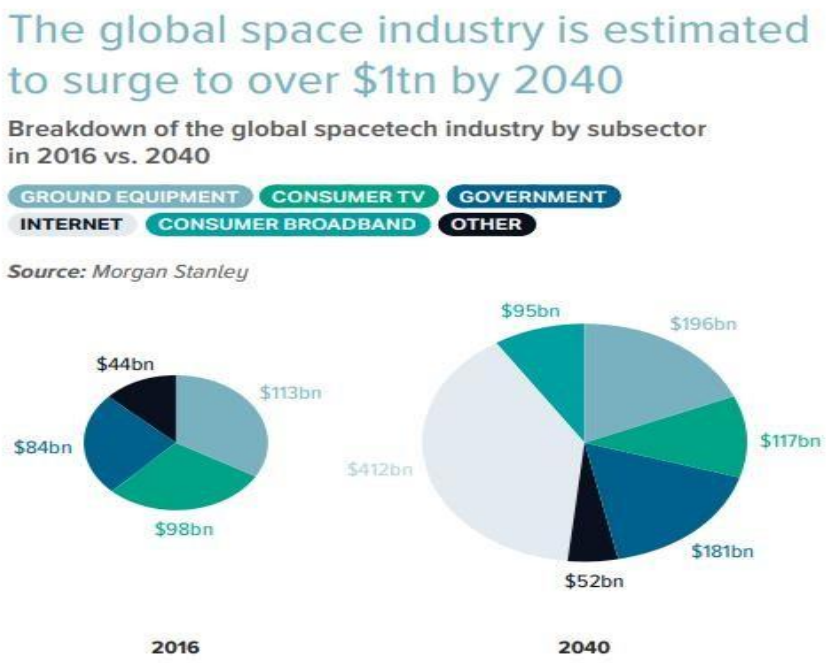


Figure 17: Répartition de l'industrie mondiale des technologies spatiales par sous-secteur en 2016 versus 2040

Les couches de l'écosystème satellitaires

Les satellites sont stationnés sur 3 orbites [107] :

- Orbite basse *(LEO ou SSO)* située entre 500 et 1.000 km d'altitude. Ces orbites sont utilisées pour les systèmes de communication, d'imagerie terrestre ou de météorologie. Ils sont majoritaires et représentent 86% du total en orbite à mai 2022.
- Orbite géostationnaire *(GEO)* située à 36 000 km d'altitude. Elle sert pour la météo ou pour les services de communication comme la télévision. Ces satellites restent à tout moment audessus du même point.
- Orbite moyenne *(MEO)* située entre 2 000 et 36 000 km. Elle est utilisée essentiellement pour les satellites de localisation.

Dans le but d'examiner les différentes menaces et d'identifier les risques dont peut être sujet la zone spatiale, une description de l'ensemble des éléments qui la compose et les liens entre eux est nécessaire. 3 segments sont identifiés [108].

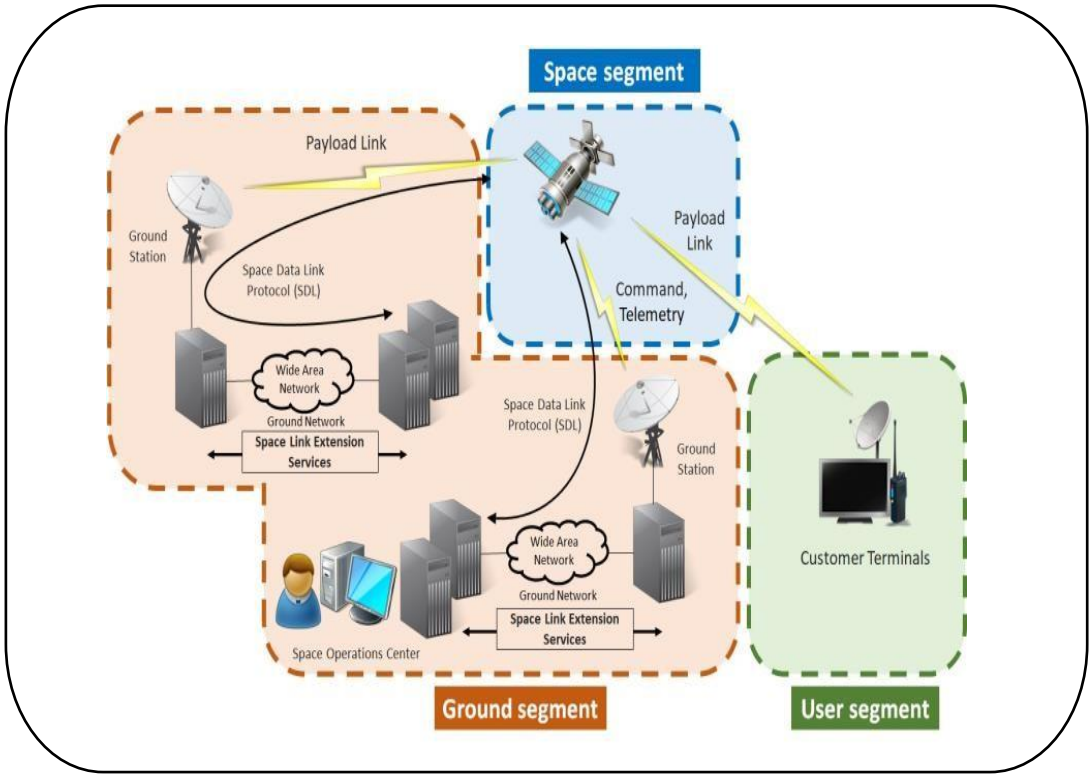


Figure 18 : Les trois segments d'un système de contrôle commande d'un satellite

- Segment terrestre *(Ground segment)*

Il est composé de tous les éléments au sol et qui servent à la télémétrie, au contrôle-commande et à la distribution de la charge utile. Il comprend une station de base, centre des opérations, du réseau terrestre, les systèmes de test, d'intégration et de lancement du Satellite [109].

- Segment spatial *(Space segment)*

Il est composé du satellite ou la constellation, des liens montants et descendants *(uplink et downlink)*. Cela inclut essentiellement une charge utile et une plateforme *("bus").*

La charge utile de communications comporte des antennes d'émission-réception et d'un ensemble de canaux de transmission et d'amplification *(ou transpondeurs)*, chacun de ceux-ci étant spécialisé pour un seul sens et pour une bande définie de fréquences.

La plateforme comporte plusieurs sous-systèmes indispensables au fonctionnement de la charge utile.

- Segment utilisateur (User segment)

Il est composé des équipements en émission et réception du signal satellite, une antenne reliée à un modem.

Vulnérabilité et menaces

Au début de l'invasion d'une partie du territoire ukrainien, le général Michel Friedling, alors à la tête du commandement de l'espace du ministère français des armées, a évoqué les faits devant des journalistes : « Peu après le début des opérations, un réseau satellitaire qui couvre l'Europe, notamment l'Ukraine, a été victime d'une cyberattaque. Des dizaines de milliers de terminaux ont été rendues inopérants » et sont « probablement irréparables. »

Le monde d'aujourd'hui n'est plus le monde d'avant. Cette cyberattaque opérée en Ukraine qui a entraîné également des répercussions sur d'autres infrastructures européennes permet de prendre conscience des vulnérabilités des systèmes spatiaux. Les dernières années ont été particulières dans le domaine spatial. On a constaté une forte augmentation du nombre de satellites en orbite : 3 591 satellites ont été mis en orbite dans l'espace entre 2019 et 2022 du en majeur partie au projet de conquête de l'espace de la société SpaceX (*2 153 satellites)* [104]. Le secteur de l'espace n'est pas en reste sur la couche du cyberespace quant à la multiplication du nombre d'acteurs et l'hybridation entre Etats et privé qui génèrent des problématiques de coopération [110]. Les armées ont vu leur besoin dans le domaine de l'espace augmenter pour le bon accomplissement de leur mission. Ce besoin conséquent ne peut plus être rempli que par les satellites militaires, les armées se sont donc pour la bonne conduite de leurs opérations tournées vers les satellites commerciaux. Ces infrastructures privées sont devenues d'éventuelles cibles militaires [111].

Avec l'entrée dans le New space, la course au développement spatial de satellites commerciaux, a poussé à mettre de plus en plus d'appareils en orbite et à diminuer leur niveau de sécurisation. L'écosystème satellitaire avant son entrée dans le cyberespace était très sécurisé. Les satellites étaient détenus par des organismes étatiques et difficiles d'accès après leur envoi dans l'espace. Les salles de contrôle au sol étaient très règlementées et il était peu probable que des acteurs malveillants puissent atteindre les commandes. La connexion entre les stations au sol et les satellites était dans la majorité des cas sans connexion internet. Que ce soit le "hardware" ou le "software" des matériels spécifiques, leur production et leur développement étaient en circuit fermé, il y avait une opacité sur le matériel et la diffusion des codes informatiques était très restreinte. Cette course à la mise en orbite et à la concurrence ont poussé à tirer les coûts vers le bas, la majorité des satellites actuels sont munis de logiciels avec des codes open source, reliés à une connexion internet et de matériels et protocoles standards. Ils sont donc plus vulnérables aux menaces cyber. La multiplication des fournisseurs et des sous-traitants qui interviennent dans la chaine d'approvisionnement et de production des satellites n'ont souvent pas le même niveau de maturité quant à la cybersécurité. Si on constate une vulnérabilité, une faille de sécurité, dans un programme au sol, il sera plus simple d'effectuer la correction que d'un satellite en orbite [112].

Si faire exploser un satellite en orbite à plus de 36 000 km de la Terre n'est pour le moment pas concevable pour un Etat sans en subir des conséquences collatérales avec prolifération des débris orbitaux, une opération disruptive dans le cyberespace est donc une option envisageable.

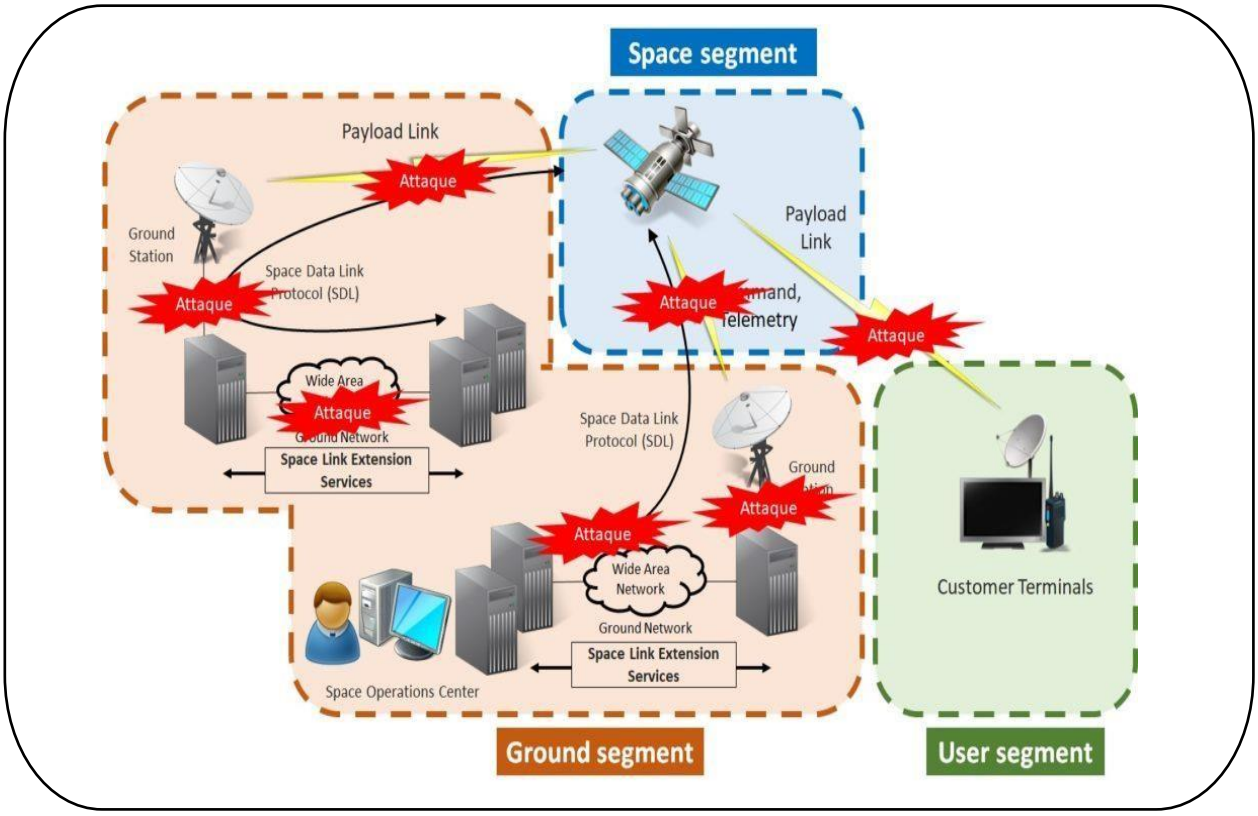


Figure 19: Positionnement des vulnérabilités et des attaques possibles

- Compromission

Le satellite KA-SAT de la société américaine Viasat a subi une panne de transmission en date du 24 février 2022, une heure avant l'entrée des troupes Russes en Ukraine. Ce satellite commercial était utilisé par l'armée ukrainienne pour ces communications satellitaires.

La méthode utilisée pour cyber attaquer et de rendre inopérante cette infrastructure spatiale, le satellite américain, est une attaque sur le segment utilisateur. Les modems reliés aux antennes clients qui permettent l'émission et la réception des communications ont été endommagés. A date, ce serait dû à un lancement de mise à jour de logiciel qui aurait été vérolée. Cette attaque a perturbé ce qui semblait être la cible, les communications du gouvernement et militaires sur le terrain ukrainien, mais elle a eu des effets ricochets et a également touché d'autres clients commerciaux utilisateurs du satellite. Parmi les victimes on a pu compter une infrastructure énergétique de l'Allemagne. Cette répercussion non ciblée sur une infrastructure critique a permis de prendre conscience à nouveau que des entités étrangères à un conflit armé peuvent être touchées sur une attaque cyber.

Si dans le cas du satellite KA-SAT ce sont les équipements au sol qui ont été touchés l'ensemble des segments de l'écosystème satellitaire peut être attaqué et mettre à mal des infrastructures critiques utilisant les connexions satellitaires [113].

Un événement européen dédié à la cybersécurité dans l'industrie spatiale a eu lieu en avril 2023 pour donner comme challenge à des Hackers éthiques de prendre à distance le contrôle d'un satellite de test et de montrer d'éventuelles vulnérabilités du système [114].

Ce test a pu mettre en exergue un type d'attaque qui est la compromission, objectif ultime de l'attaquant. Le satellite était sous leur total contrôle en s'introduisant dans le système de bord.

Ils ont réussi à prendre le contrôle de la caméra de ce satellite d'observation en ayant les commandes et d'envoyer une image altérée. Ils auraient pu pousser l'exercice encore plus loin et pointer la caméra vers le soleil qui ce qui aurait abouti à une destruction irrémédiable du satellite.

- Usurpation

Cette attaque consiste à envoyer un signal à une cible se substituant et se faisant passer pour une source légitime. Compromettre le système reste le but ultime en induisant en erreur la cible. Dans le cas de la zone spatiale, le plus courant est l'usurpation de la géolocalisation (*par exemple GPS pour les Américains ou Galileo pour les Européens)*. La victime est dupée et ne réalise pas qu'elle subit une attaque contrairement au brouillage. Les signaux GPS servent à se situer dans l'espace mais également à maintenir la synchronisation temporelle. La victime penserait être dans un lieu et un espace-temps différent. Selon l'observatoire du monde cybernétique, [115] la pose d'un drone américain en 2011 sur le sol iranien en vue de sa capture aurait été perpétrée avec ce type d'attaque.

- Espionnage

L'objectif de ce type d'attaque est de réaliser des écoutes illégitimes d'un signal. S'il est peu coûteux d'effectuer la captation du signal, casser ou récupérer les clés de chiffrement est de plus en plus difficile à réaliser dans la mesure où les communications sont désormais chiffrées pour assurer leur confidentialité. Dans le cadre d'un chiffrement trop faible, ce genre d'attaque reste possible si les attaquants arrivent à casser le chiffrement.

Le new space, vecteur de prise de conscience

Avant la fin des années 1980, seul deux Etats étaient capable d'atteindre l'espace à savoir les deux puissances étasunienne et russe. Ensuite, plusieurs autres Etats ont suivi en développant une compétence et une autonomie pour placer leurs satellites en orbite. La Chine, Israël, la France, l'Europe pour ne citer qu'eux sont entrés dans cette zone spatiale. Le New Space a donné une nouvelle image de la carte du Ciel. Les grandes puissances étatiques ne sont plus les seules à dominer ce secteur, la conquête spatiale s'est démocratisée avec l'arrivée de nouveaux acteurs privés. Ce domaine comme le secteur des câbles sous-marins a subi une hybridation Etat-privé.

On constate depuis une vingtaine d'années une montée en puissance du conflit sino-américain par le biais de leur politique de défense spatiale en affirmant leur objectif de protéger ou obtenir le contrôle de l'espace par tous les moyens que ce soit défensif ou dans l'atteinte des capacités adverses. Les Chinois à travers du cyber espionnage s'intéressent depuis longtemps à l'industrie spatiale pour récupérer le savoir-faire américain et ainsi les concurrencer dans ce domaine.

Les Russes et les Chinois énoncent dans leurs doctrines militaires que le moyen de réduire l'efficacité militaire de leurs adversaires se fait par des capacités anti-spatiales [116]. Ces deux pays développent à cette fin des armes antisatellites cinétiques (ASAT). Les Américains et les Indiens ont également

procédés aux tests de ce type d'armes. Pour autant, procéder à ce genre d'attaques n'est désirable pour aucun des Etats qui en a la capacité. En effet, les puissances sont de plus en plus dépendantes pour leur économie, le rayonnement politique ou le soutien aux forces armées de l'espace. Attaquer par destruction directe d'un satellite est facilement attribuable vu les moyens de reconnaissance actuels. L'entrée dans l'écosystème de l'Espace et son développement ont généré un investissement conséquent et toute destruction de satellite risquerait d'altérer toute la zone exo/extra-atmosphérique du fait du syndrome de Kessler [117].

Le cyber génère donc des menaces dans la nouvelle militarisation de l'espace. Les risques d'occasionner des débris spatiaux seront minimes. L'objectif sera de neutraliser partiellement ou totalement la cible et d'effectuer une compromission ou altération du système de contrôle et de ses données.

L'Europe ne doit pas rester en marge du développement des satellites pour sa souveraineté numérique et doit converser une autonomie dans le domaine. Pour éviter qu'elle ne subisse une dépendance aux GAFAM également dans ce secteur et être maître de sa sécurité, l'Union Européenne a investi dans un projet de constellation IRIS² [118]. L'objectif est de sécuriser ses infrastructures et transformer l'Europe en un hub entrepreneurial dédié au New space.

Dans cette nouvelle conquête de l'espace par la mise en orbite de plus en plus de constellations, les menaces cyber pèseront de plus en plus. Cette guerre hybride de conquête sera le théâtre des enjeux de pouvoir et ainsi augmenteront les menaces sur ces actifs. L'enjeu sera d'être indépendant sur l'utilisation des infrastructures et de sécuriser les différents segments en étroite collaboration avec les différents acteurs. Sur le plan réglementaire, La régulation par la communauté internationale des activités électroniques et cybernétique dans l'espace permettra un début de garantie d'un d'espace sécurisé et accessible.

La géopolitique des Datas centers, l'enjeu de souveraineté.

Le développement des NTIC a généré un accroissement exponentiel des données et a bouleversé leurs traitements et méthodes de stockages. Parmi ces évolutions, on a vu apparaître les datacenters.

Toutes les données que nous créons, utilisons, transférons ne sont pas que virtuelles, elles ont également un support matériel. Parmi ces supports à grande échelle, il y a les datacenters. Ce sont de grands entrepôts hébergeant de nombreux serveurs auxquels nous pouvons être connectés en permanence. Ce stockage peut être interne à une entreprise par exemple, mais il peut également être localisé chez un prestataire ou fournisseur. On a vu ainsi se développer le cloud computing qui consiste à déporter sur des serveurs distants des données et traitements informatiques traditionnellement situés en interne. Le coût d'entrée de ces prestations s'étant réduit au fil des années, de nombreuses entreprises à travers le monde y ont recourt. C'est ce qu'on appelle l'infogérance.

La vitesse de circulation des flux de données s'étant accrue, les datacenters n'ont pu pour impératif d'être situés à proximité des utilisateurs. Leur implantation peut être à l'autre bout du globe sans entraver le fonctionnement du cloud. Datacenters, utilisateurs et prestataires peuvent ainsi dépendre d'Etat différent.

Cette innovation technologique a introduit un changement de paradigme, on a assisté à une centralisation des données et ressources numériques.

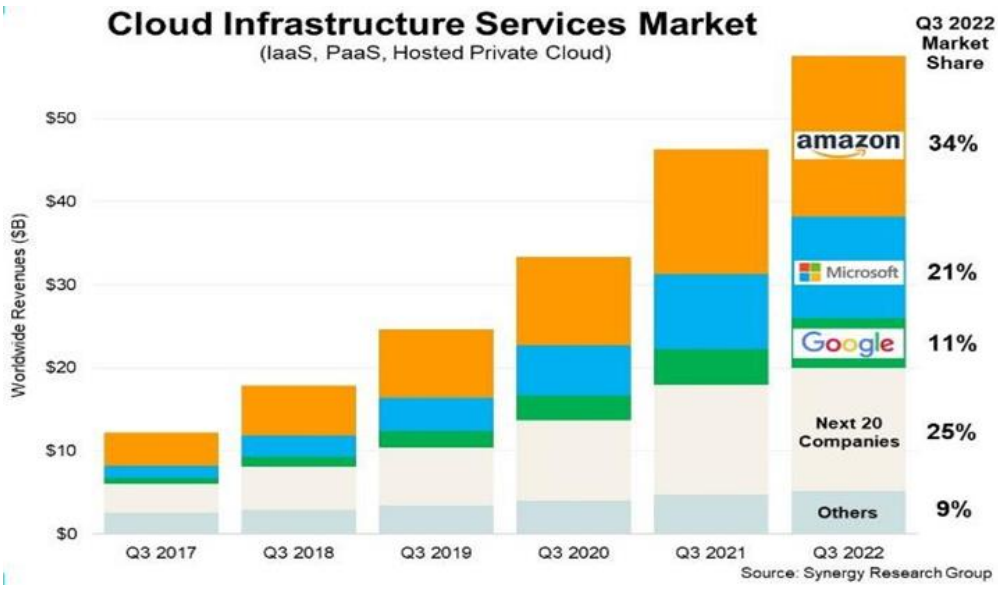
De nouveaux enjeux de sécurité apparaissent. Lorsque les ordinateurs et serveurs étaient le lieu de stockage et traitement des données chez les utilisateurs, la responsabilité de la sécurité leur incombaient. Dans l'informatique en nuage *(Cloud)*, les risques sur la disponibilité des données, leur intégrité et leur confidentialité sont également pris en compte chez le prestataire. Il se charge notamment d'assurer la sécurité et le bon fonctionnement des ressources informatiques qu'il héberge.

Pour permettre une connectivité optimale, les entités propriétaires des datacenters ont localisé les infrastructures physiques à proximité des points de raccordement des câbles terrestres ou des câbles-sous-marins [119]. On constate ainsi une centralisation du stockage des données en un même lieu (un datacenter pour mutualiser) et également en une même localisation (proche des autoroutes de l'information).

Le second enjeu également indispensable est l'intégrité des données car la corruption, l'altération ou la perte de ces éléments suivant le domaine des entités (par exemple bancaire), administrations ou organisation (par exemple la santé) peut se montrer critique.

Enfin, le troisième enjeu et non des moindres est la confidentialité des données, préoccupation croissante depuis le passage au cloud computing et l'affaire Snowden. Cet employé de la CIA et contractuel de la NSA, dénonçait au grand jour le réseau de surveillance de masses des Etats-Unis. Ce renseignement a pu être effectué par l'accès aux datas centers de grandes sociétés américaines sous couvert de lutte contre le terrorisme, dispositif du Patriot Act. Cette loi, votée en 2001 aux États-Unis permet à l'administration d'exiger un accès à toute donnée stockée par une entreprise américaine – ce qui assujettissait l'ensemble des GAFAM. Une loi complémentaire est venue s'ajouter le Clarifying Lawful Overseas Use of Data (CLOUD) Act en 2018 permettant aux instances de justice de contraindre les fournisseurs de services établis sur le territoire des États-Unis, par mandat ou assignation. Cette affaire a généré un contexte de méfiance généralisée à l'encontre des fournisseurs américains qui représentent plus de la moitié du chiffre d'affaires du secteur au troisième trimestre 2022 (Figure ci-dessous) et plus de la moitié en nombre d'infrastructures à travers le monde.

Dans cette nouvelle architecture des réseaux, les datacenters sont devenus essentiels au bon fonctionnement des gouvernements, entreprises et toutes organisations par le monde. Etant donné cette configuration, ils peuvent être des cibles critiques pour mettre à mal les infrastructures essentielles.



Ils peuvent être sujet non seulement à des sabotages physiques lors de conflits armés mais font aussi l'objet d'attaques cyber. Les menaces sur les datacenters et le besoin de contrôle des données au sein des infrastructures critiques civiles ou militaire sont devenus un problème de sécurité pour les Etats comme pour les populations (données personnelles).
Sur les relations internationales, cette interrogation s'étend également sur les enjeux de puissance. Pour accéder à ce contrôle, les acteurs peuvent actionner plusieurs leviers pour atteindre ce contrôle. Le premier moyen physique qui passe par l'acquisition et le développement d'infrastructures nationales de datacenters.

Une conservation sur le territoire national de données dit sensibles serait actionnée [120].

L'enjeu économique n'est donc plus le seul but des parties prenantes pour investir dans les actifs nationaux. Les aspects politiques et stratégiques sont pris en compte et cette question revêt une question de souveraineté nationale, voire de puissance. La notion de « souveraineté numérique », amenant à la souveraineté des données, couvrirait les trois couches, des infrastructures nationales, une industrie du numérique locale et des contenus nationaux. Ce trio est également la « Sainte Trinité » de l'économie des années 2020 exacerbée par la crise du COVID-19.

Cette stratégie est celle déjà adoptée par les grands puissants du numériques que sont les Etats-Unis, la Chine et la Russie à moindre mesure. Ainsi, pour échapper à l'impérialisme de ces trois pays et pour sécuriser leurs données, de nombreux pays dans le monde ont saisi le besoin de souveraineté. Ainsi, on voit apparaître une géopolitique également sur les datacenters en Europe et particulièrement en France.

En effet, l'ANSII a mis en place en 2016 un visa de sécurité nommé SecNumCloud proposé aux entreprises françaises qui serait prestataire d'un cloud souverain [121] et une aide en 2022 aux startups pour répondre au cahier des charges [122]. Une collaboration Européenne entre la France et l'Allemagne a également été mise en place pour un certificat de sécurité. Ce label commun est nommé European Secure Cloud [123].

L'adoption par les Etats de ces politiques publiques en matière de souveraineté numérique dans les prochaines années auront surement un impact sur le secteur des câbles sous-marins. Les flux de communication internationales se réduisant intrinsèquement avec la baisse des besoins en transmission de données.

LA COUCHE LOGIQUE OU LE VOYAGE RISQUE DE L'INFORMATION

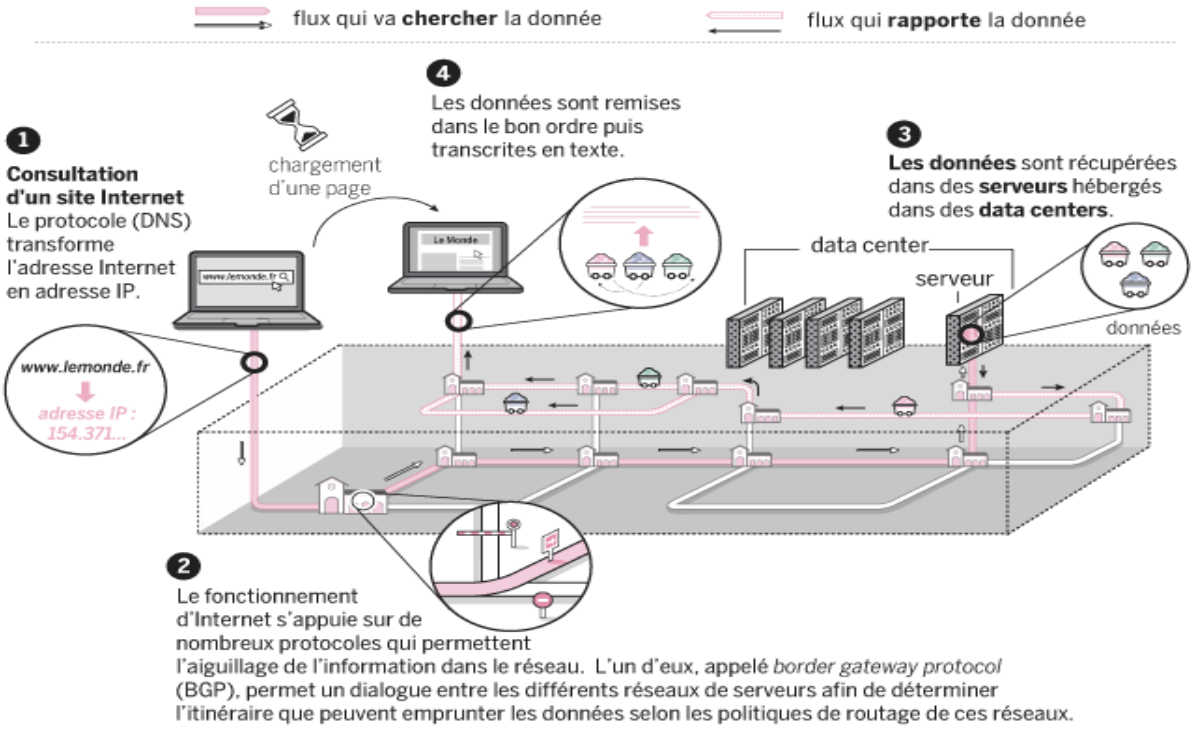


Figure 21: les protocoles majeurs d'Internet

Cette seconde couche logique et applicative est composée des services (logiciels applications, interfaces, programmes) qui auront pour objet la transmission des données entre deux points du réseau, le voyage des flux d'information. L'architecture logique de tous ces systèmes d'informations repose sur un socle commun, un langage compris par tous les ordinateurs du monde qui est le protocole TCP/IP.

Le routage des données par les points d'échanges

L'ensemble des réseaux nécessitent d'être interconnectés pour pouvoir échanger des informations. Cette interconnexion est réalisée grâce à des équipements réseaux appelés routeur. Ils permettent de faire passer les informations d'un réseau à un autre. Il existe plusieurs protocoles de routage, mais celui utilisé sur Internet est BGP (Border Gateway Protocol). Chaque réseau annonce via ce protocole les informations pour le joindre, ainsi de proche en proche les routeurs sont capables de construire une table de routage du réseau internet, ce qui leur permet de déterminer quel routeur de son entourage permet d'aller vers quel réseau.

Ce protocole historique d'internet a été conçu sur la base de la confiance dans l'annonce des routes. Le postulat à sa construction est que les données communiquées des réseaux interconnectés seront exactes, lors de l'annonce de leurs groupes d'adresses IP (Internet Protocole).

.

Figure 22: Carte de France des IXs

Il existe plusieurs façons entre deux acteurs pour s'interfacer, soit par l'achat de Transit à un opérateur local ou par un accord de peering entre les deux acteurs qui sont bien plus économiques. Il existe également dans certains datacenters des points d'échange appelés Internet eXchange Point (IX ou IXP) qui permettent de réaliser des peering à grande échelle avec l'ensemble des acteurs qui sont sur ce points d'échange.

Du fait de leur implantation dans des datacenter, on trouve souvent des concentrations dans les datacenters historiques, puisque ce sont bien souvent les endroits où il y a le plus d'opérateur et du coup, l'endroit où il faut aller. Si on prend l'exemple de la France, on a une forte concentration en région parisienne avec notamment le datacenter Telehouse 2 situé rue voltaire à Paris ou les DC Interxion et Equinix à Aubervilliers et Saint Denis.

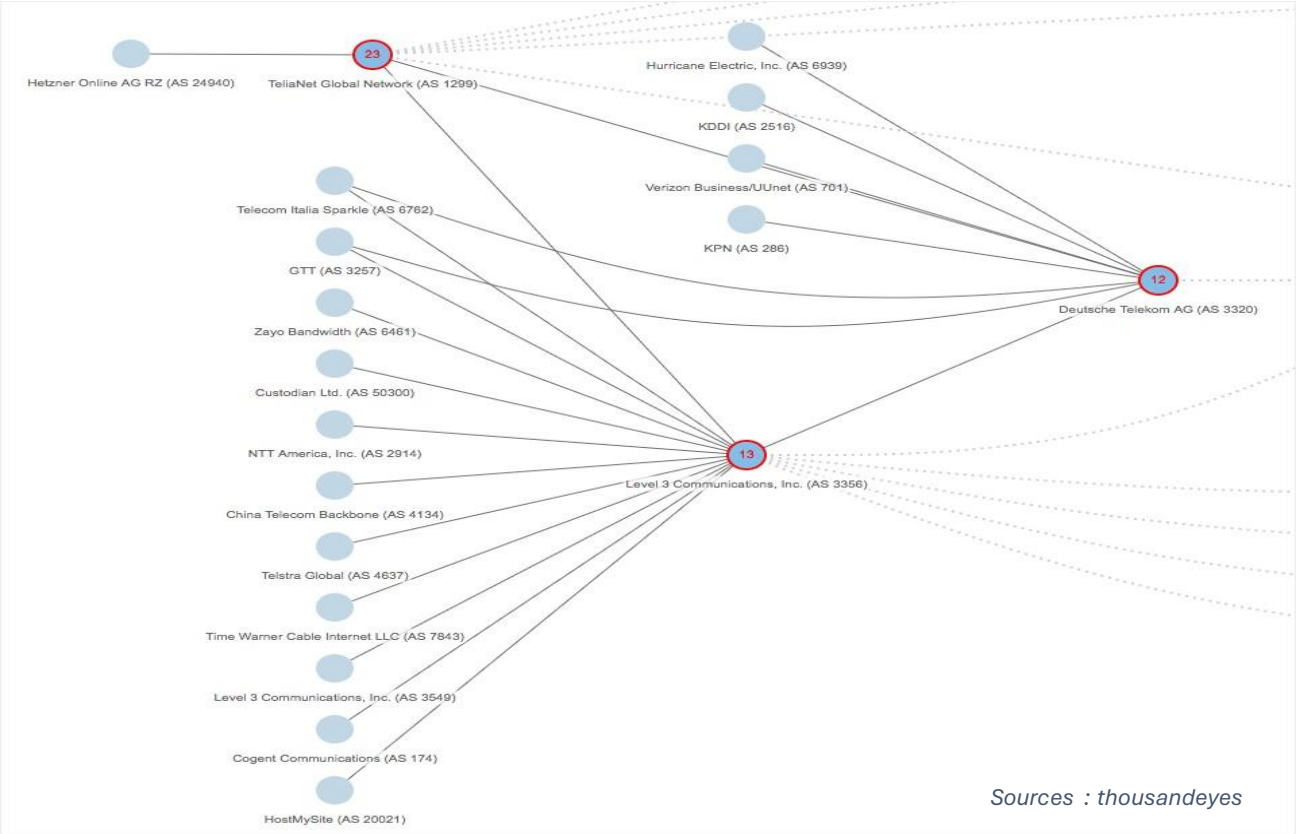


Figure 23: Une visualisation de la panne DE-CIX et du nombre d'interfaces d'appairage affectées au niveau 3, Deutsche Telekom et TeliaNet.

Certains datacenters deviennent, du fait de ces point d'accès, très sensible. Les impacts d'une coupure de courant ou d'un autre incident par exemple ne passent pas inaperçu.

La société ThousandEyes (racheté par Cisco en 2020 [124]) a fait l'analyse de la panne du 9 avril 2018 du point d'échange de francfort le DE-CIX qui est un important IXP au niveau européen. On constate sur la figure 17 que les systèmes impactés (en rouge) par la panne ont impacté la connectivité de certains réseaux. L'impact a été significatif, notamment en Allemagne. Le sabotage ou la destruction de certains point stratégiques pourrait avoir un impact significatif.

Figure 24: Internet Exchange Map (18/05/2023)

Infrastructures critiques

> Les entreprises en sont désormais des cibles privilégiées : « […] il y a deux sortes d'entreprises : celles qui ont été piratées (par le cyber) et celles qui ne le savent pas »
> Olivier Kempf (Docteur en science politique), 2015

Les cyberattaques contre les infrastructures critiques de plus en plus fréquentes interpellent aujourd'hui tous les Etats à travers le monde. L'espace cyber est devenu un terrain d'affrontements, l'écho des tensions qui préoccupent le monde venant servir et appuyer sans réserve des opérations militaires qui font aujourd'hui des guerres, des conflits hybrides. Le théâtre des opérations militaires bien que toujours réels, sont accompagnées d'une forme aussi dévastatrice et silencieuse avec des angles d'attaques multiples par le biais des infrastructures critiques gérées certes par les Etats à travers les entreprises et autres établissements publics mais aussi par des entreprises privées qui sont autant

de points d'attaques pour les cybers criminels pouvant toucher et paralyser le cœur des Etats. Dès lors les enjeux pour les Etats sont de deux ordres un enjeu sécuritaire mais aussi du renforcement de la coopération entre autorités publiques et Entreprises privés.

Les enjeux sécuritaires et la coopération entre Etats en matière cyber.

Face aux innombrables attaques qui les visent constamment, les Etats semblent avoir choisi la collaboration et la coopération pour endiguer le fléau de la cybermenace. Cette situation a poussé les Etats à adopter une position de cyber-résilience avec des stratégies basées sur le partenariat entre Etats mais aussi sur le partenariat inter étatiques pour juguler les cyberattaques sur les infrastructures critiques. L'attaque Wannacry avait paralysé temporairement des villes et mis à genoux des ministères entières aux États-Unis en France et en Grande Bretagne.

Des actes ont été déjà posés dans ce sens avec l'accord entre Singapour et la Canada en matière de cybersécurité pour faire face aux menaces et attaques par le partage d'informations. Bien avant par le biais du CSA (cyber Security Agency of Singapour) des accords avaient été déjà signés des accords avec l'Australie, les États-Unis, l'Allemagne, le Japon, les Pays Bas, l'Inde et la France. Dans le même sillage Israël et le Japon renforçaient leur partenariat en matière de cyber avec la signature d'un accord dans les domaines de l'échange d'information et de programme, de la recherche et de la formation dans le domaine cyber.

Aussi l'Union Européenne a émis plusieurs directives et règlements pour renforcer sa cyber résilience et à favoriser la coopération entre ses membres. En réaction à l'attaque de la Russie sur l'Ukraine et de manière opérationnelle l'Union Européenne a activé la "Cyber Rapid Reponse Team" pour soutenir l'Ukraine face aux cyberattaques liées à la guerre, ce qui est une première.

Les attaques cyber dans leur majorité s'inscrivent dans le contexte de la stratégie de guerre hybride et de déstabilisation mise en place par la Russie contre les pays occidentaux et les grandes démocraties . Les cibles les plus en vue par Moscou en la matière sont l'Ukraine, le Royaume Uni et les Etats Unis. La stratégie russe en matière de cyberattaques touche des domaines divers et variés, allant de la désinformation à la guerre électronique en passant par l'espionnage industriel de même que les infrastructures critiques. Ces attaques sont faites de manière ciblée avec comme objectif de mettre le doute et affaiblir la confiance accordée aux autorités, de s'immiscer dans la politique intérieure, d'influencer la politique interne avec comme objectif principal une déstabilisation. L'exemple récent est lié à la guerre en Ukraine avec des attaques visant à détruire le réseau électrique ukrainien en décembre 2015 et qui a perturbé et coupé la fourniture d'électricité à environ 250 000 foyers pendant plusieurs heures.

Les différentes initiatives prises actuellement dans le cadre de la guerre Russo ukrainienne pour protéger les infrastructures critiques sont édifiantes [125].

D'un autre coté la Chine s'active grandement en matière de cyber par des attaques et constitue aussi une menace dans l'espace cyber avec des capacités non négligeables. Dès 2015 les velléités chinoises de centraliser et de renforcer leur force cybernétique de ses forces armées ne font aucun doute avec une ambition première : devenir la plus grande puissance à défaut une puissance majeure dans le cyberespace.

Pékin détient les capacités les plus performantes et les plus sophistiquées au monde et l'objectif principal de ses attaques est centré dans des opérations d'espionnage industriel, de technologie de pointe contre des entreprises et des infrastructures et services critiques mais aussi à asseoir sa politique interne comme externe.

En dehors de ces deux pays cités d'autres acteurs étatiques n'en constituent pas moins un danger dans le domaine des attaques cybernétiques sur les infrastructures critiques d'autres pays. C'est le cas d'Israël et de l'Iran. Depuis Stuxnet (qui sera développé par la suite), l'Iran s'est doté de moyens dans le domaine cyber et mène des attaques au Moyen Orient en vue de déstabiliser les processus démocratiques de certains pays de la zone, de vol de propriété intellectuelle et industrielle d'entreprises et à créer des dissensions dans les pays inscrits sur son registre d'ennemis.

Tout en accusant l'Iran d'être à l'origine d'attaques contre ses infrastructures essentielles et critiques Israël cherche à se doter « d'un Dôme » de fer contre les cyberattaques.

« Nous tentons d'imposer les meilleures normes possibles en termes de cybersécurité aux entreprises de communication afin de protéger Israël et de créer une sorte de 'Dôme de fer' face aux cyberattaques sécuritaires. Nous subissons des milliers de cyberattaques chaque année », a déclaré Hendel.

« Les réseaux de communication sont une cible attractive pour les cyberattaques commises par des éléments hostiles », a-t-il poursuivi, notant que de tels piratages pouvaient entraîner le détournement d'informations confidentielles concernant des citoyens israéliens. Si les entreprises de communication sont parfois la cible d'attaques, elles servent aussi de porte d'entrée aux hackers qui cherchent à s'infiltrer et à infecter d'autres actifs stratégiques.

Il n'y a pas une seule infrastructure vitale qui ne soit pas connectée d'une manière ou d'une autre à un serveur relié au champ des communications. Les dernières attaques montrent que les acteurs politiques ou autres considèrent les infrastructures de communication comme des cibles privilégiées qui, elles-mêmes, mènent à des cibles stratégiques de premier plan » [126]

Cette déclaration du ministre des Communications d'Israël fait suite à de nombreuses attaques présumées iraniennes dont certaines ont visé des installations hydrauliques en 2020. C'est dans cette démarche que Israël a signé des accords de coopération en matière de cybersécurité avec les Etats-Unis suite à la visite d'une délégation américaine sur le sol israélien.

En France, le 15 février 2021, l'ANSSI révélait une campagne d'attaque compromettante du mode opératoire « Sand Worm » ayant pour cible plusieurs entités françaises avec comme titre : « campagne d'attaque du mode opératoire Sand Worm ciblant des serveurs Ceinturon ». Plusieurs entreprises et non des moindre utilisent ce logiciel dont TOTAL, EDF, AIR FRANCE, ou la RATP. Le mode opératoire étant attribué à des hackers affiliés aux services secrets russes [127].

Une liste non rendue publique dénombre à peu près 250 entités susceptibles d'être attaquées. Ces infrastructures sont réparties dans 12 secteurs d'activité. Les « OIV » (Opérateurs d'Importance Vitale) sont considérés par l'État comme indispensables à l'existence et la survie de la nation, et/ou dangereuses pour le bien-être de la population. Des cibles de choix pour les hackers ou pour un agresseur potentiel, parmi lesquelles on compte les plus évidentes : centrales nucléaires, gares, hôpitaux, ou encore réseau électrique. Tous ces sites sont incorporés à un dispositif qui exige une surveillance permanente [128].

« Les personnes susceptibles d'attaquer des organismes d'importance vitale sont pour la plupart des entités étatiques », explique le chercheur et hacker français Baptiste Robert, *« c'est-à-dire des groupes d'assaillants extrêmement structurés »*. Pour cet expert, il faudrait malgré tout plusieurs mois, voire des

années pour réussir à pirater ces lieux. « La France dispose elle aussi d'une armée de "cyber-soldats", 3000 spécialistes dont le travail consiste justement à contrer les tentatives de piratage. » [129,130]

« Les enjeux sécuritaires pour les Etats touchent le militaire et le cyber sert aujourd'hui d'appui aux opérations militaires sur les théâtres de conflits. L'enjeu et la dimension militaire du cyber a fait que la France a accentué sa défense militaire dans le domaine du cyber avec les responsables du cyber commandement des vingt-sept Etats membres de l'Union européenne. » [131]

Les cyberattaques entre Etats bien que fréquentes et dévastatrices parce qu'agissant sur les infrastructures critiques, d'autres acteurs non étatiques, des hackers, groupes privés appartenant au monde des pirates informatiques criminels sont aussi responsables de nombreuses cyberattaques sur des infrastructures critiques avec des motivations diverses. Cette recrudescence des cyberattaques opérées par des acteurs non étatiques dont les plus connues sont faites par rançongiciel interpellent les opérateurs d'infrastructures critiques sur la nécessité de protection des réseaux des infrastructures critiques.

Cependant mettre en place des méthodes dissuasives contre les cyberattaques sur les infrastructures critiques suppose de pouvoir identifier, contraindre et sanctionner les auteurs des attaques. La complexité et le nombre sans cesse grandissant rend difficile l'identification et l'attribution d'où la nécessité d'un partenariat Etats et entreprises privées dans ce domaine.

La nécessité d'un partenariat Etats et entreprises privées

Les accords entre Etats dans ce domaine ont certes leur importance, mais ne saurait être efficace sans une efficacité opérationnelle : le privé. La fédération des actions et initiatives entre le secteur privé et le secteur public constituent un élément indispensable face à la menace de plus en plus croissante des cyberattaques sur les infrastructures critiques.

En effet, les acteurs privés par leur position et leur importance dans les secteurs critiques de l'Etat ont accès à des informations de grande importance que les Etats et les forces de défense et de sécurité ne possèdent pas. C'est dans ce cadre que les États-Unis ont signé une loi sur la cybersécurité faisant obligation aux entreprises "traitant des infrastructures critiques" qui subissent des cyberattaques ou paiement de rançongiciels à collaborer avec la CISA par un signalement dans les 72 heures ou la journée selon les cas [132].

Cette loi, promulguée à la suite de l'attaque contre un pipeline en mai 2021 [133], est donc pour améliorer et construire une cybersécurité résiliente des infrastructures critiques face aux cyberattaques.

La mutualisation des ressources et l'automatisation des process face aux incidents que public et privé apprendrons les uns des autres à conjuguer leurs efforts et à combattre mieux les cybers attaquants.

En France, le Campus Cyber est une preuve patente puisque des OIV (opérateurs d'importance vitale) et des OSE (opérateurs de services essentiels) sont réunis dans un même écosystème, pour partager des informations et bonnes pratiques sur les cybermenaces afin d'en comprendre et saisir leur évolution.

La nature des attaques sur les infrastructures critiques

Les cyberattaques sont devenues une arme redoutable du 21eme siècle. Les infrastructures vitales regroupent toutes les installations que l'on considère comme indispensables à la vie et au fonctionnement d'une société, qu'elles soient de nature physique ou numérique.

Ces infrastructures sont de plus en plus connectées au monde numérique exposant ainsi ces systèmes et services aux risques d'attaques informatiques.

Des attaques cyber ont déjà eu lieu et ont touché des infrastructures vitales à travers le monde que ce soient des cybersattaques touchant les systèmes informatiques et par ricochet des systèmes vitaux essentiels à la vie des populations. Les procédés peuvent être divers et variés : hameçonnages, ingénierie sociale, virus informatique, déni de service, etc.

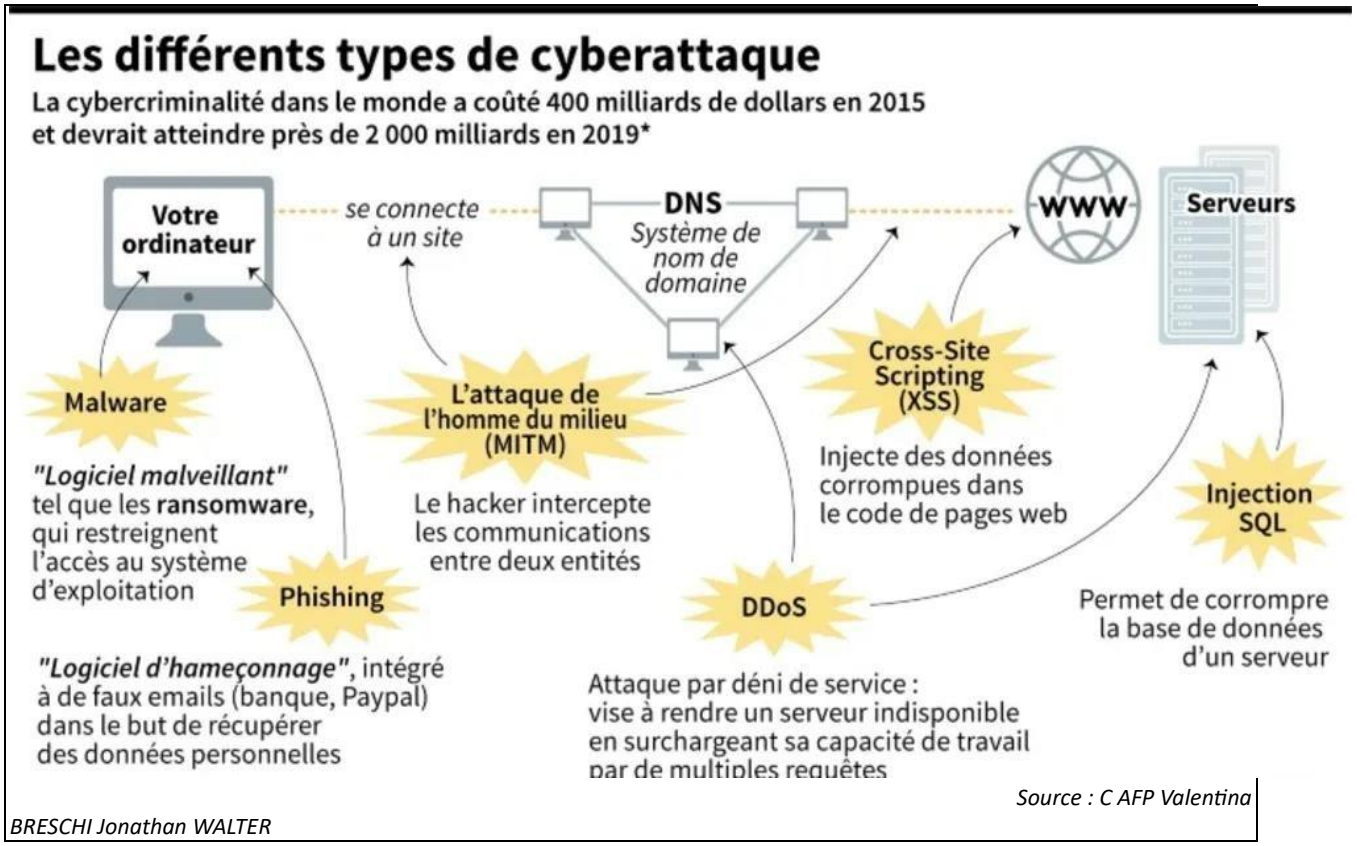


Figure 25: Les différents type de cyberattaque

1. Logiciels espions, virus et cheval de Troie

Les attaquants vont insérer un code malveillant dans un système informatique afin de le compromettre, l'altérer volontairement, dans le dessein de tromper et/ou d'en prendre le contrôle. Les virus informatiques sont à la source de la majorité des attaques. Les Etats et gouvernements considèrent comme infrastructures vitales les systèmes critiques nécessitant une protection accrue contre les attaques informatiques.

Une cyberattaque sur un des systèmes d'une organisation d'importance vitale peut causer des dommages économiques et sociaux considérables. En conséquence, la cybersécurité des

infrastructures vitales est primordiale pour la sécurité nationale et la continuité des activités économiques. Un exemple d'attaque par logiciel espion, est celui de l'affaire Solarwinds. Cette affaire constitue une attaque d'envergure survenue en décembre 2020 qui dévoilait une opération de cyber espionnage sophistiquée contre des entreprises et organisations occidentales.

L'attaque Solarwinds, *(une entreprise américaine de logiciel de gestion)* a touché des clients de la société qui étaient fournisseurs de solution de supervision et de gestion des réseaux informatiques de plusieurs institutions publiques et grandes multinationales.

Il s'agissait d'une attaque cyber dite de la « supply chain attack avec de multiples vecteurs d'attaque de propagation de la compromission par rebond ». Trois vecteurs d'attaques *(au moins)* ont été identifiés disait marc Antoine Ledieu avocat et RSSI [134]. Principalement :

- Un " cheval de Troie " dans le code source d'une mise à jour du logiciel Orion de Solarwinds *(censé centraliser la surveillance, l'analyse et la gestion de systèmes d'information)*
- Une vulnérabilité dans le service "office 365" de la société Microsoft
- Une vulnérabilité du côté d'un produit de la société VMware

Les attaquants ont pu injecter un code malveillant dans la mise à jour du logiciel de Solarwinds. Le CERT-FR parlait « de campagne d'intrusion par le biais d'une compromission de mise à jour de la plateforme de gestion et de supervision appelée « ORION »[135].

Les agences de sécurité américaines ont attribué cette cyberopération aux attaquants soutenus par l'Etat Russe plus connus sous le nom de ATP29 ou Cozybear. De son côté, la Russie nie toute implication [136].

Les conséquences de l'attaque sont importantes et la société Solarwinds a révélé que le virus avait touché 18 000 de ses clients dont 425 des 500 entreprises étatsuniennes clientes dont le Département du trésor, celui de la sécurité intérieure et le Département de l'énergie.

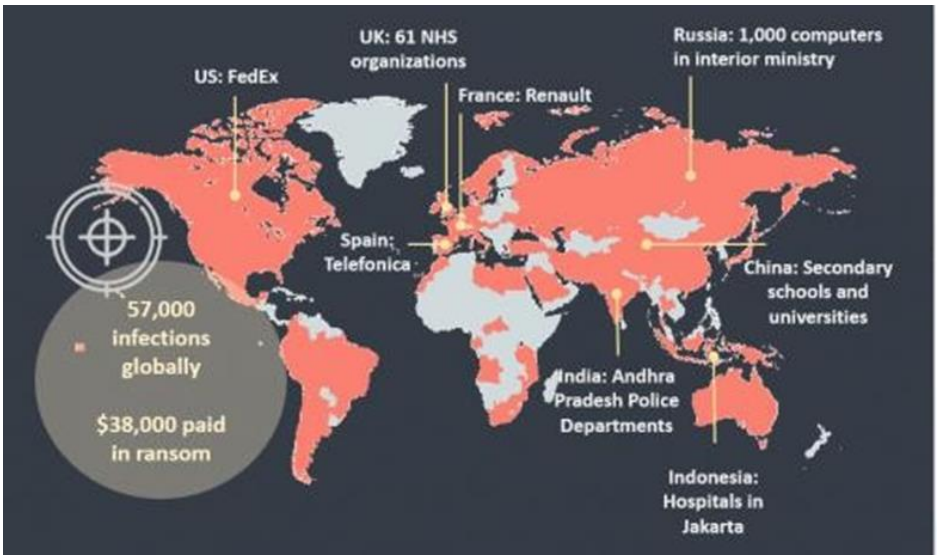
Mais également des entreprises privées telles que Microsoft, FireEye et Malwarebytes ; des institutions, des universités et de grandes entreprises françaises. [137].

2. Les attaques par exploitation de la vulnérabilité des logiciels

Les attaques par ransomware peuvent aussi entraîner des conséquences sur les organismes d'importance vitale. Ces attaques ont pour but d'extorquer de l'argent (monnaie ou cryptomonnaie) en utilisant un ransomware, un type de programme malveillant. Ce programme chiffre les données d'un système empêchant leur disponibilité à un instant T. Ce fut le cas avec WannaCry. Il convient dès lors de se demander quelle est la conséquence probable d'une attaque par ransomware.

En 2017 (12 mai -15 mai), l'attaque du ransomware WannaCry a affecté plus de 300 000 ordinateurs dans 150 pays, notamment des compagnies ferroviaires en Chine, des pharmacies en Russie, des aéroports en Allemagne, des entreprises en Amérique du Nord et des hôpitaux britanniques.

La National Health Service fut touchée avec une infection sur plus de 70 000 appareils dont des scanners IRM ou des réfrigérateurs de stockage de sang poussant certains services à refuser les urgences [138].



Source : Rhidi, n.d.

Figure 26: Wanna Crypt worm attack

3. Atteintes par un support physique externe

En 2010 le monde découvrait ce qui est considéré comme l'un des malwares les plus sophistiqués jamais créés : Stuxnet. Il a été spécialement conçu pour attaquer les systèmes de contrôle industriels pour le programme nucléaire iranien. Ce virus s'est propagé via des failles de sécurité dans Windows et des clés USB infectées. Il a par la suite affecté les centrifugeuses d'enrichissement d'uranium pour modifier les vitesses de rotation de celles-ci, endommageant ainsi les équipements. Cette attaque provient des États-Unis avec l'aide d'Israël, dans le but de neutraliser et saboter le programme nucléaire iranien. L'analyse de Stuxnet a plus que mis en lumière la possibilité et la capacité des hackers professionnels bien financés et bien structurés à concevoir et développer des programmes malveillants ultrasophistiqués et à perpétrer des attaques pour perturber les infrastructures stratégiques et /ou vitales d'un pays. Cette attaque sans précédent a également mis en exergue la vulnérabilité croissante des systèmes de contrôle industriels face aux cyberattaques. Dès lors, les gouvernements et entreprises ont renforcé leur sécurité informatique pour protéger leurs systèmes contre de telles menaces.

C'est le premier virus jamais découvert pouvant espionner et reprogrammer des systèmes industriels à niveau de risque élevé. Stuxnet reprogramme des automates programmables industriels produits par Siemens et rend invisible ses modifications. Rappelons que les automates programmables Siemens sont utilisés par des centrales hydro-électriques ou nucléaires mais aussi pour la distribution d'eau potable ou les oléoducs.

Le virus a touché 45 000 systèmes informatiques, dont 30 000 situés en Iran, dont plusieurs PC appartenant à des employés de la centrale nucléaire de Bouchehr. Il y eu 15 000 autres systèmes informatiques infectés situés dans divers pays : en France, en Inde, en Allemagne et en Indonésie, tous utilisateurs de technologies Siemens. Les attaques de type cyber visant les infrastructures critiques ou les objets connectés ne sont pas les seuls moyens dévastateurs dont les gouvernements et organisations doivent faire face ; il existe d'autres types d'attaques ayant comme support le cyber aussi puissantes que les cyberattaques : la guerre informationnelle.

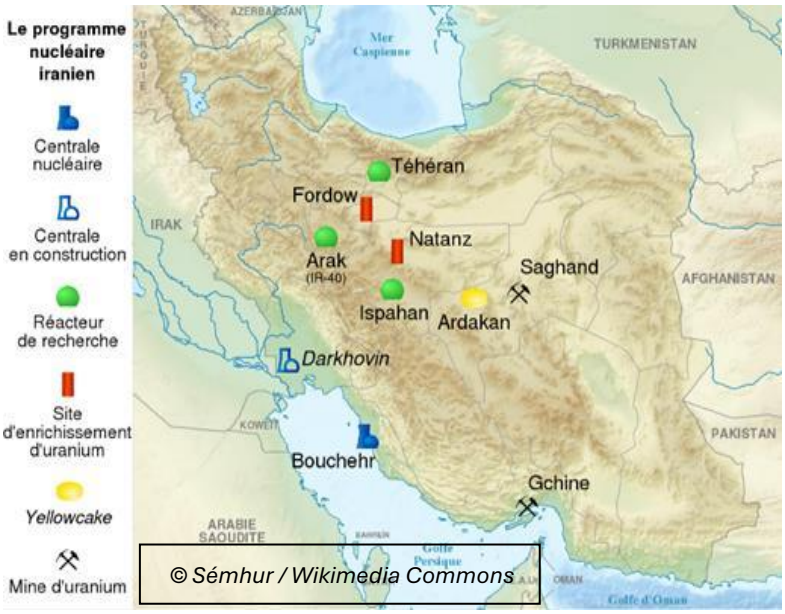


Figure 27: Carte des installations nucléaires iraniennes

Objets connectés

Un objet connecté est un objet qui a la capacité de se connecter à un réseau de communication *(Internet des Objets (Internet of things IOT en anglais) via Wi-Fi, Bluetooth, réseau internet mobile notamment 5G….)* et peut selon les cas, recevoir, stocker, traiter et transmettre des données, recevoir et donner des instructions pour fonctionner. Ces objets peuvent être autonomes ou fonctionner avec un smartphone ou une tablette permettant de les contrôler ou de servir de relais pour échanger des données. Ces données peuvent être consultables sur un appareil mobile ou sur un service Internet [139].

Cette définition montre que les Etats, les entreprises ou même les populations tout simplement utilisent chaque jour et à chaque instant des objets connectés pouvant transporter des données d'entreprises, données d'Etats et de gouvernements, données personnelles, de santé etc. Ces données peuvent faire l'objet de récupération lors d'attaques malveillantes comme la possibilité d'hacker un appareil pourvu de webcam ou de caméra de sécurité en en prenant le contrôle. Nos objets connectés donnent aujourd'hui plus de possibilités aux hackers de mener des cyberattaques. Des exemples prouvent aujourd'hui que les menaces sur les objets connectés par attaque cyber sont bien réels. En exemple :

- La découverte en 2015 d'une vulnérabilité ayant entrainée le retrait du marché de près d'un million de véhicules chez le constructeur de JEEP. Cette vulnérabilité permettait ainsi de prendre le contrôle à distance, dont le système de freinage à distance, de la Jeep cherokee.
- Une plainte déposée contre Amazon en 2020 sur une faille du système de sécurité sur des modèle de sonnettes sans fil produits par Ring *(entreprise appartenant à Amazon)*, Vivint et Remo. Les vulnérabilités donnaient la possibilité de se connecter au le réseau des domiciles et ainsi pouvoir espionner les individus.

Les objets connectés rythment la vie quotidienne aussi bien personnelle que professionnelle offrant ainsi une surface d'attaque de plus en plus vaste entrainant une explosion des menaces aux

conséquences potentiellement destructrices sur l'écosystème des objets connectés. Les méthodes utilisées par le cyber attaquants peuvent être variées tels que les botnets, logiciels malveillants, piratages d'appareils en ayant des accès non autorisés pour prendre le contrôle de leurs fonctions [140].

Les cyberattaques d'IOT peuvent atteindre des infrastructures vitales et/ou physiques en s'attaquant par exemple au contrôle de sécurité d'un système industriel pour causer des dommages matériels. On assiste aujourd'hui à un monde avec des objets connectés sur toutes les chaînes de vie *(maison, transports, industries, économie et santé),* on parle de villes connectées. Les risques de cyberattaque à travers ces objets sont de plus en plus forts d'où la nécessité d'une veille et alerte à plusieurs niveaux.

- Une sensibilisation des utilisateurs sur les risques associés à l'utilisation de ces objets connectés.
- La surveillance de la sécurité des objets connectés pour détecter les activités suspectes via le net et éliminer les cyberattaques potentielles.
- Les mises à jour régulières des micrologiciels et logiciels pour une correction permanente des vulnérabilités sur les objets connectés.

Les cyberattaques à travers les objets connectés sont en constante croissance et continuerons à évoluer du fait des inventions et avancées technologiques. Cela constitue une menace permanente de la vie sociale, économique et industrielle. C'est pourquoi cette évolution technologique doit être accompagnée de la mise à jour continuelle des mesures de sécurité pour faire face aux techniques et tactiques des cyberattaquants [141].

GUERRE INFORMATIONNELLE

Les technologies de la communication que sont les satellites et les câbles sous-marins et leur développement ont abouti à l'ère de l'information, expression associée aux années 1980. S'en est suivie l'ère du numérique dans les années 1990 avec la démocratisation des ordinateurs personnels et l'apparition de l'e-commerce. Le changement le plus impactant sur l'information est apparu dans les années 2000, avec la connexion de machines et les logiciels participatifs. Les utilisateurs ont été reliés entre eux par la création de plateformes comme Facebook en 2004 et Twitter en 2006. L'information est devenue immédiate et mondiale avec l'apparition des réseaux sociaux, des médias numériques et des messageries instantanées *(ex. WhatsApp).* Le véritable impact de ces nouveaux vecteurs de l'information, est que les barrières ou filtres entre le créateur de l'information et l'usager sont amenés à disparaître. L'internaute est devenu acteur dans le choix de ses sources d'information et aussi créateur de nouveaux contenus en effectuant également leur partage [142].

La révolution numérique a transformé et augmenté les canaux de communication et a bousculé les relations que les gouvernements nationaux entretiennent avec leur société et entre eux. Les opérations menées dans le but d'obtenir un avantage informationnel sur un adversaire ne sont pas nouvelles et ne sont pas non plus l'apanage des pays autoritaires. La vitesse de propagation de l'information a généré de nouvelles vulnérabilités et offre de nouvelles armes cyber à celui qui veut attenter à la souveraineté d'un Etat.

Dans cette partie, nous détaillerons les risques et menaces sur les différents canaux de communication et les objectifs des attaquants sur cette désinformation, surinformation et sur la propagande.

Les menaces et risques

Devenues omniprésentes les fausses informations sont considérées aujourd'hui comme « l'arme la plus puissante sur la planète » poussant les observateurs les plus avertis à parler d'« *arme de destructions massives »* ou même « d'armes de distractions massives ». Si les Etats sont beaucoup mieux armés face à la désinformation qu'il y a quelques années, les contenus qui inondent les réseaux sociaux sont néanmoins plus difficiles à contrôler avec l'émergence de nouvelles plateformes : Facebook, Instagram, YouTube, WhatsApp, TikTok, et dernièrement Telegram.

Espionnage, manipulation de l'information, propagande, la lutte informationnelle est devenue une arme puissante qui accompagne les manœuvres militaires conventionnelles. Elle se déploie dans le cyberespace. Les multiples risques sont nourris par ce besoin de guerre informationnelle qui fait une jonction entre le cyber, la réputation et la désinformation. Les conséquences peuvent être multiples pour les Etats et/ou les entreprises victimes : faillite ou contrôle de l'entreprise, vol de secrets intellectuels ou industriels ou même de fichiers clients, diffusion de documents dans la presse pouvant atteindre la stabilité de l'Etat (révélations, désinformation, atteintes à la réputation).

La Chine et la Russie en sont les maîtres et le pratiquent depuis fort longtemps et se sont munis de doctrine dont l'objectif est de militariser le cyberespace. Les États-Unis l'ont déjà compris et pratiqué pour légitimer des guerres et embarquer le monde à leur cause (guerre du Golfe). La France aujourd'hui assume de plus en plus cette guerre informatique d'influence jusqu'à affirmer l'asymétrie. *« La frontière entre compétition et confrontation, qui permettait de distinguer le temps de paix (...) crise (...) guerre, est aujourd'hui profondément diluée. Elle laisse place à de multiples zones grises où, sous couvert*

d'asymétrie ou d'hybridité, se déploient des actions d'influence, de nuisance voire d'intimidation, qui pourraient dégénérer », avait expliqué en février 2020, le président de la République française Emmanuel Macron.

« Lorsqu'elle est utilisée à bon escient, l'arme de l'information permet de gagner sans combattre », affirmait l'ancienne ministre des Armées Florence Parly, lors d'une présentation de l'action des armées dans le domaine de la lutte informatique d'influence.

C'est une position assumée que la guerre des temps modernes est multifacettes et que la France devrait elle aussi avoir sa stratégie d'influence dans cette guerre de l'information au même niveau que les autres grandes puissances (Chine, Etats-Unis, Russie).

Les différents supports médiatiques utilisés nous permettrons d'étudier avec des exemples les rôles et zones d'influence ainsi que les acteurs précités.

Réseaux sociaux et autres canaux informationnels

Réseaux sociaux et politique

Il est établi aujourd'hui que la Russie et l'Iran ont essayé d'influencer les élections présidentielles américaines. Les États-Unis se sont également immiscés dans des élections dans d'autres pays ; ce qui en fait un phénomène plus ou moins global [143]. La motivation politique est souvent une immixtion dans les affaires intérieures d'un pays : une ingérence étrangère.

Un impact psycho social peut aussi être recherché touchant une population plus ou moins jeune incitant la colère collective, des troubles internes en vue d'une déstabilisation sociale ou le renversement d'un régime *(Printemps arabes...)*.

Nos applications nous délivrent tous les jours des informations mais la plupart de ces flux sont souvent sujets à des manipulations. Les motivations peuvent être diverses et variées : financières, politiques, géostratégiques ou autres.

La guerre de l'opinion : l'exemple russe

Il existe une vraie guerre de l'information opérée par les Etats et de stratégie d'influence sur l'espace cyber. La Russie a pris de l'avance en la matière et a réussi à créer en 2013 une agence de la recherche Internet avec des salariés qui interviennent en permanence sur les différents réseaux sociaux avec pour but d'influencer l'opinion et dérouler l'agenda des intérêts de la Russie en matière d'influence, de diffusion de fausses nouvelles et de désinformation.

La stratégie russe, destinée à acquérir du pouvoir stratégique avec le développement de ses forces numériques à travers cette agence, prouve à outrance la guerre de l'opinion pour pouvoir acquérir du pouvoir géostratégique pour faire face et affaiblir les démocraties occidentales notamment l'Europe qui sont les principaux opposants.

Des armées sont aujourd'hui déployées sur le net « troll » en vue de créer de la désinformation en ligne, l'intelligence artificielle aidant avec comme objectif le pouvoir d'agir sur l'espace informationnel

pour mobiliser ou démobiliser des populations et faire basculer la bataille d'opinion dans un sens ou dans un autre.

Plusieurs actions ont été menées avec la diffusion de fausses informations visant à créer la confusion notamment en Afrique avec comme exemple la présence de Wagner en Afrique.

L'Afrique théâtre d'opération de la guerre Informationnelle : L'exemple Wagner

Les « Wagner leaks » ont fini de démontrer et de prouver comment une entreprise de désinformation et de déstabilisation informationnelle a fini par s'installer géographiquement en terre africaine et influencer l'opinion publique africaine à travers une guerre informationnelle sans précédent au détriment des occidentaux notamment la France. La présence de Wagner en Afrique inquiète à plus d'un titre ; déclarée entreprise criminelle par les Etats-Unis en 2023 notamment avec la guerre en Ukraine, le groupe para militaire russe gagne du terrain en Afrique. Wagner s'y était déjà installé depuis longtemps utilisant des techniciens aguerris pour asseoir son influence et sa guerre informationnelle sur les réseaux sociaux [144].

L'intervention de Wagner en Afrique est présente sur tous les réseaux sociaux et son influence sur le cyberespace de plus en plus visible.

La France serait la victime directe d'attaques informationnelles de Wagner. Passé colonial mal géré, héritage colonial exacerbé, et opérations militaires aux résultats mitigées (opération Barkane au Mali), la France en premier et les occidentaux ont créé une faille dans laquelle Wagner à travers sa puissante machine de désinformation allait s'engouffrer pour avoir une assise militaire sur ces territoires et créer la sympathie des populations et des dirigeants des pays au détriment de celle occidentale, la France en tête.

Une guerre d'influence se joue entre la France et la Russie au Mali provoquant bouleversements économiques et coups d'états n'épargnant pas le voisin burkinabé.

Selon l'AFP, vendredi 22 avril *« L'armée française a affirmé avoir filmé des mercenaires russes en train d'enterrer des corps près de la base de Gossi, au Mali. D'après l'état-major, cette manœuvre doit ensuite servir à accuser les Français, d'avoir laissé un charnier derrière eux »* [145].

La guerre en Ukraine s'enlisant, le Kremlin cherche à déstabiliser l'Occident en menant une guerre informationnelle au Sahel, notamment contre la France. Pour cela, Moscou utilise une armée de l'ombre composée de mercenaires, trolls et sociétés écrans à la solde de Vladimir Poutine. Leur mission est de calomnier, décrédibiliser et diaboliser l'Occident afin de promouvoir la vision du monde de Poutine. Cette guerre informationnelle se mène également dans le cyberespace, comme le montrent les révélations des Vulkan Files [31], qui dévoilent les dessous de la guerre électronique russe [146].

Réseaux sociaux et guerre en Ukraine

La guerre n'a plus de barrière géographique avec le cyber. La présence physique sur le théâtre des opérations n'est plus nécessaire pour être impliqué dans la guerre. De partout dans le monde, on peut envoyer des photos, vidéos, et autres images pour mobiliser ou essayer de mobiliser des personnes.

La guerre n'est plus réellement caractérisée par l'affrontement de deux armées sur un même territoire, mais aussi par le champ de bataille virtuel ou "cyber-guerre". Au-delà de la possibilité de couper les réseaux internet d'un pays pour l'empêcher de se défendre, il y a la diffusion des fausses informations (fake news) sur les réseaux.

La guerre sur les réseaux sociaux se passe de mots et empêche le recul et l'analyse permettant de rechercher et vérifier le vrai. Le rôle des algorithmes s'impose à l'esprit et à la perception. Exemple de "TikTok" avec la diffusion d'images sans fil conducteur ou lien logique permettant de vérifier l'information même s'il n'est bien sûr pas le seul terrain de la guerre à coté de WhatsApp ou Instagram, Twitter, YouTube, Meta ou autres [147].

La guerre qui se déroule sur les trois zones air terre mer a aussi pris la forme d'une bataille d'influence qui se joue sur les réseaux sociaux. L'intelligence artificielle a permis de relayer la propagande avec la création d'activistes, ou de fausses images et même de faux commentaires.

Depuis 2014 les réseaux sociaux continuent de jouer un rôle prépondérant dans la couverture de la guerre qui continue de se dérouler. Des images, des vidéos de la guerre sont utilisées sur les plateformes numériques pour faire du partage d'informations par les Ukrainiens souvent en temps réel. Des rassemblements et manifestations pour soutenir l'armée ukrainienne sont également relayés par les réseaux sociaux pour dénoncer l'agression russe [148].

D'un autre coté la désinformation et la propagande notamment par les médias russes et partisans séparatistes pro russes sont véhiculées à travers les réseaux sociaux. Ce phénomène est amplifié par les faux comptes pour semer la confusion et accentuer la propagande.

La guerre en Ukraine a également entrainé une polarisation accrue sur les réseaux sociaux, avec des Ukrainiens et des Russes s'exprimant souvent dans des espaces en lignes séparés. Les discussions sur la guerre ont souvent été passionnées et émotionnelles, avec des accusations de mensonges et des manipulations de part et d'autre.

En fin de compte, les réseaux ont été un outil important pour les Ukrainiens pour partager des infos et opinions sur la guerre en cours, mais également pour propager de la désinformation et pour polariser davantage les opinions.

Médias

Les médias traditionnels ont toujours été considérés dans la mentalité collective comme une source d'informations fiables et impartiales. Cependant, force est de constater que dans la société actuelle, les médias traditionnels se heurtent à une crise de confiance croissante. D'une part, cela est dû à la prolifération des médias numériques et sociaux, avec une accessibilité sans précédent aux informations et à la variété des sources d'information pour le grand public.

D'autre part, cela est dû à la prolifération de fausses informations et des théories complotistes en ligne, qui ont mis en doute la crédibilité des médias traditionnels. Cette "guerre de l'information" engendre des conséquences non négligeables, notamment pour les conflits armés.

Le contrôle de l'information est primordial pour les Etats, gouvernements et groupes armés dans la guerre moderne. Ils utilisent ces médias dits traditionnels afin de façonner la perception du public face à la guerre en Iraq, en Syrie, et aujourd'hui la guerre Russo- ukrainienne sur laquelle nous allons nous appesantir.

1- En Iraq

Les médias traditionnels ont été utilisés et manipulés afin de légitimer l'invasion de l'Iraq en 2003. Des preuves erronées ont été présentées pour décrire « l'arsenal d'armes de destruction massive » détenu par Saddam Hussein.

2- La Guerre en Syrie

Afin de justifier leurs positions, les protagonistes de cette guerre ont utilisés les médias traditionnels pour véhiculer des récits différents dans le conflit syrien. Les rebelles opposés au régime de Bachar al Assad utilisent les médias pour témoigner de la violence du régime, tandis que ce dernier utilise les médias d'états pour les qualifier de terroristes.

3- La guerre en russo-ukrainienne

Les médias d'Etat dit traditionnels sont constamment utilisés pour donner une perception de la guerre en Ukraine.

La Russie utilise des médias d'État en présentant les rebelles pro-russes comme étant des défenseurs de la population russophone alors que les Ukrainiens utilisent des médias pour présenter les rebelles comme étant des militants soutenus la Russie.

« L'important dans une guerre informationnelle est d'avoir la main sur les opinions publiques » disait Xavier Eutrope journaliste à la revue des médias.

L'histoire récente du drone attaquant le siège du parlement russe est une excellente illustration de l'utilisation de la propagande sur fond de guerre.

Le 3 mai 2023 à Moscou, un communiqué du Kremlin annonce une attaque de drone sur le parlement russe sans dégâts matériels, ni de victimes. Les médias en ligne et les chaines de télévisions russes d'abord et celles du monde entier diffusaient déjà cette image. Les vidéos surveillance et vidéos amateurs montraient le film d'un drone abattu au-dessus de la coupole du palais des sénats au kremlin.

L'information a été relayée par toutes les chaines du monde provoquant une réaction des puissances mondiales.

Les services de presse du président et les médias russes affirment sans ambages que la résidence du chef de l'Etat était la cible de drones que les militaires et services de sécurité ont abattus et neutralisés. Comme un leitmotiv tous les médias russes qualifient cet évènement d'acte terroriste contre la Russie et en premier chef contre son président par le régime de « NAZI de Kiev » qui de fait doit être déclaré comme organisation terroriste. Nous rappelons que c'est la première fois que le Kremlin fait l'objet d'une attaque depuis la 2ème Guerre Mondiale.

La grande force des médias comme relais puissant de l'information pour servir de support et agir ainsi sur les masses populaires des nations et/ ou légitimer d'avance ce qui pourrait émouvoir toutes les nations du monde entier : telle est la tactique pour préparer les consciences à d'éventuelles atrocités que pourraient commettre la Russie.

Les termes odieux pour qualifier les dirigeants Ukrainiens ne manquent pas pour légitimer à souhait cette guerre de conquête de l'Ukraine de Vladimir Poutine comme étant une croisade contre le mal à la veille de la célébration du 9 mai. Cette fête grandeur nature de la victoire de l'union soviétique sur l'Allemagne Nazie diffusée sur toutes les chaines de télévisions russes est l'occasion de jouer la

surenchère et faire ainsi le parallèle entre la grande guerre Patriotique et celle menée actuellement pour la défense de sa patrie en Ukraine.

Progressivement mais surement la propagande russe marque dans la conscience collective russe l'image d'un ennemi Nazi terroriste à réduire au néant. Tous les parallélismes sont de l'ordre du possible allant jusqu'à une comparaison avec les attentats du 11 septembre 2001 contre les tours jumelles à New York avec un message principal : Ce n'est pas la Russie qui aurait déclaré la guerre à l'Ukraine mais bien le contraire.

La guerre de l'information est sans nulle doute ce qui déterminera l'avenir de la situation en Ukraine, mais aussi le futur de la paix et de la sécurité de toute la population mondiale. Malheureusement, cette guerre informationnelle est aujourd'hui hors de contrôle [149].

La guerre informationnelle est un moyen pour les acteurs de la guerre de contrôler la perception du public, créant tantôt la confusion totale, tantôt en imposant une vision particulière de la guerre. La crédibilité des médias traditionnels est aujourd'hui remise en question, ce qui a renforcé la méfiance du public à leur égard. Cependant une autre forme de désinformation beaucoup plus puissante et sophistiquée est pratiquée par la Russie et plus connue sous le nom de fermes à trolls.

Fermes à trolls

Les fermes à trolls sont des regroupements et organisations qui agissent sur Internet avec comme spécialité la désinformation. Les usines à trolls ou fermes à trolls recrutent, rassemblent et coordonnent des trolls dans le net, des hackers spécialistes payés pour diffuser de manière intelligente et coordonnée des informations partiellement ou totalement mensongères sur les réseaux sociaux.

Les méthodes et structures utilisées dans la campagne de désinformation relativement à l'actuelle guerre en Ukraine sont évidemment l'œuvre des usines des à trolls russe. Il s'agit littéralement d'une équipe d'employés, de stagiaires, de prestataires et d'experts du net logés dans une ou d'anciennes usines de saint Petersbourg avec comme mission principale essaimer le net avec des propagandes pro russe et antis occidentales à travers les plateformes numériques [150], Instagram, twitter…). Parmi leurs cibles des pays, des médias internationaux mais aussi des personnalités politiques.

Les usines à trolls spécialistes et experts de la fabrication, de la propagande constituent aujourd'hui un aspect de la guerre de l'information redoutable avec des moyens modernes [151].

C'est incontestablement un des éléments clé de la stratégie russe pendant cette guerre en Ukraine. Il s'agit bien d'une stratégie bien éprouvée depuis de nombreuses années, déjà en 2016 durant la campagne américaine avec la découverte de l'existence d'un organisme dénommé l'« Internet Agency Research » pour organiser des manifestations factices imitées des mouvements sociaux.

Si la Russie est citée en exemple sur cette méthode, une récente publication du 27 octobre 2021 de Gabriel Thierry prouve que cette pratique était aussi un jeu favori de la Chine. Le rapport s'inquiète sur les méthodes agressives de la Chine sur la toile : utilisation de fermes à trolls, de faux comptes, de doxing ou de loups guerriers…. Cette publication s'appuyant sur un rapport de l'ISREM (Institut de recherche stratégique de l'école militaire) permet de comprendre l'ampleur de telles pratiques et ses enjeux géostratégique et d'influence.

Faisant le parallèle sur les fermes à trolls russe de l'Internet Research Agency à Saint Pétersbourg, ce domaine intéresse de plus en plus l'armée populaire de libération chinoise.

Les contenus étant créés par des tiers et diffusés par d'autres rend leur traçabilité quasi impossible aiguisant ainsi l'appétit de Pékin à utiliser à outrance cette sous-traitance. Ainsi Sur l'île de Taïwan, un Etat souverain revendiqué par la République populaire de Chine, la ferme à trolls est ainsi très utilisée et partagée par des partis pro-réunification avec la Chine continentale s'immisçant ainsi dans les débats politiques locaux et étendre son influence.

Pékin mènerait aussi dans sa guerre informationnelle anti occidentale des opérations de Doxing (publications d'informations personnelles d'un internaute dans le but de lui nuire) plus précisément sur Hong-Kong. Cette ancienne colonie britannique depuis sa rétrocession à la Chine en 1997 voit ses libertés de plus en plus restreintes. Des militants prodémocratie y sont la cible de ses attaques orchestrées. L'origine des Dox, HKLeaks, serait attribuée aux autorités chinoises et à l'armée de libération chinoise. La pratique chinoise en la matière s'étend sur la création de faux comptes par le truchement de l'intelligence artificielle pour étendre sa propagande, mais aussi de l'utilisation de la diplomatie du loup guerrier rompant avec la diplomatie traditionnelle qui se montre très offensive sur les réseaux sociaux [152].

Les prises de parole des loups guerriers semblent étrangement portées par la création de comptes anonymes sur les réseaux sociaux. Exemple avec le compte Twitter de l'ambassade de Chine en Hongrie, suivi à 98 % par des non-Hongrois. Dont « un nombre anormalement élevé d'entre eux venant du Moyen-Orient, d'Asie du Sud et d'Afrique », rapportent les auteurs. Des abonnés localisés de façon disproportionnée au Pakistan. Un pays qui avait justement servi de plateforme d'essai aux débuts de la « twitterisation » diplomatique chinoise.

Les gouvernements occidentaux veulent impliquer les géants des plateformes numériques de l'internet et des réseaux sociaux dans la lutte contre ces campagnes de désinformation déstabilisantes, il s'avère cependant que vue la complexité du sujet l'intention est plus facile à matérialiser que la mise en œuvre.

Nous constatons au travers de l'analyse des couches physique, logique et sémantique du cyberespace que chacun de ces niveaux peuvent impacter les échanges et les risques s'y afférents.

Que ce soit la première strate des couches basses du milieu numérique au travers des câbles sous-marins de communication, la seconde par les chemins de la donnée ou la troisième par les plateformes d'intermédiation relèvent de multiples enjeux géopolitiques et stratégiques.

Source : la revue des médias INA

Figure 28 : Usines à trolls russes: la revue des médias

À l'ère numérique, la protection des flux d'information et des infrastructures dédiées est devenue un enjeu de sécurité majeur pour tous les dirigeants. Cette question touche à la sécurité nationale dans la mesure où des adversaires extérieurs peuvent mettre en péril la stabilité d'un pays et porter atteinte aux

fondements de son système politique en catalysant le mécontentement, en manipulant des informations et en menant des campagnes d'influence.

LES ENJEUX D'UNE MONTEE EN PUISSANCE, LES NOUVEAUX OUTILS ET FUTURES PERSPECTIVES D'ENGAGEMENTS

La notion de cyber puissance a des limites mouvantes, mais lorsqu'on cherche à déterminer une définition basique, la puissance économique est un indicateur à corréler mais limitant. De ce point de vue, les cas de la République Populaire de Chine *(RPC)* et des Etats-Unis peuvent paraître d'excellents modèles matures, mais leur histoire et caractéristiques intrinsèques ne sont pas copiables. Les risques et menaces identifiés précédemment nous ont montré que dans ce champ de conflictualité qu'est le cyberespace, un déséquilibre de fait existe à l'avantage des Etats dits non-démocratiques. Il est intéressant dans ce cas, de se poser la question d'une méthode ou tout du moins, une stratégie de montée en puissance des moyens de lutte informatique défensifs et offensifs.

Enjeu de compétitivité mais également de survie pour certains, la création d'un écosystème numérique solide et pérenne, demande aux États et aux entreprises, une adaptation à des nouveaux modèles d'organisations plus horizontaux. Face à des menaces et à des attaquants de plus en plus spécialisés, protéger leurs infrastructures vitales est un défi permanent. Dans ce contexte, un premier jalon pourrait être la mise en place d'un tel écosystème. Pour cela, une volonté étatique nous paraît indispensable pour établir une stratégie d'obtention de moyens défensifs, offensifs, économiques ou de formation.

Pierre angulaire de cette stratégie, la lutte informationnelle dans le champ cybernétique a récemment élargi le concept traditionnel d'influence que les armées utilisent depuis plus de 2500 ans. Outil offensif hybride, désormais également utilisé dans l'infosphère privée, la cyber-influence connaît des développements dont les limites n'ont pas été atteintes.

En définitive, cette montée en puissance des Etats dans le champ informationnel renforce leurs besoins de maîtrise des technologies disruptives comme la cryptographie, le quantique, le new space ou les concepts de souveraineté. Les problématiques liées que sont la résilience et l'efficience peuvent s'illustrer par la préparation d'un exercice de prospective.

QUELLE RECETTE POUR UN ECOSYSTEME MATURE ?

La croissance des menaces

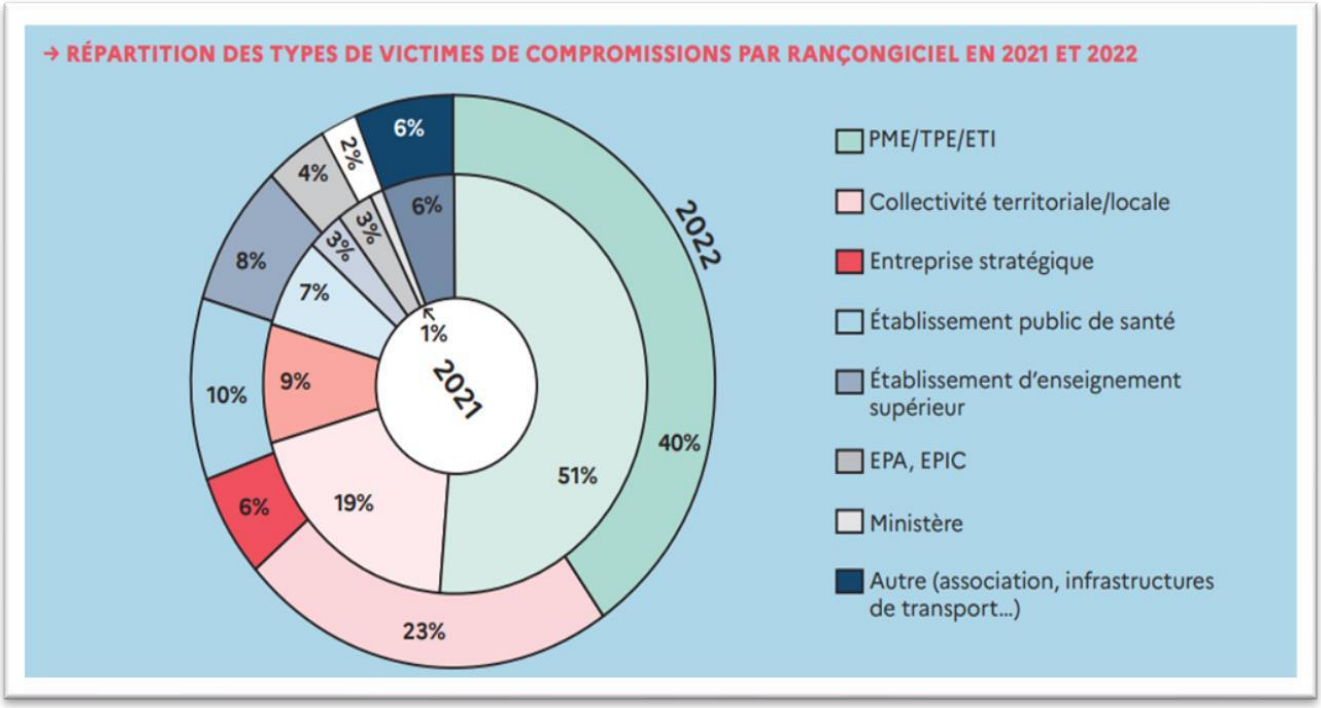
La numérisation du monde progresse à un rythme effréné, et ce dans toutes les sphères sociales. Les objets et lieux connectés, les applications et progiciels de gestion se développent de plus en plus sur le marché. La conséquence de ce développement est un élargissement croissant de la surface d'attaque des infrastructures numériques.

Pour le cas de la France, si les menaces cyber recensées concernent moins les opérateurs régulés par l'ANSSI, les entités les moins protégées deviennent de facto les cibles privilégiées des attaquants [153]. De

manière générale, le niveau du risque est élevé. Bénéficiant de leur avantage, les attaquants sont de plus en plus performants.

On note à ce titre une tendance de la part des cyber attaquants étatiques, à l'imitation des vecteurs d'attaques traditionnellement utilisés par les cybercriminels *(utilisation massive de rançongiciels)*, afin de maintenir un lien discret avec le réseau ciblé. Les attaques dites de « supply chain », qui visent la compromission d'éléments périphériques d'un système d'information *(comme les sous-traitants, prestataires, fournisseurs)*, sont également parmi les plus pratiquées.

Les collectivités locales ou territoriales sont très touchées par les cybermalveillances. Cibles de choix, elles sont le parent pauvre des représentants du gouvernement et ont un retard en infrastructures à rattraper.



Source : ANSSI

Figure 29: Panorama de la cybermenace 2022

Les objectifs malveillants sont toujours les mêmes : obtenir un gain financier, espionner un concurrent ou faire des opérations de déstabilisation. Pour cela, ce sont souvent les vulnérabilités les plus diffusées qui servent de points d'entrées, et dont les mises à jour correctives ne sont pas faites par négligence.

Ainsi, il apparaît clairement que la majorité des attaques cyber sont effectuées dans le champ commercial ou auprès de systèmes civils. Cette tendance peut s'expliquer par le fait que le développement des infrastructures liées à l'internet civil s'est fait à une époque de paix relative, sans prise de conscience du concept de « security by design ». Il en résulte que les systèmes civils sont en quelque sorte le ventre mou de la sécurité informatique.

Dans ce contexte, il est légitime de se demander si la responsabilité de la mise en place des moyens de sécurisation ne devrait pas incomber aux acteurs du champ commercial et civil, qui sont les cibles privilégiées des cyber attaquants ?

Un commencement de réponse serait la prise en compte du risque cyber à sa juste valeur, ainsi que le suivi des bonnes pratiques d'hygiène informatique [154]. Des moyens de développement des capacités de détection des attaques, associés à une sensibilisation régulière des personnels pourraient être pris en compte. Malheureusement, dans une économie du temps de paix, la rentabilité est le maître mot. Et sans l'intervention d'un cadre normatif restrictif, les arbitrages budgétaires des entreprises ne vont traditionnellement pas dans le sens de la sécurisation des infrastructures ou du patrimoine informationnel.

Avec leurs pouvoirs régaliens d'édition des lois et d'administration, les États et entités étatiques tiennent une place naturelle de régulateur. On pourrait donc penser que le responsable semble être désigné. Mais comme vu précédemment, le chemin vers la régulation de l'écosystème numérique n'est pas terminé. La construction législative se heurte à l'inertie du changement.

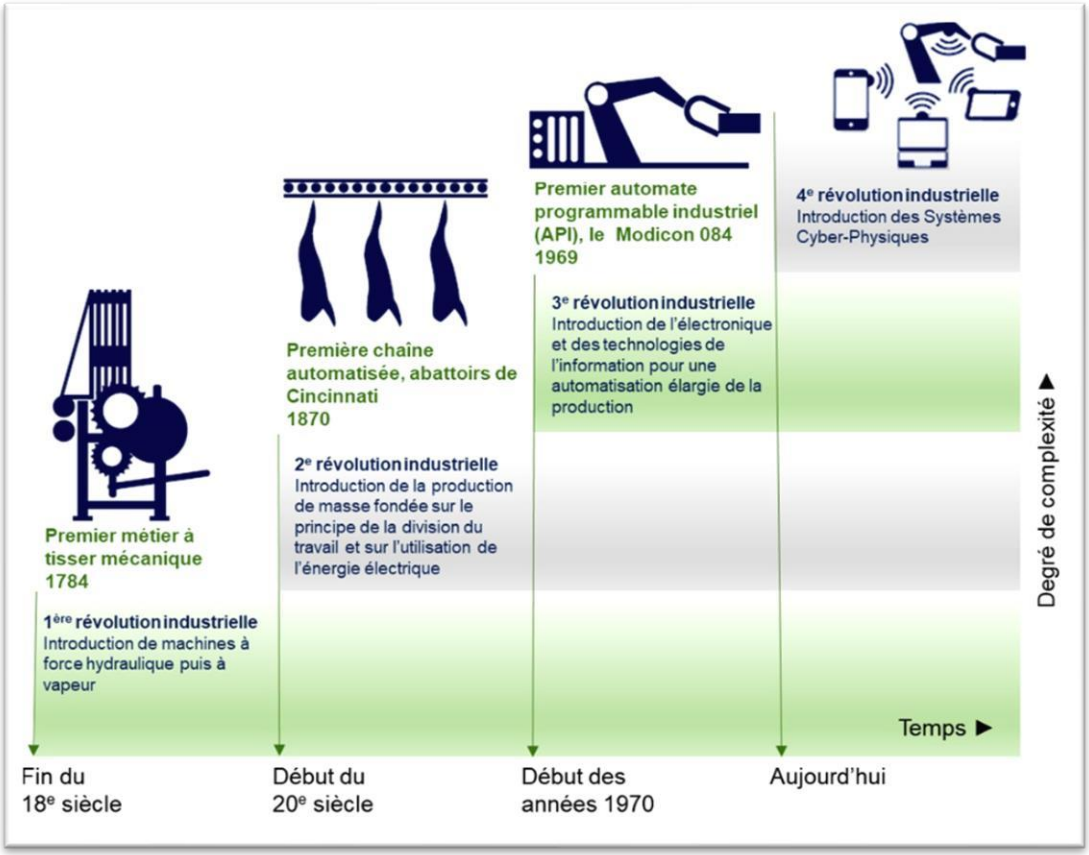
Investissements, R&D, formation : les économies européennes en construction

Le caractère évolutif des technologies liées à l'écosystème cyber et les méthodes employées par les attaquants rendent la quête d'une maturité totale, un objectif permanent. De plus, les éléments socio-démographiques, géographiques et de développement économique de chaque pays, sont autant de critères pouvant modifier certains aspects de cette maturité. Se fier à un des nombreux indicateurs de comparaison pour déterminer les leaders et donc les meilleurs modèles *(Global Cybersecurity Index, National Cyber Security Index, National Cyber Power Index etc.)*, pourrait amener à une mauvaise interprétation du résultat, du fait des méthodes d'analyse et de classement différentes [155].

Une manière d'aborder le sujet de la montée en puissance pourrait être de prendre en compte les thématiques investissements, écosystème d'entreprises, recherche et développement *(R&D)* et formation de la filière cybersécurité. Les pays de l'Union européenne sont des exemples intéressants du fait de leur politique réglementaire commune. Les efforts sont ainsi équilibrés sur l'ensemble du territoire de l'UE. Le programme Horizon Europe 2027 [156] est le programme clé de financement de la recherche et innovation. Mais la mise en perspective par rapport au marché mondial, montre les différences de motivation. L'exemple de l'intelligence artificielle est parlant : sur les 300 milliards de dollars d'investissements dans l'intelligence artificielle *(IA)* estimés au niveau mondial en 2023, l'Europe tiendra la deuxième place avec plus de 20% [157].
La réalité est que les Etats-Unis *(50%)* et la RPC *(environ 20%)* font cavaliers seuls dans cette course. La stratégie française fait partie du plan France 2030 qui vise à accélérer la transformation des secteurs clés de l'économie par l'innovation [158], mais les efforts mis sur la table *(1,5 milliards d'euros à horizon 2025)* semblent dérisoires par rapport aux leaders du marché. Pire, selon une récente étude initiée par les principales organisations européennes en IA *(113 start-ups et 7 fonds venture capital sondés)*, le cadre réglementaire restrictif du futur AI act empêchera le développement de la filière et devrait engendrer des relocalisations hors Union Européenne *(UE)*, des coûts de mise en conformité pour les startups européennes, et des investissements hors UE [159].
D'autres technologies de rupture semblent en revanche portées en avant par les instances européennes, comme les investissements dans les technologies quantiques *(calcul quantique et chiffrement quantique)*. Des projets bilatéraux semblent initiés comme le protocole d'accord bilatéral de coopération dans les technologies quantiques du 31 août 2021 entre la France et les Pays-Bas, ou l'initiative OpenQKD qui vise à sécuriser les données des infrastructures critiques via la distribution de clefs quantiques. La France est

en revanche la mieux représentée via plusieurs grands industriels et organisations *(Thales, Orange, le CNRS…)* [160].

Le paysage industriel européen est quant à lui, plus difficile à structurer. Il existe une diversité de profils que l'on peut réunir sous l'appellation de base industrielle et technologique de la cybersécurité *(BITC)* [161]. L'analogie volontairement calquée sur le monde de la défense est un premier indice d'une corrélation évidente entre les deux filières. Devant faire face aux deux pôles leaders que sont ceux de la RPC et les Etats-Unis, la stratégie européenne a pour but de créer un marché unique souverain et un pôle de compétence.



Avec une offre couvrant tous les secteurs *(B2C – Business to customer, B2B – Business to business, B2G – Business to government)*, quasiment tous les schémas de ventes sont présents, ainsi, segmenter cet écosystème par solution ou client peut permettre d'offrir une grille de lecture simplifiée. Les multinationales spécialisées dans l'intégration sont représentées *(pour l'essentiel américaines : Microsoft, IBM, Dell, Cisco, etc.)*, tout comme les équipementiers *(STMicroelectronics, Schneider Electrics, Siemens, etc.)*. Ce sont des acteurs pivots du marché. Sont également représentés, les éditeurs de logiciels et d'applications *(Symantec, Kaspersky, etc.)* ainsi que les Entreprises de Services Numériques *(Atos, Cap Gemini, Sopra Steria etc.)*. On peut également noter l'entrée sur le marché de groupes télécoms *(Orange, British Telecom etc.)* mais aussi de défense *(Thales, Airbus, BAE, Rhode & Schwarz, Leonardo etc.)*.

Une approche géographique cette fois, permet de distinguer les pôles les plus dynamiques. Les capacités de cette BITC sont essentiellement concentrées sur trois pôles. En Allemagne par exemple, on trouve des acteurs spécialistes des infrastructures et réseaux sécurisés *(Secunet, Rhode & Schwarz, Siemens, Deutsche Telekom, etc.)* qui soutiennent un marché de plus de 6 milliards d'euros en 2021. Ils participent tous depuis 2011 à l'effort de soutien du plan Industrie 4.0 [162].

Source : Acatech, Forschungsunion (2013),
Umsetzungsempfehlungen für das

Zukunftsprojekt Industrie 4.0 : Abschlussbericht des Arbeitskreises Industrie 4.0, avril 2013, p.

Figure 30: DFKI, 2011

Lancé sous le mandat d'Angela Merkel et alors que tous les Etats sont encore dans une stratégie d'outsourcing des capacités industrielles, ce plan met en place une stratégie qui a pour but de mettre l'industrie allemande à l'avant garde en développant la numérisation des usines, avec des technologies d'amélioration du rendement comme l'internet des objets, la réalité augmentée, le machine learning, l'intelligence artificielle ou encore le big data.

Les parties prenantes du projet Industrie 4.0 sont les acteurs de l'informatique appliquée, le gouvernement au travers du Bundesministerium für Bildung und Forschung *(BMBF, ministère de l'Éducation et de la Recherche)* et les acteurs de l'industrie des biens d'équipement. Le constat du succès de ce programme est grandement dû au soutien de l'Etat allemand à toutes les étapes de son développement.

Un autre pôle à considérer est celui du Royaume Uni, malgré sa sortie de l'Union Européenne. Avec plus de 1800 entreprises recensées et un marché de plus 12 milliards d'euros, la BITC britannique est très dynamique et attire de nombreux investissements étrangers. Fers de lance de cette industrie, on retrouve les entreprises BAE, Sophos ou encore Darktrace, qui sont considérées comme des acteurs majeurs de niveau mondial [163]. Les segments les plus importants représentés sont ceux des infrastructures logicielles, la gestion des identités et accès, les logiciels de contrôles de conformité. Le gouvernement a annoncé la mise en place d'une stratégie ambitieuse de renforcement de la résilience nationale face aux menaces cyber. Devenu incontournable, le sujet de la sécurisation des infrastructures critiques est également pris en compte dans cette stratégie, et plus particulièrement le secteur de la santé [164]. Il faut noter cependant, la place particulière qu'occupe le Royaume Uni dans la communauté du renseignement avec le GCHQ, qui est un des services les plus performants au monde dans les techniques de renseignement électromagnétique, et qui est partie prenante de l'alliance des « 5 eyes ».

Dernier élément du trio de tête mais pas par la taille, la BITC française. Son marché atteint 14,1 milliards d'euros en 2021, en hausse de 7% par rapport à l'année précédente. Cet écosystème est composé de plus de 2100 entreprises *(dont 75 grandes entreprises, 70 ETI , 671 PME, 1 342 microentreprises générant moins de 2 millions de CA en 2021)* [165]. On retrouve des acteurs historiques des infrastructures *(Orange),* d'électronique de défense *(Thales, Safran)* et des entreprises de services numériques *(Atos, Capgemini, etc.)*.

Figure 31 : Sociétés de cybersécurité françaises

A l'heure actuelle, la stratégie française de développement de la cybersécurité n'a réellement pris corps que récemment. Lancée en février 2021, la stratégie nationale d'accélération de la cybersécurité présente 4 piliers [166]:

- Le développement des solutions souveraines et innovantes de cybersécurité.
- Le renforcement des liens et synergies entre les acteurs de la filière.
- Le soutien à la demande (individus, entreprises, collectivités et État).
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre.

Avec une volonté de permettre la création de 37 000 emplois supplémentaires, l'effort français se porte sur une gradation du niveau d'expertise sur le modèle pédagogique *existant (de Bac pro à Bac + 8)*. Élever la sensibilisation de la population, deuxième axe de ce plan formation, permettrait de renforcer le niveau de sécurité globale en apportant un "vernis cyber". Le cycle de vie extrêmement court des produits du monde numérique ajoute une problématique sur l'obsolescence quasi programmée des programmes de formation.

Pour faire face à cela le plan France 2030 indique *: « La stratégie propose également d'établir un meilleur diagnostic sur le long terme des besoins, métiers et formations existants et de communiquer pour orienter les étudiants de manière plus efficace ».*

Il apparaît également que le développement de formations courtes de type "qualifications", pourrait répondre à cette problématique de ruptures technologiques intermédiaires.

L'ensemble de ces mesures est inclus dans le plan France 2030, qui a pour but de relancer la compétitivité française dans les secteurs d'avenir de production.

Les récents événements géopolitiques entre les pôles Russo-Ukrainien et Sino-Américain, ont également motivé le gouvernement et le ministère des armées à présenter la nouvelle mouture de la loi de programmation militaire pour la période 2024-2030 [167]. Le doigt a été pointé sur les lacunes structurelles, notamment cyber et traduit en en objectifs de lutte informatique offensive (LIO), lutte informatique défensive (LID) et lutte informatique d'influence (L2I).

Dans le deuxième cercle de la BITC Européenne, composé d'acteurs de niche de moindre taille *(Italie, Espagne, Suède ou Estonie)* le cas de l'Estonie est intéressant du fait de son histoire et de sa frontière commune avec la Russie. Au sortir de la Deuxième Guerre mondiale, l'Allemagne nazie laisse la place à l'URSS, qui occupe le territoire estonien jusqu'en 1991.

L'attrait pour la technologie commence en 1965 avec le premier ordinateur soviétique dans une salle de classe. La stratégie du "bond du tigre" [168] est mise en place par les autorités estoniennes afin de fournir un ordinateur à chaque étudiant du pays *(17 000 à l'époque)*. Le pays est confronté à une fuite de données sensibles des citoyens en 1995 *(Noms et adresses, numéros de carte d'identité, numéros de téléphones, enregistrements téléphoniques et bancaires)* qui furent compilées et vendues par un hacker autodidacte estonien [61]. L'initiative de centraliser les données des citoyens est mise en place en 2001 avec la création du logiciel X-road. Lors de la "crise du soldat de bronze" [169], les tensions apparaissent entre la Russie et l'Estonie après qu'une cyberattaque massive paralyse des sites gouvernementaux, de banques et de médias pendant plusieurs heures. Le gouvernement estonien prend alors la décision de se constituer une capacité militaire de LIO et de LID à travers la Cyber Unit
[170].

Depuis le début du conflit russo-ukrainien, on assiste à une croissance de 30% du nombre de cyber soldats estonien. Eesti Kaitseliit, la ligue de défense estonienne *(groupe né au moment de l'indépendance de l'Estonie en 1991)*, peut compter sur 350 bénévoles qui utilisent leurs drones pour surveiller la frontière avec la Russie.

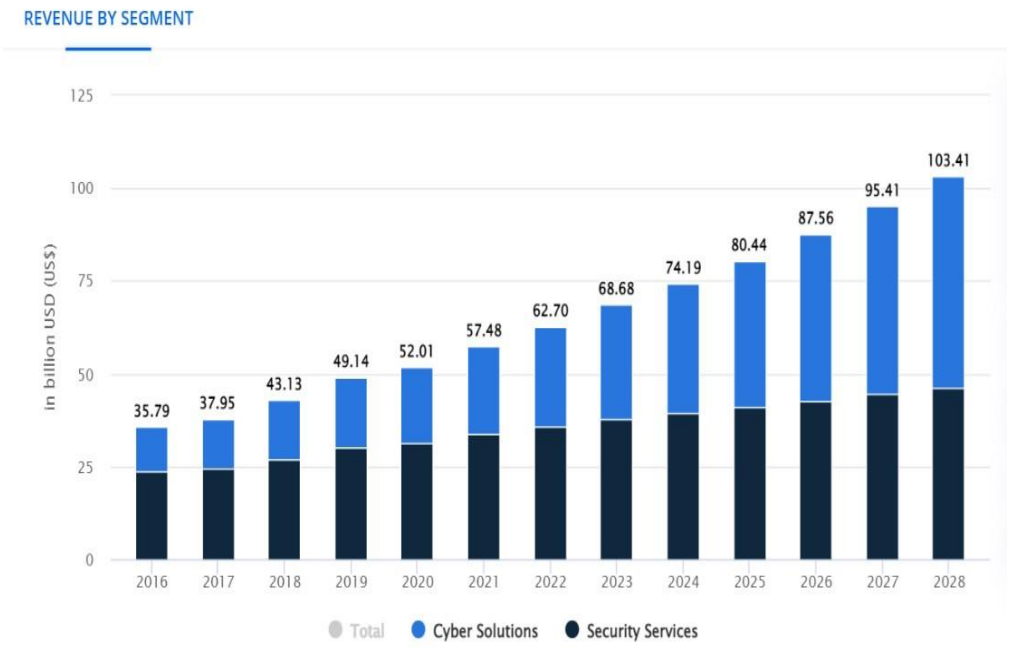
La BITC estonienne possède également une « licorne » dans la cybersécurité avec la société Guardtime.

Depuis 2018, une initiative française de Gov Tech, nommée France identité [171] a pour objectif de proposer un accès à des services publics ou privés. Le service est censé apporter de la sécurité durant les phases d'utilisation. Ce projet de digitalisation des données sensibles annonce une volonté étatique de répondre aux problématiques de souveraineté numérique, en rétrécissant la frontière entre identité physique et identité numérique. Les avancées sociétales pourraient à l'avenir rendre inutiles les procédures de MultiFacteur Authentification *(MFA)*, et la biométrie dans ce cas sera la technologie d'avenir.

Les économies du temps de guerre : un modèle à suivre ?

Etats-Unis

Berceau historique du développement de l'internet et première puissance mondiale, l'écosystème d'entreprises de cybersécurité américain est le plus développé au monde. Les leaders de l'industrie numérique que sont les GAFAM sont les moteurs de l'économie nationale. Ils contribuent également au développement de cet écosystème par des investissements massifs.



Figur32 :Cybersecurity market - United States, March 2023, Statista

Durant l'année 2021, l'administration américaine annonce vouloir renforcer la cybersécurité globale du pays, et s'appuie sur les GAFAM dans cette tâche [172]. Cette relation entre l'Etat et les entreprises, est la force de cette économie.

La contrepartie de l'Etat dans cette stratégie, est un soutien par la création d'un arsenal juridique cyber *(Patriot & Cloud Act, Persistent Engagement, ITAR)* qui permet d'étendre l'influence et la domination des entreprises américaines sur les marchés. Depuis l'arrivée de l'administration Biden, on assiste également à un renforcement du protectionnisme aussi bien dans le discours que dans les actes *(Inflation Reduction Act du 16 août 2022)*. Le but à peine caché est de renforcer la production américaine. Tendance qui semble suivie dans les grandes puissances commerciales *(UE, Japon)*.

Avec un budget supérieur à 800 milliards de dollars pour 2023, la puissance économique et technologique de cet écosystème sert également de marché pour ces entreprises de cybersécurité. Les plus grandes entreprises de la défense américaine développent toutes des produits ou services cyber, ce qui confirme la fonction de catalyseur d'une base industrielle et technologique de défense.

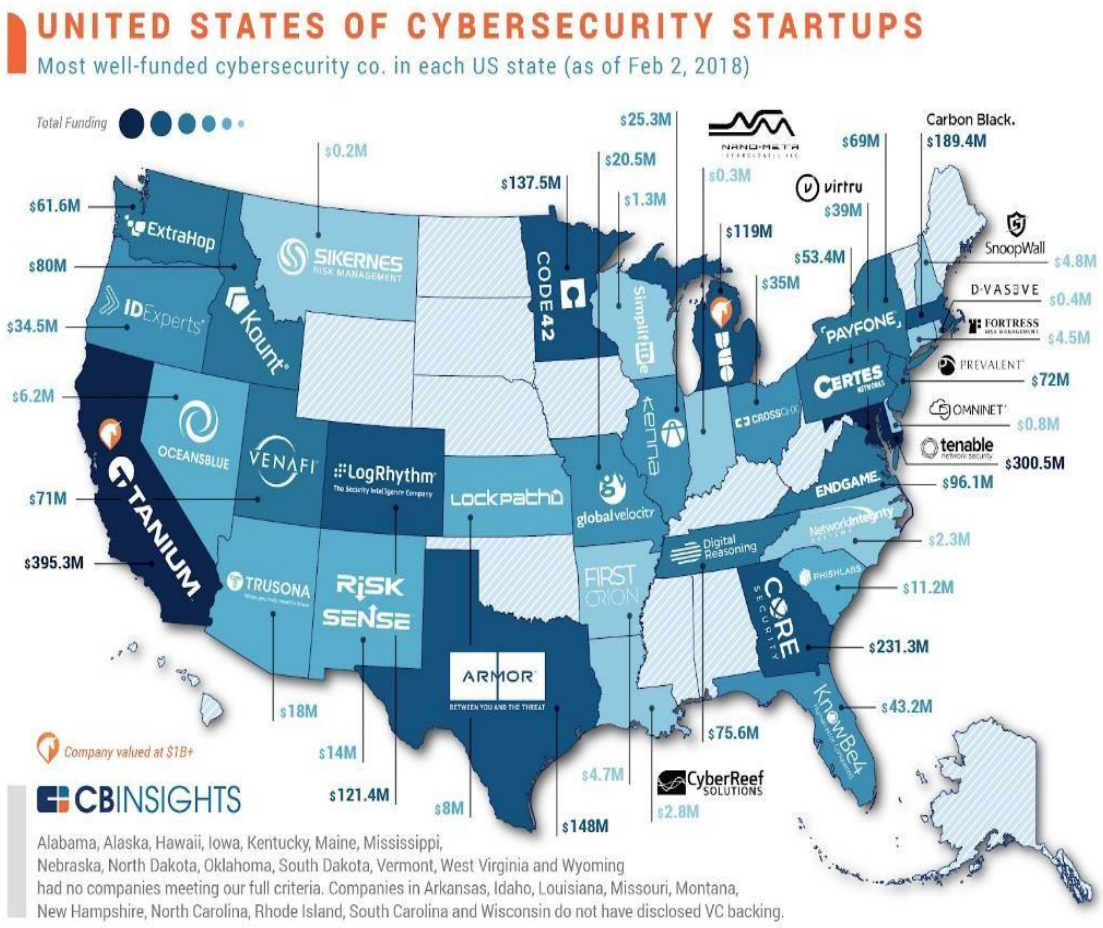


Figure 33 : USA cybersecurity startups

Le pivot stratégique américain vers le sud Pacifique, motivé par le nouvel ennemi chinois, est traduit dans le cyber par une volonté de renforcer la sécurisation de l'IoT [173] avec l'IoT Cybersecurity Improvement Act [174]. Une harmonisation des standards de certifications inter-agences serait un autre axe de cette stratégie. Le rééquilibrage des approvisionnements en délocalisant certains éléments de la chaîne de valeur technologique a été conforté par le CHIPS Science Act [175], en vue de garder un avantage compétitif notamment dans le développement des microprocesseurs.

L'organisme clé dans cette stratégie est le NIST *(National Institute of Standards and Technology)*. Il est responsable du renforcement de la sécurité des infrastructures critiques [176] et du développement de la sécurisation des logiciels [177]. Il pilote également une initiative nationale sur la prise en compte des enjeux de formation [178].

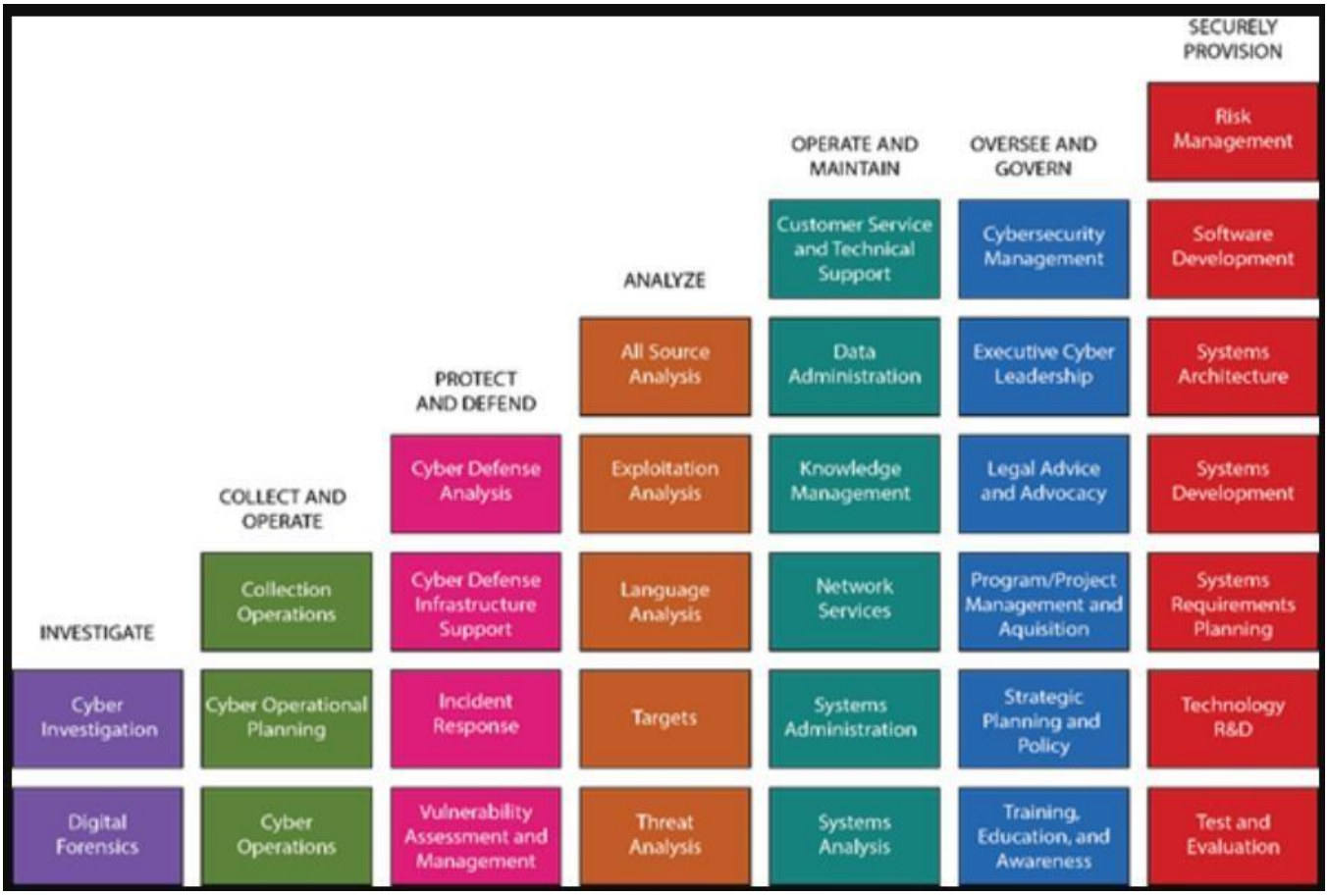


Figure 34 : Framework NICE

Baptisé NICE Framework, ce programme a été créé par l'administration Bush en 2008 afin d'augmenter la taille et la capacité de la compétence en cybersécurité de la société américaine. Il propose un référentiel commun de tâches à maîtriser, de connaissances de pratiques et qualités nécessaires pour réussir dans les métiers de la sécurité des systèmes d'information. Il est à destination des entreprises, organismes de certification, écoles et universités, institutions scientifiques et conseillers en cyber sécurité. L'approche américaine est donc d'unifier les pratiques et le langage sans forcément rigidifier les formats de formations.

Les agences étatiques comme le FBI sont également sollicitées dans des chantiers en lien avec la lutte contre la menace ransomware [179]. En collaboration avec le CISA, ils sont à la tête du Joint Ransomware Task Force (JRTF), une alliance de 30 pays réunis dans l'optique de partager du renseignement sur la menace ransomware. Le leadership dans le développement des technologies post-quantiques, semble être un autre grand thème de cette stratégie [180].

En définitive, le modèle américain démontre des points forts dans son écosystème d'entreprises, son leadership normatif, sa base industrielle et technologique de défense puissante et sa maîtrise des infrastructures. Le conflit potentiel avec la RPC semble être un élément de justification pour le développement d'une stratégie de repli sur soi, et de renforcement des capacités cyber, avec en filigrane la préparation pour une confrontation multi champs multi domaines *(MDMC)*.

Israël : incubateur de talents

La BITC israélienne est tournée vers l'innovation. 25% des start-ups sont dans la cybersécurité *(soit environ 300 entreprises)*. Plus 40% des investissements mondiaux en cybersécurité sont fait en Israël *(soit plus de 15 Md$ en 2022)* [181]. 80% de ces investissements sont faits en R&D.

La construction de cet écosystème à succès est due à deux raisons. La première est de nature historique. Dès les années 1960 un développement d'entreprises technologiques commence. Soixante ans plus tard, ce que les Israéliens appellent la Silicon Wadi, est l'héritière [182] de cette initiative, qui n'est plus concentrée dans une vallée mais dispersée sur l'intégralité du territoire.

La deuxième raison est d'ordre existentiel. En effet, l'Etat d'Israël se trouve à un carrefour civilisationnel, un environnement instable qui a obligé les pères fondateurs à intégrer dans leur pensée stratégique, un concept de sécurité nationale autour de plusieurs axes, dès sa création en 1947. L'idée d'une supériorité qualitative qui contrebalance l'infériorité quantitative. Ce concept a donc permis le développement du renseignement comme avantage tactique afin d'anticiper et dissuader. La Recherche et le développement dans les nouvelles technologies devenait une question de vie ou de mort.

Les pères fondateurs se sont reposés sur un socle académique scientifique de qualité et préexistant à la formation de l'Etat, comme le Technion d'Haïfa *(1912)*, l'Université hébraïque de Jérusalem *(1924)* et l'Institut Weizmann des sciences *(1934)*, afin de former et d'investir dans les technologies de l'innovation. L'informatique est développée très tôt *(Weizac, premier ordinateur israélien en 1950)*, ce qui a lancé l'Etat à soutenir les projets qui ont mené à la maturité du système académique [183].

L'armée à en parallèle compris très tôt le potentiel mais aussi les menaces de l'outil cyber, et a décidé de développer ses capacités à travers un processus de recherche de jeunes talents dès le lycée, afin de mettre à profit leurs compétences dans une unité spécialisée en renseignement électronique : l'unité 8200. Formés, les personnels faisant partie de cette unité ont la capacité de pouvoir développer des technologies, et de les commercialiser par la suite. Ce parcours exceptionnel n'étant pas la norme, la plupart des personnels de cette unité viennent abonder les rangs de l'écosystème d'entreprises de cybersécurité Israélienne.

Ce rôle d'incubateur permet un feu roulant générationnel d'esprits créatifs, et prouve les liens étroits qui existent entre le privé et l'Etat. Selon Nicolas Ténèze, auteur de Israël et sa dissuasion : Histoire politique d'un paradoxe, *« En Israël, il n'y a pas véritablement de frontière entre le militaire et le civil, les deux sont perméables et se développent ensemble, mutualisent leurs compétences »*.

On remarque également que cette expertise est recherchée à l'étranger. L'Etat joue alors le rôle de facilitateur, coordinateur ou arbitre dans les négociations avec les parties prenantes. La cybersécurité est donc un outil d'influence majeur qui reste difficile à maîtriser lorsqu'il s'agit de business. Les récents scandales autour de l'utilisation d'outils cyber offensifs israéliens [184] ou de lutte informatique d'influence viennent ternir le portrait d'un système modèle dont d'autres pays veulent imiter le succès.

Russie : Souveraineté numérique en construction

La promulgation de la loi sur un système internet fermé, le Runet, du 4 novembre 2019 semble avoir posé les jalons d'une dynamique de repli sur soi russe pour mieux maîtriser ses frontières numériques.

La construction de ce réseau commence de manière un peu chaotique dans la décennie 1991 - 2000. En effet l'Etat doit se reconstruire et place ses efforts sur d'autres sujets. En 1998 pourtant, le gouvernement

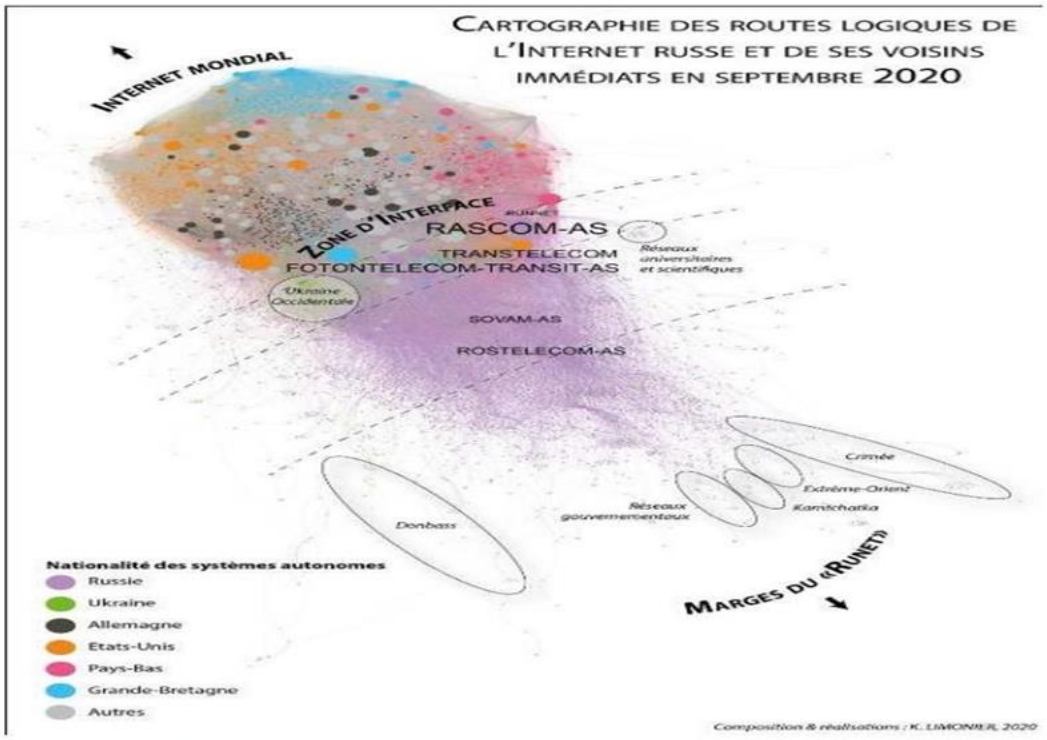
Russe juge que les enjeux du numérique et de l'informatique sont l'un des thèmes majeurs des conditions de sécurité des relations internationales.

La place de la souveraineté numérique commença à s'imposer dans le débat russe au tournant des années 2010.

Deux événements vont marquer l'année 2013 et changer la vision du pouvoir russe sur l'outil cyber : les révélations d'espionnage massif de la NSA au profit du gouvernement américain par Edward SNOWDEN et la doctrine GERASIMOV sur la prise en compte des moyens cybernétiques comme multiplicateur d'effets des guerres hybrides du futur.

Le mouvement est en marche et le pouvoir russe se met à légiférer dans ce sens.

Dans la foulée en 2014, la Douma promulgue une législation [185] sur la localisation des données des personnes physiques et morales russes sur le territoire national. Puis les lois Larovaïa [186] renforcent cette tendance en forçant les entreprises agissant sur internet à stocker les métadonnées de leurs utilisateurs sur le territoire national pour une durée de 3 ans. Elles doivent également fournir un accès à leur plateforme par une "porte dérobée" et une copie de leurs clés de chiffrement afin de permettre aux services de sécurité d'investiguer.



Source : données GEODE. Auteur : K. Limonier, 2020.

Figure 35 : Cartographie des routes logiques de l'internet russe

Selon Kevin Limonier *« La stratégie adoptée par la Russie est donc celle d'un contrôle intégral des données circulant sur le réseau, avec l'ambition d'établir de véritables « frontières numériques » dans un cyberespace dont on a longtemps prétendu qu'il ne pouvait en posséder et qu'il échappait à la géographie et aux pouvoirs »*.

Le dialogue avec les acteurs du numérique n'est pas forcément aligné avec le Kremlin sur ces sujets, comme l'indique l'échec du blocage de la messagerie Telegram dont le directoire refuse de communiquer les clés de chiffrement. Les représailles de l'Etat russe contre la société fondée

par Pavel Dourov ont engendré des incapacités d'accès sur des services étatiques dues aux interconnexions avec des services étrangers [187].

Ces difficultés de blocages montrent une stratégie du Kremlin à deux vitesses, qui doit être conduite en conjonction de moyens de transformation d'un réseau qui est physiquement lié à l'internet mondial. La cartographie de la couche basse du réseau russe faite par le travail de Kevin Limonier démontre ainsi les nombreuses interconnexions sur la frontière ouest du territoire.

L'internet russe est de plus composé de nombreux acteurs avec par exemple plus de 6575 systèmes autonomes (AS) en 2020, soit le troisième plus grand nombre au monde (2111 pour la France) 188. Plus surprenant, selon un rapport de 2015 de la cour des comptes russe, le pays contiendrait plus de 15433 Fournisseurs d'Accès Internet (FAI). Ce grand nombre de FAI s'explique par une défiance chronique de la population sur le contrôle étatique. Les initiatives d'installation de routeurs (TSPU) permettant la filtration des flux se heurtent à la résistance passive de certains relais locaux 189.

Si la réduction des points d'entrées est un processus lent pour des raisons techniques, on assiste à un pivot des points d'entrées du réseau russe historiquement à l'ouest *(pays frontaliers)* vers le Sud-est *(Chine)*. La déconnection totale reste également un objectif lointain, et la hausse du rythme de cette stratégie ne pourrait-elle pas voir le développement potentiel d'un marché noir de la connexion satellitaire ?

Instrument de contrôle et non de développement, la formation aux métiers ou sciences liées à internet n'est en revanche pas la priorité du gouvernement. Si la qualité de l'enseignement académique reste de très bon niveau, notamment en mathématiques, elle reste « bien plus défaillante dans les domaines appliqués », selon K. Limonier. Il poursuit en ajoutant que cela « explique non seulement la faiblesse de la Russie dans les domaines matériel et logiciel, mais aussi la nécessité de recourir à des trolls mercenaires ».

Les infrastructures critiques, terrain potentiel du seuil de l'agression?

La définition d'infrastructure critique est une notion à géométrie variable au cours du temps, qui a commencé à émerger après la deuxième guerre mondiale mais dont la dimension informationnelle s'est développée en parallèle des progrès de l'informatique et des signaux électromagnétiques.

Les Etats Unis sont les premiers à intégrer la notion de Critical National infrastructure en 1995 après une série d'attentats sur leur territoire (world trade center 1993, Oklahoma city) et celui du métro de Tokyo. L'attaque du 11 septembre 2001 perpétrée par des membres du groupe salafiste Al Qaïda sur New York et Washington vont cristalliser l'importance de parer les menaces terroristes dont l'impact n'avait jamais été estimé correctement. À partir de ce moment-là, les entités de la défense dans son intégralité, seront les garantes de la stratégie de protection des infrastructures critiques. Le Patriot Act donnera au Commandement de défense aérospatiale nord-américain (NORAD) la responsabilité des actions de protection contre ces menaces. L'ouragan Sandy frappe la côte Est des Etats-Unis en 2012. Le bilan officiel fait état de plus de 150 morts, et les dégâts matériels sont estimés à plus de soixante-dix milliards de dollars. Cet événement fait entrer les catastrophes naturelles dans le champ des menaces majeures contre les infrastructures critiques, du fait de leurs impacts sur les réseaux énergétiques, d'eau, et informationnels.

L'Union Européenne sera la première entité étatique à sanctuariser la catégorisation de domaines vitaux essentiels à la survie des Etats. La commission européenne mentionne onze catégories dans un livre vert en 2006 [190]

La prise de conscience française s'est faite très peu de temps après avec la création des dispositifs de Sécurité des Activités d'Importance Vitale (SAIV) [191]. Douze catégories sont créées pour différencier des secteurs d'activités (figure 6), et les rattacher à un ministre coordinateur qui devient de fait l'interlocuteur privilégié des problématiques/métiers liées. Une liste classifiée de plus de 200 Opérateurs d'Importance Vitale (OIV)est ainsi créée. L'intégration et la sécurisation des Systèmes d'Information d'Importance Vitale est un apport du ministère de la défense en 2013 dans son livre blanc de la défense nationale [192]. L'ANSSI coordonne la création de groupes de travail en lien avec les ministères afin de déterminer un calendrier de mise en application des mesures liées à la sécurisation de ces SIIV. Un décret codifie les mesures et les délais de mise en œuvre [193].

Sector	Product or service
I. Energy	1. Oil and gas production, treatment and storage, including pipelines 2. Electricity generation 3. Transmission of electricity, gas and oil 4. Distribution of electricity, gas and oil
II. Information, Communication Technologies, ICT	5. Information system and network protection 6. Instrumentation automation and control systems (SCADA, etc.) 7. Internet 8. Provision of fixed telecommunications 9. Provision of mobile telecommunications 10. Radio communication and navigation 11. Satellite communication 12. Broadcasting
III. Water	13. Provision ok drinking water 14. Control of water quality 15. Stemming and control water quantity
IV. Food	16. Provision of food and safeguarding food safety and security
V. Health	17. Medical and hospital care 18. Medicines, serums, vaccines and pharmaceuticals 19. Bio-laboratories and bio-agents
VI. Financial	20. Payment services/payment structures (private) 21. Government financial assignment
VII. Public & Legal Order and Safety	22. Maintaining public & legal order, safety and security 23. Administration of justice and detention
VIII. Civil Administration	24. Government functions 25. Armed forces 26. Civil administration services 27. Emergency services 28. Postal and courier services
IX. Transport	29. Road transport 30. Rail transport 31. Air traffic 32. Inland waterways transport 33. Ocean and short-sea shipping
X. Chemical and nuclear industry	34. Production and storage/processing of chemical and nuclear substances 35. Pipelines of dangerous goods (chemical substances)
XI. Space and Research	36. Space 37. Research
Source: Commission des Communautés Européennes, 2005, p. 24	

Figure 36: Les 11 secteurs d'importance vitale européens

La volonté de l'UE d'harmoniser les règles de sécurisation des systèmes d'information de chacun des membres a mené à la création de la directive NIS 2 le 10 novembre 2022. L'ambition de ce texte est de pousser les Etats et leurs entreprises à prendre la mesure du risque cyber sur les infrastructures critiques, mais la question se pose sur la faisabilité opérationnelle d'une telle réglementation dans une Union Européenne dont la maturité cyber de ses pays membres est inégale?
Cependant, les menaces dans la couche physique mentionnées dans la partie précédente sont un rappel de l'étendue d'une surface d'attaque aux dimensions difficilement estimables, et dont l'intérêt des attaquants semble grandissant [194,195].

Relation Etat / entreprise : zone de faiblesse à renforcer ?

Les exemples précédents nous ont montré les limites physiques et le rattrapage technologique qu'il est nécessaire de faire pour vouloir faire une transition d'un réseau interconnecté à un réseau fermé. Le rôle de l'Union Européenne dans ce sujet est plus un frein qu'une aide.

La problématique des infrastructures critiques est désormais bien identifiée, mais le fait qu'elles aient été développées par des sociétés privées dans une période de grande insouciance de paix relative a créé un décalage entre leur agenda commercial et les risques et menaces auxquelles elles font face. L'initiative NIS 2 est un commencement de solution mais les délais, les mesures et l'amplitude des éléments société concernées semblent trop éloignées de la réalité.

Une stratégie de montée en puissance des capacités cyber à un coût moindre serait d'attaquer le problème du côté du cadre règlementaire. Mais cela implique une relation Etat-secteur privé forte afin de créer une dynamique de développement de ce dernier avec le concours d'un complexe militaroindustriel comme terreau de développement. Côté français, la création du COMCYBER semble suivre cet axe, et les récents efforts dans les annonces stratégiques *(France 2030, Accélérateur de la Cybersécurité Nationale)* et les projets de défense *(LPM 2024-2030)*, demandent encore du temps pour donner des effets.

Le salut ne viendrait-il pas de la formation des jeunes générations sur un format israélien ? La force du complexe militaro-industriel français et le pivot technologique des stratégies de militaires vers le MDMC semble ouvrir une voie royale pour un développement de l'outil cyber.

La cyber-influence : un outil offensif complémentaire

Après avoir vu en seconde partie les différents risques et méthodes liés aux trois couches qui composent l'internet, nous aborderons dans cette partie un bref historique de l'utilisation de l'influence dans le contexte militaire depuis le cinquième siècle avant JC, pour ensuite se concentrer sur les moyens de défense et de contre-attaque potentiels que l'on peut mettre en place à échelle Étatique ou supra-Étatique.

Historique et Concept

Une des premières traces de l'utilisation de l'influence remonte au 5ème siècle avant JC dans le plus ancien traité de stratégie à ce jour : L'art de la guerre de Sun Tzu [196]. Si la période et l'auteur de l'œuvre sont sujets à débats, l'objectif de l'écrit est de vaincre l'adversaire sans effusion de sang, en passant par la maîtrise des actions psychologiques et de l'information. Souvent comparé avec ce précédent exemple, Arthashâstra est un traité de stratégie de Kautilya découvert au XXème siècle, où intervient la notion de : *« l'importance de façonner une fausse perception de la réalité dans l'esprit de l'adversaire tout en exploitant ses faiblesses par la séduction »* [197]. Mais la maîtrise de l'information autour d'un narratif commun et à destination du peuple apparaît pour la première fois en 1622 où dans le cadre du Concile de Trente, le pape Grégoire XV fonde la « Congrégation pour la propagande de la foi ». De là naquit le terme de « Propaganda », du latin « Propagare », c'est-à-dire propager, répandre [198].

L'utilisation de cette technique de diffusion de masse trouvera un essor certain au XXème siècle dans les démocraties occidentales. En pleine Première Guerre mondiale, en réponse à la découverte d'une agence allemande de propagande, plusieurs initiatives britanniques de manipulation de l'information furent lancées à destination des populations des pays neutres afin de les faire basculer en faveur des alliés [199]. Cette compétence acquise sera maintenue au sortir de la guerre par le Foreign Office. Un département similaire naîtra en Russie lors de la révolution de 1917, à destination de la population interne au pays. La propagande est classée en fonction de la source d'information : ouvertement identifiée *(propagande blanche)*, opérant sous fausse identité *(noire)* ou intentionnellement occultée *(grise)*. C'est durant la Deuxième Guerre mondiale que toutes les techniques détaillées précédemment seront utilisées et renforcées, que ce soit dans les pays de l'axe ou chez les alliés. L'utilisation de messages sur la radio publique, ou le largage de tracts seront fait dès 1941 par la Psychological Warfare Division [200]. Le but étant de produire un effet tactique, à savoir la baisse de moral des troupes allemandes.

En France, la prise en compte de l'outil informationnel durant un conflit commence avec la guerre d'Indochine mais prend réellement forme lors de la guerre d'Algérie avec la création du Traité Toutes Armes numéro 117 qui cadre "l'emploi de l'arme psychologique". La distinction est faite entre la guerre psychologique à destination de l'ennemi, et les actions psychologiques à destination des populations neutres ou amies.

Mais la communication qui est faite par les journalistes sur les conflits du Vietnam et de la guerre d'Algérie n'emporte pas l'aval de l'opinion publique.

Au cours des années 1980, les armées trouvent la solution permettant de faire d'une pierre deux coups afin de maîtriser le récit et ainsi la réputation auprès de l'opinion : la création d'un service de communication intégré et opérationnel. Dès lors, l'action des armées sera intégrée dans un narratif stratégique servant les besoins de politique intérieure et extérieure. Par la maîtrise des éléments visuels et sémantiques, on peut désormais valoriser l'action belligérante et dénigrer &l'ennemi.

Un nouveau phénomène change la donne et on assiste à une perte de contrôle de la communication par les armées : les fuites de données et les lanceurs d'alertes. L'enchaînement des scandales *(Abu Ghraib, wikileaks, Assange, etc.)* fait comprendre l'importance d'internet dans le succès de ces phénomènes. La cyber-influence devient un axe majeur de la stratégie des grandes puissances.

La puissance de l'appareil étasunien

La dimension stratégique d'une communication d'État a été formulée pour la première fois aux Etats-Unis en 2007. Avec le Président des Etats-Unis au sommet de la hiérarchie, le département d'Etat conduit la communication stratégique. En deuxième cercle se trouve le département de la défense qui s'occupe également de la manœuvre d'influence globale, et de l'appui informationnel aux opérations militaires. Les capacités opérationnelles sont divisées entre l'United State Special Operations Command *(USSOCOM)* et son équivalent dans le cyber *(CYBERCOM)* [201].

La diffusion de contenu en ligne est le premier axe de l'influence américaine. C'est le Global Engagement Center qui en est responsable. Pour mener à bien ces opérations, le Web Ops Center du CENTCOM est chargé de la création et de la gestion des personas et avatars en ligne. Des moyens de lutte informatique offensive sont souvent ajoutés à ces opérations de lutte informatique d'influence.

Pour avoir un impact de masse sur la sphère informationnelle, l'emploi de prestataires est inévitable. Cette coopération se fait sous le format de la délégation [202]. Des entreprises de taille majeure comme la CACI *(22 000 employés et 6,5 milliards de dollars de chiffre d'affaires en 2022)*, ou la SAIC *(26 000 employés et 7,5 Md$ de chiffre d'affaires)*, Booz Allen Hamilton *(29 000 employés et 8,3 Md$ de chiffre d'affaires)*, ou de plus petite envergure comme KeyW, Secure Mission Solutions, Vencore. Leur cadre contractuel leur permet même de contribuer et mener des opérations offensives et défensives [202]. Ces cybers mercenaires semblent ne pas avoir les mêmes problématiques que leurs homologues portant des armes, le CENTCOM est garant du contrôle de leurs actions [202].

La cyber influence russe, levier d'existence géopolitique

Contrairement au modèle américain, la stratégie d'influence russe repose sur l'idée que l'information est une ressource stratégique et une arme de guerre qui s'utilise aussi bien à l'extérieur qu'à l'intérieur. Il faut maîtriser l'information de bout en bout de la chaîne, afin de créer un encerclement cognitif de la cible.

La première décennie des années 2000 voit un développement de l'internet et des groupes de hackers sans qu'aucun contrôle de l'Etat ne puisse en stopper l'expansion. À cette époque, le pouvoir russe voit internet comme un terrain d'influence occidentale. Les révolutions de couleurs, les différents printemps arabes et la révolution ukrainienne lui font peur d'une extension de ce phénomène sur son territoire. Mais c'est sous la présidence de Vladimir Poutine en 2016 que le gouvernement russe prend des engagements d'actions et d'investissements dans le champ informationnel :

"La Russie cherche à assurer sa perception impartiale dans le monde, développe ses propres moyens d'information efficaces pour influencer l'opinion publique à l'étranger, contribue au renforcement des positions des médias russes dans l'espace médiatique mondial en leur accordant le soutien nécessaire de la part de l'État, participe activement à la coopération internationale dans le domaine médiatique, prend les mesures nécessaires pour repousser les menaces à sa sécurité informatique. A cet effet un large recours aux nouvelles technologies de l'information et de communication est prévu. La Russie cherchera à élaborer un ensemble de normes juridiques et éthiques pour l'utilisation fiable de ces technologies. La Russie défend le droit de chaque individu à l'accès aux informations objectives sur les événements dans le monde, ainsi qu'aux différents points de vue sur ces événements." [203]

La traduction organisationnelle de ce système de cyber-influence [201] est un premier pôle médiatique *(Russia Today, Sputnik)* directement aligné avec la volonté du Kremlin. Ils sont les relais et caisses de résonances de campagnes d'influence, ou de déstabilisation [204].

En parallèle, le ministère de la défense et ses troupes d'opérations d'information sont responsables de missions de contre propagande en ligne, ainsi que d'opérations de LIO via la direction générale du renseignement (GRU) et ses unités spécialisées en attaques techniques (26165 et 74455). Le dernier pôle est incarné par les services du ministère de l'intérieur. Son service fédéral de sécurité (FSB) dispose de capacités en LIO et LII au travers de Centre 18.

Le deuxième cercle des acteurs de la cyber-influence russe est composé d'acteurs civils reconnus comme des 'hackers patriotiques selon Vladimir Poutine [205]. Les plus connus d'entre eux sont des groupes experts dans le sabotage, l'extraction de données et l'intrusion. Ils sont nommés Fancy Bear (APT 28) et Cozy Bear

(APT 29). Le premier serait lié à l'unité 74455 du GRU, et responsable de la cyberattaque contre TV5 Monde en 2015 [32] et le piratage des équipes de campagne du candidat Macron en 2017 [206]. Le deuxième serait quant à lui lié au Centre 18 du FSB.

La manipulation de l'information au profit du pouvoir russe est également une de leurs spécialités. Leur principal outil dans cette tâche sont les nombreuses usines à trolls. En surcommunicant sur les réseaux sociaux, ils tentent de tromper la perception de l'opinion publique sur l'intérêt que suscite un sujet d'actualité. La plus célèbre de ces usines est l'Internet Research Agency, fondée par le milliardaire russe Evgueni Prigojine, propriétaire par ailleurs de l'armée de mercenaires Wagner.

Si cette maîtrise technique et cette omniprésence dans l'infosphère cyber démontre un certain niveau de puissance de la Russie, l'étude approfondie des autres métriques de développement dépeignent un tableau bien moins reluisant. Par cet exemple, on peut constater le retour sur investissement géopolitique de l'outil cyber.

La cyber-influence chinoise, jeu de go à échelle mondiale

La réélection de Xi Jinping lors du XXème congrès du Parti Communiste Chinois le 22 octobre 2022 n'est pas un événement surprenant en soi, mais plutôt un témoignage d'une volonté de maintenir un cap méthodologique et une concentration des pouvoirs. L'objectif est clair : devenir la première puissance mondiale pour le centenaire de la création de la RPC.

Pour se faire, il y a deux idées majeures dans la construction de la stratégie globale : la notion modernisée de front uni, qui vise à "mobiliser les amis du Parti pour frapper ses ennemis" en "façonnant les forces externes au Parti pour en assurer sa pérennité" [207]. Conçue en 2003, on trouve également la doctrine des "Trois guerres" *(psychologique, de l'opinion publique, du droit)* qui "visent respectivement à influencer les décisions de l'adversaire, à modeler son opinion publique et à forger un environnement normatif favorable à la Chine, ne doivent pas être comprises comme une version chinoise de la guerre hybride, mais comme une continuité de l'action du Parti" [208]. Ces concepts théoriques nous permettent de comprendre l'intérêt historique et global de l'emploi de l'influence. Ce n'est pas un simple outil mais le fondement de leur stratégie de développement.

L'accélération de ce mouvement commence avec l'arrivée de Xi Jinping au pouvoir, qui prend la mesure du développement des technologies annexes à internet, et qui s'en sert pour mener les grands chantiers de la propagande, de l'endoctrinement idéologique et de l'ingénierie du contrôle social [209].

Au niveau organisationnel [201], le système chinois est le plus large des systèmes présentés dans notre analyse. La primauté de l'élaboration du récit revient au comité central à travers le Groupe de pilotage de la propagande. Les médias officiels *(China Daily, le quotidien du peuple, Global Times)* subissent son contrôle minutieux. La parole est ensuite prêchée à l'étranger au travers d'un réseau de diffuseurs qui reçoivent leurs instructions du Bureau de l'information du ministère des affaires étrangères et du département du travail du front uni. Ce dernier est également la clé de voûte de la diffusion en interne de la politique de lutte contre les mouvements de déstabilisation dans les régions autonomes *(Xinjiang, Tibet, Hong-Kong, Taiwan)* et contre la secte Falun Gong *(tombée en disgrâce dans les années 1990)* [210].

Dans le même esprit qu'en Russie, la perception d'internet a d'abord pris la forme d'un champ d'influence occidentale. A la fin des années 1990, la solution prend forme d'une architecture physique au nom évocateur, et d'un arsenal législatif de contrôle : "Great firewall" [211]. Afin d'opérer un contrôle

sémantique du contenu, le choix est fait d'agir à partir de la couche physique : listes noires d'adresses IP, filtrage et redirection DNS, filtrage URL par proxy, inspection de paquets TCP, man in the middle attacks.

L'Armée Populaire de Libération *(APL)* est un vecteur de ce narratif du comité central, mais aussi un bras armé adepte de la LIO avec la Force de Soutien Stratégique *(FSS)* [212,213], responsable des domaines cyber, informationnel, électronique et spatial.

Des acteurs civils font partie de cet écosystème, comme China Electronics Technology Corporation, ou certaines universités. Mais on peut surtout noter l'importance des sociétés chinoises et de leur position de capteurs d'informations.

La promotion de l'image de la Chine est un volet important de cette communication. Les réseaux sociaux *(wechat, weibo)* sont des relais internes puissants dans le but d'empêcher les actions collectives dissidentes, mais également externes *(via Facebook ou Twitter)* pour défendre les intérêts nationaux. Les usines à trolls sont les vecteurs de cette communication.

Une communication offensive par la discréditation sert les objectifs de cette stratégie globale, et est souvent doublée d'actions sur le terrain pour corroborer les besoins de dénigrement [214]. On peut noter également l'orientation de cette stratégie dans le volet des revendications territoriales avec ses régions autonomes, ou méridionales [215].

3.1.7 Organiser sa défense

Pour lutter à armes égales contre les attaques d'influences étrangères, le premier facteur à prendre en compte est le nombre de personnes dédiées à cette tâche. Là encore, la primauté de l'action revient au détenteur du pouvoir de la violence légitime. Ce monopole appartient à l'Etat. À la suite des opérations d'influences menées sur le sol français lors de l'élection présidentielle de 2017, la menace a été prise au sérieux et la riposte s'est organisée autour de la volonté de se donner des moyens de lutte dans le champ informationnel.

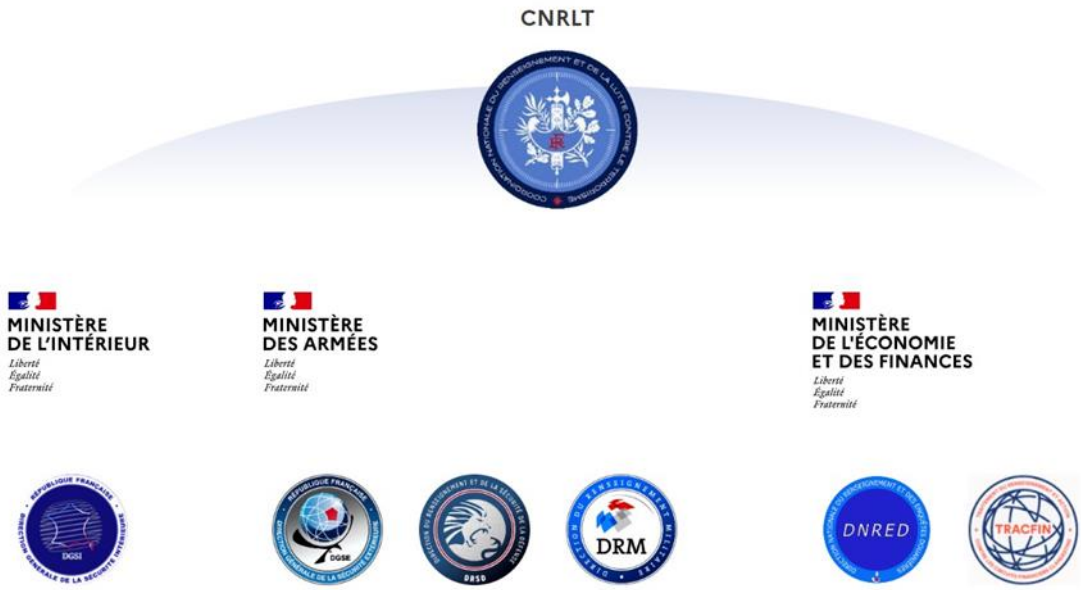


Figure 37 : Le premier cercle du renseignement

Source : DGSI

Parmi les nombreux services permettant la défense des intérêts de la France, la DGSI est la responsable naturelle par sa longue expérience dans les mécanismes de détection des opérations d'ingérence et de manipulation de l'information. Mais dans les faits, les relations sont interdépendantes au sein de la communauté du renseignement et les moyens assez limités. La création de la cellule VIGINUM [45] le 13 juillet 2021 au sein du SGDSN est une initiative dont *« La mission principale de VIGINUM est de détecter et de caractériser des ingérences numériques étrangères affectant le débat public numérique en France. Pour ce faire, le service étudie les phénomènes inauthentiques (comptes suspects, contenus malveillants, comportements anormaux, aberrants ou coordonnés) qui se manifestent sur les plateformes numériques. »* [45]. La taille modeste de ce groupe *(environ 100 personnes)* pose la question de la proportionnalité et de la suffisance des moyens face aux menaces. Le ministère des armées prend ainsi le pas de cette volonté étatique et instaure une doctrine de lutte informatique d'influence [44] en octobre 2021, placée sous la responsabilité du COMCYBER. Les moyens humains alloués semblent plus crédibles avec environ 2000 cybers combattants à terme, et pourraient faire de la France un leader européen. Au travers de ces deux initiatives, on décèle la transformation d'un modèle organisationnel traditionnellement vertical vers quelque chose de plus horizontal, plus agile.

Médias et plateformes d'information : quelles précautions prendre ?

Terreau de propagation des campagnes d'influences, les médias font partie d'un espace informationnel où l'encadrement est difficile du fait des libertés fondamentales liées *(comme la liberté de la presse, liberté d'expression)*. Les Etats-Unis font figure de précurseurs dans ce domaine avec la législation Foreign Agent Registration Act de 1930. Ayant détecté les signaux faibles d'une mouvance nazie et soviétique sur leur territoire, un moyen de contrôle et de surveillance fut d'enregistrer toute association à but non lucratif recevant des fonds venant de l'étranger. Les organisations de défense des

droits de la presse libre n'ont eu de cesse depuis de dénoncer cette initiative liberticide [216]. C'est en 2012, sous le mandat de Vladimir Poutine, que les hostilités sur la surveillance des ONG financées à l'étranger ont été relancées. Cinq ans plus tard, ce statut était étendu aux entités diffusant de l'information. En 2019 la tendance s'est accentuée et radicalisée, avec l'ajout sur la liste des agents de l'étranger des blogueurs et journalistes.

Le conflit Russo-Ukrainien nous apporte un exemple supplémentaire. En 2022, les médias Russia Today et Sputnik, notoirement connus pour être des relais d'opinions du Kremlin, ont été interdits de diffusion par la présidente de la Commission Européenne. Sur le sol français, c'est l'ARCOM *(fusion du CSA et de Hadopi)* qui est responsable de veiller au respect de la loi du 22 décembre 2018 : "relative à la lutte contre la manipulation de l'information impose aux principaux opérateurs de plateforme en ligne de prendre des mesures en vue de lutter contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité d'un des scrutins mentionnés au premier alinéa de l'article 33-1-1 de la loi du 30 septembre 1986" [217]. Cet outil législatif introduit la notion d'opérateur de plateforme [d'information] en ligne, et leur impose de coopérer en matière de lutte contre la diffusion de fausses informations. Après identification par l'ARCOM, ces derniers doivent suivre la recommandation du 15 mai 2019 [218] qui tient en 7 points :

- La mise en place d'un système de signalement accessible et visible.
- La transparence des algorithmes.
- La promotion des contenus issus d'entreprises et agences de presse et de services de communication visuelle.
- La lutte contre les comptes propageant massivement de fausses informations.
- L'information des utilisateurs, sur la nature, l'origine, les modalités de diffusion des contenus et l'identité des personnes versant des rémunérations en contrepartie de la promotion des contenus d'information.
- Favoriser l'éducation aux médias et à l'information.
- Les informations à transmettre à l'ARCOM.

La place des acteurs privés : un pôle majeur de succès ?

L'étude des trois leaders a fait apparaître un dénominateur commun : une implication des acteurs privés civils dans la conduite de la stratégie de cyber-influence. Le cadre légal semble être d'une importance capitale pour maintenir un contrôle de leur action et ainsi les intégrer dans une action homogène. Leur agilité, leur pragmatisme et les moyens alloués à la R&D dans certains grands groupes sont des avantages qui sont difficilement transposables dans l'administration étatique.

De plus, les meilleures pratiques marketing ne sont que des améliorations des techniques de propagandes militaires, adaptées aux consommateurs. Les acteurs civils ont généralement une maturité dans l'utilisation et l'exploitation des indicateurs du marketing numérique. Le ciblage d'audience et la personnalisation de contenus sont autant de compétences maîtrisées par les acteurs de l'écosystème numérique.

Les techniques de veille et d'OSINT sont également bien intégrées dans les grandes entreprises dans leurs stratégies de positionnement dans leur environnement concurrentiel.

Une place grandissante des acteurs privés pourrait être un multiplicateur d'effet d'une influence stratégique. Cependant, la culture française dans le domaine semble encore très centrée sur le monopole de l'État pour les actions sous le seuil.

La sensibilisation

Les campagnes de manipulation de l'information visent potentiellement tous les utilisateurs directs ou indirects de l'écosystème numérique. L'éducation aux médias devient un besoin pour préparer ces derniers aux menaces et risques auxquels ils font face. Le taux de pénétration des utilisateurs de réseaux sociaux touche des populations de plus en plus jeunes [219]. Dans ce contexte, la sensibilisation dès le plus jeune âge devient un enjeu pour la sécurité de leurs données personnelles.

L'éducation à la pensée critique doit intervenir dès que l'utilisateur est confronté aux problématiques de responsabilisation *(au collège en France)*. Mais la portée d'une telle matière ne prend de la dimension qu'à partir des études post-baccalauréat.

Les entreprises matures intègrent déjà ces problématiques, conscientes des enjeux qui pèsent sur leur patrimoine *(informationnel et marchant)*. On peut même trouver des coachings en gestion de crise pour les profils décideurs. Mais ce sont les plus petites structures et les positions les plus basses qui sont généralement négligées.

La simplicité est également une nécessité dans cette démarche, afin de réunir tous les publics pour une tranche d'âge donnée. En effet, les attaquants visent toujours les profils les moins sensibilisés, afin de toujours trouver un point d'entrée dans la surface d'attaque de leur système cible. Le caractère ludique d'une formation *(en utilisant la gamification)*, permet de susciter l'intérêt et ainsi multiplier les occasions de sensibilisation.

Le défi des nouvelles technologies de l'information

"L'IA désigne la possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité." - Définition du Parlement européen.

L'histoire de l'IA commence avec les avancées technologiques de la deuxième guerre mondiale en cybernétique de Norbert Wiener. Dans son article "Computing Machinery and Intelligence" de 1950, Allan Turing consacre la notion de la possibilité de penser pour une machine. Le terme Intelligence Artificielle est inventé par John McCarthy en 1956. Les progrès de l'IA s'accélèrent avec l'arrivée des premiers micro-processeurs en 1970. Deep Blue, l'IA de la société IBM qui joue contre Kasparov en 1997 remet cette technologie au-devant de la scène. Ce sont les progrès des super calculateurs et l'avènement des data centers enfermant des bases de données qui mènent l'IA au niveau que nous connaissons aujourd'hui avec la plus médiatique d'entre elles à date : Chat GPT [220].

Têtes de pont de ce mouvement, les IA génératives permettent déjà de générer du contenu comme du texte, du code, des images, de la musique et des séquences vidéo assemblées. Utilisant le Machine Learning *(ML)* via les technologies d'apprentissage supervisé et par renforcement, ces IA ont des atouts indéniables mais également des limites. L'histoire récente nous prouve que la technologie et ses effets ne sont pas encore maîtrisés, en majeure partie du fait que le monde numérique est interconnecté

physiquement mais également socialement. Ainsi la diffusion d'un deep fake sur twitter du pentagone en feu, à la suite à une explosion, peut engendrer des effets de fluctuation sur les marchés financiers. Le fait d'apprendre des requêtes qui lui sont posées font penser qu'une génération d'IA spécialisée dans un domaine devrait voir le jour [221].

Dans le cyber, des IA auront une place de plus en plus décisive dans le tempo de la gestion des opérations en accélérant les phases de traitement et de reconnaissance de l'information. On peut imaginer également l'aide de l'IA dans le ciblage toujours plus précis d'une audience par des messages générés sur les réseaux sociaux, se fera de concert de stratégies d'intoxications ou de désinformation.

Le contre-espionnage ou la détection d'opérations d'influence pourrait être un axe de développement par l'IA, grâce à sa capacité d'analyse des signaux faibles.

Mais dans cette course à l'équipement, on peut imaginer un équilibrage des forces entre l'attaque et la défense [222] , qui mènerait de facto à une dissuasion permanente.

Une limite à ne pas perdre de vue lorsqu'il s'agit de mettre en place un système performant utilisant l'IA, est la potentielle dérive liberticide sur les populations. On peut noter qu'en chine, c'est une volonté d'Etat : *« Le [but] ultime est de manipuler les valeurs, l'esprit/l'éthos national, les idéologies, les traditions culturelles, les croyances historiques, etc., d'un pays pour les inciter à abandonner leur compréhension théorique, leur système social et leur voie de développement et d'atteindre des objectifs stratégiques sans combattre »* [208].

La modification de contenu est un mode opératoire permettant la désinformation ou l'intoxication. Avec les contenus deep fake associés à la puissance du Deep Learning, on peut s'attendre à des tentatives de déstabilisation hyper ciblées et personnalisées.

Une contre-mesure potentielle pourrait venir de la technologie de la Block-chain. Décentralisée, ne nécessitant pas d'intervention tierce, elle peut permettre la transmission et le stockage de données [223]. En ajoutant un token unique d'identification, on pourrait créer une notion de version originale et ainsi ajouter de la traçabilité en cas de doute. Les défauts ciblés sur la solidité du chiffrement pourraient également être renforcés avec les technologies de chiffrement post quantique en cours de développement [224]. La problématique de la consommation énergétique de l'utilisation de cette technologie reste cependant une limite non dépassée à l'heure actuelle.

Guerre d'influence, une survie économique

La présentation de ces modèles de stratégie de lutte informationnelle, nous permet d'affirmer qu'ils sont devenus le vecteur principal d'action des Etats pour leur existence géopolitique, comme le cas de la Russie l'illustre. L'asymétrie des effets produits par leurs outils permet à des pays aux caractéristiques générales inférieures, de lutter sur un plan d'égalité ou, tout du moins, de dynamiser la création d'un écosystème privé-public fort. L'Etat d'Israël est l'exemple mature de cette stratégie.

Mais la lutte informationnelle sert également de terrain d'affrontement pour les idéologies concurrentes des leaders économiques que sont les Etats-Unis et la RPC. C'est en basant sa stratégie globale sur ce thème que la RPC veut positionner son modèle économique comme une alternative au modèle occidental, en diffusant un récit public basé sur la bienveillance, mais en utilisant des moyens dissimulés d'intoxication de l'opinion publique occidentale et de leurs décideurs.

Avatars des puissances en jeu dans cet affrontement, les entreprises sont les entités combattantes mais également les cibles de ce conflit où l'information est l'arme principale. L'avantage tactique de l'assaillant semble à date accentué par la taille d'une surface d'attaque des acteurs privés en progression constante. Mais la maîtrise des avancées technologiques qu'apportent l'IA, le quantique et le new space pourrait permettre de réduire cet avantage à une situation de dissuasion permanente.

QUELLES PERSPECTIVES EN 2030 ?

Nous, militaires, tendons à attribuer à la cyberguerre un rôle majeur dans les conflits du futur. Or, dans ce conflit-là, le cyber n'a pas tout fait, malgré la domination russe initiale. Quand la poudre parle, la lutte informatique offensive trouve ses limites. Dans la phase préparatoire de la guerre comme dans sa phase intensive, les actions de sabotage cyber ont été atténuées au profit d'une guerre classique bien plus létale, cinétique et brutale. On peut être tenté de développer une vision un peu romantique selon laquelle tout se fera à l'avenir dans le monde virtuel, mais la réalité est qu'il est nécessaire de prendre en compte tous les aspects d'un conflit.

Général de division Aymeric Bonnemaison, commandant de la cyberdéfense [225]

Anatomie du système

Afin de compléter notre analyse des thématiques clés et de leur tendance passées, l'apport d'une vision long terme par la prospective nous paraît indispensable du fait du sujet hautement stratégique qu'est la maîtrise de l'outil cyber et de ses extensions. A travers un exercice guidé utilisant la méthode des scénarios, nous cherchons à éclairer les potentialités d'un avenir fictif - que les caractéristiques structurelles de la France sont le parfait terrain d'étude - qui pourrait être défavorable si les méthodes actuelles étaient maintenues. L'idée est d'apporter une nouvelle lecture des tendances géopolitiques actuelles et des phénomènes prégnants, en les croisant avec ruptures composées de signaux faibles ou de thématiques inexplorées.

Placer le regard dans un cadre spatiotemporel et géopolitique différent, est essentiel. Nous utilisons des variables critiques influençant ce système en profondeur, afin de pouvoir mettre à jour des potentielles faiblesses. De plus, le récit doit être créatif mais aussi le plus proche de la réalité d'un point de vue opérationnel, afin de pouvoir en tirer des enseignements que l'on peut traduire en mesures correctives concrètes.

Les initiatives prospectivistes sont l'apanage traditionnel des armées. La mission Red Team Défense du ministère des armées a été créée dans ce sens, en associant les compétences d'auteurs et dessinateurs de science-fiction avec des experts scientifiques des armées [226].

France 2031 : Tensions internes aux confins de la République

Paris, Palais de l'Elysées, Samedi 7 juin 2031, 21h32. La réunion vient de se terminer et toutes les plus hautes autorités du pays se lèvent de leur chaise lorsque le président Breton sort de la salle de crise. On trouve un panel d'officiers des trois armées et de hauts fonctionnaires, dans une salle orientée autour d'un écran d'une dizaine de mètres de diamètre. On trouve une table en "U", équipée de postes avec chacun un écran, un clavier, un téléphone filaire, un bloc note, un stylo et une bouteille d'eau. Trois groupes de tables équipées de la même manière et pouvant accueillir chacune 4 personnes sont en deuxième cercle. L'ambiance est tendue et malgré les nombreuses personnes communicant au téléphone à voix haute, on peut noter que les performances de l'insonorisation sont exceptionnelles, afin de travailler en autonomie dans la durée.

L'écran principal contient plusieurs diagrammes et tableaux, et on distingue un encadré rouge sur la partie supérieure avec la mention Cyberattaque majeure.

L'actualité géopolitique de l'année 2031 est particulièrement intense. La récente alliance des seventeen eyes (Etats-Unis, Royaume-Uni, Canada, Australie, France, Danemark, Pays-Bas, Norvège, Allemagne, Italie, Espagne, Suède, Israël, Corée du Sud, Japon, Finlande et Estonie), a été conçue à l'initiative des Etats-Unis afin de maintenir un réseau de puissances alliées positionnées en étau autour de l'axe Moscou-Pékin, et ainsi apporter un effet multiplicateur pour les opérations multi domainesmulti champs. La politique de la terre brûlée opérée par la Russie en Ukraine a laissé un champ de ruines, sur la partie Est du territoire. 20 millions de personnes ont fui la zone pour se rapprocher de la capitale Kiev, ou plutôt ce qu'il en reste. Les six ans de guerre ont permis à l'économie russe de se relancer à travers le développement d'un complexe militaro-industriel, l'exploitation minière et la vente d'hydrocarbures. La fin du conflit déclenchée par la mort de Vladimir Poutine, s'est soldée par la signature d'un traité et par la création d'un no-man's land qui s'étend de la frontière Bélarusse en passant par Kharkiv et Marioupol et jusqu'à la mer Noire. Arrivé en fonction en 2025 et appliquant une ligne politique moins dure que son prédécesseur mais devant faire face à l'émergence de tensions claniques, Sergueï Sobianine est l'ancien maire de Moscou et incarne l'image d'un leader vent debout dans la tempête qu'il a forgé par sa gestion exemplaire de la crise de la COVID-19. Il est acteur d'une realpolitik qu'il oriente dans un duopole de l'alliance BRIC (dont le cinquième membre est maintenant la Turquie) par le maintien des grands chantiers stratégiques et technologiques.

La croissance chinoise reste sur une courbe ascendante depuis le quatrième mandat de Xi Jinping, malgré la volonté de Washington de relocaliser la production de certains éléments critiques de la chaîne de valeur de l'industrie technologique américaine, et l'enlisement du projet "One belt, one road" des suites de la crise de la dette qui a touché le pays au tournant 2024. L'intense lobby américain à l'OMC pour une réévaluation du statut de pays en développement de la Chine a abouti en 2026, mais n'a pas ralenti la croissance chinoise comme les pays occidentaux l'espéraient. Le climat de guerre froide entre la Chine et les Etats-Unis est arrivé à son paroxysme durant l'hiver 2028 lors de la tentative infructueuse d'influencer le scrutin de la présidentielle de Taiwan par des campagnes massives de désinformation sur les canaux numériques et par des manifestations de groupements pro chinois. Vainqueur in extremis, le parti démocrate progressiste demanda l'aide de la puissance de frappe des officines américaines pour lutter à armes égales dans le champ de la cyber-influence.

La crise de la dette américaine de 2024 faisant écho à la crise chinoise, a plongé la finance mondiale dans une période d'instabilité et de défiance qui a duré plus de deux ans. La réponse du scrutin fut le retour de Donald Trump au pouvoir et de sa politique conservatrice. Appuyé par la majorité au sénat, le mandat de Trump a été marqué par un renforcement de la relocalisation des éléments technologiques critiques de la chaîne de valeur de l'industrie numérique. C'est durant son mandat que le renforcement des lois anti-trust a été effectué, contre toute attente. Le contrôle renforcé des GAFAM motivé par une volonté de dynamiser l'économie numérique a permis de lancer plusieurs nouveaux géants de la data et de l'IA.

Successeur désigné, le conservateur Ron DeSantis brigue la présidence en 2028, aidé par le retour de la croissance mondiale et la volonté des faucons d'aider le gouvernement de Taipei dans la lutte contre les déstabilisations chinoises. Résolument décidés à reprendre le contrôle de l'ordre économique mondial, Washington ordonne à la septième flotte de stationner sur l'île de Diego Garcia et à la troisième flotte de se positionner sur l'île de Guam.

Cette démonstration de force s'est accompagnée de mouvements de sous-marins américains dans le détroit de Malaka en 2029 et de tests de missiles hyper véloces dans le Pacifique en 2030. Le matraquage médiatique qui a suivi l'arrivée américaine dans la zone indo-pacifique a ajouté un peu plus de pression sur les pays périphériques de la Chine et leurs gouvernements. La réplique chinoise

s’est faite sous la forme de tests grandeur nature d’armes de nouvelle génération, à grand renfort d’images diffusées sur les réseaux sociaux. En pointe dans le développement des drones, l’Armée Populaire de Libération a démontré ses capacités de défense lors d’un essai d’interception de missile par un essaim de drones coordonné en 2029 et par le test d’une arme à impulsion électromagnétique à effet dirigé sur un essaim de drones en 2030.

Cette nouvelle guerre froide prend essentiellement la forme d’opérations de déstabilisation et d’intoxication dans les pays alignés des deux blocs. De nature informationnelle, ces opérations ont gagné en ampleur et en rapidité d’exécution, et ciblent des portions de populations de plus en plus hétérogènes, mais dont les dénominateurs communs sociaux démontrent une maîtrise du ciblage et de la personnalisation du message. Les phases d’élections sont ainsi devenues le terrain favori de ces campagnes, au point que l’actualité est rythmée par la divulgation des opérations d’influence les plus spectaculaires.

La France se positionne dans le sillage américain pour des raisons historiques, en tête du deuxième cercle régional d’Europe. Le rôle d’acteur de médiation et relais d’opinion du président Macron a donné une existence politique internationale temporaire à la France. Le dialogue s'essoufflant avec la balkanisation du conflit, la situation de dépendance énergétique américaine, la rupture du co-leadership européen franco-allemand et les tensions internes manipulées par Moscou, ont été les facteurs d’alternance qui ont mené à l’élection de l’ancien ministre de l’Économie et commissaire européen Thierry Breton en 2027, sous une alliance de droite conservatrice. Engagé dans le maintien des objectifs du plan de relance France 2030, il marque son quinquennat par un style détaché du peuple mais engagé dans la conduite des grands piliers de cette stratégie : “Mieux vivre, mieux produire, mieux comprendre”. Décrié dans les sondages, il fait l’objet de campagnes d’intoxication et de déstabilisation venants de mouvances de plusieurs horizons politiques, financées par des sociétés russes et manipulées par les fermes trolls à moteur IA Iraniennes et Nord Coréennes. L’annonce de la dernière candidature de Marine Le Pen au mois de mai pour les élections de 2032, a été le déclencheur d’une campagne d’une ampleur encore jamais égalée. Plusieurs mouvements de grève paralysent la fonction publique depuis lors.

Une carte du monde se trouve sur l’écran central. Le filtre Heatmap a été sélectionné. On distingue plusieurs points chauds sur le territoire de la France métropolitaine et des territoires d’outremer, car il est contrasté par rapport au reste de la carte. Plusieurs formes géométriques accompagnées d’un encart nominatif semblent être positionnées dans la Mer des Philippines. Au centre de cette formation on peut lire distinctement R91, l’indicatif visuel du porte avion Charles de Gaulle. L’escorte du fer de lance de la Marine Nationale est composée de huit bâtiments (cinq frégates, un ravitailleur, et deux sous-marins). La formation est intégrée dans un dispositif des seventeen eyes d’une taille sans précédent. Censé permettre de coordonner les procédures et matériels des pays de cette alliance, cet événement est surtout un énième moyen de pression et de communication à l’initiative des Etats-Unis et à destination de Pékin. La Marine Nationale a envoyé pour l’occasion plusieurs SCAF (système de combat aérien du futur) en configuration marine, censés valider une batterie de tests en condition opérationnelle, en vue de qualifier le nouvel aéronef franco-allemand en capacités nucléaires et missiles hypervéloces. Tous les moyens de chasse aéroportée sont donc déployés mais la capacité de projection de l’armée française s’est renforcée au cours de la dernière décennie avec l’arrivée de quinze avions ravitailleurs Airbus A330 MRTT, deux nouveaux avions radars AWACS, vingt engins de débarquement amphibie, dix frégates de défense et d’intervention, dix bâtiments de lutte anti sousmarine et anti-mines. Les moyens de reconnaissance et de lutte radiocommandés ont également

renforcé les bâtiments de commandement et les portes hélicoptères, permettant d'augmenter les capacités de situation awareness et d'autodéfense.

Avec les commandes de nouveaux matériels confirmées au cours de l'année 2028, dans le nouveau projet de loi militaire 2029-2036, la filière est porteuse d'emplois et les chantiers de l'Atlantique et de Cherbourg fonctionnent à plein régime. Derrière cette nouvelle LPM, l'ambition serait de faire de l'armée française un maillon fort dans la conduite d'opérations armées internationales ou sous mandat de l'OTAN, dans les futurs conflits Multi Domaines Multi Champs (MDMC).

Le général commandant les forces de cybersécurité (COMCYBER) est debout face à un auditoire concentré et à l'écoute. Il est à la tête d'une force dont les compétences transversales sont offensives, défensives et informationnelles. Il est le second du CEMA depuis une réorganisation de l'Etat Major des Armées en 2028. Il vient de présenter devant l'assistance l'étendue de la situation au président : nous faisons face à une attaque hybride sur deux fronts internes. La situation est complexe du fait de l'échelle spatio-temporelle de la menace. Dans la nuit de vendredi à samedi, plusieurs attaques simultanées ont frappé des installations critiques sur Kourou et Cayenne. Des essaims de drones de loisirs, ont touché la tour de contrôle de l'aéroport de Cayenne et le centre spatial de Kourou. Les trois stations de suivi, de météo et de poursuite du centre spatial sont touchées. La méthode cinétique dite Pearl Harbor a été employée. Le nombre et la vitesse des flottes de drones est associé à leurs différents capteurs pour faire des plongées rapides aux trajectoires coordonnées, imprévisibles et redoutablement précises. Les cibles sont les éléments extérieurs d'envoi et d'émission des flux de données comme les antennes, paraboles, éléments optiques, sondes et capteurs. La destruction des éléments accessibles directement est effectuée par vagues successives cinétiques, bénéficiant de l'énergie accumulée durant la phase d'accélération et faisant de chaque drone un projectile. Pour les dispositifs couverts, les essaims de drones ont cumulé les effets cinétiques par l'explosion commandée par court-circuit des batteries de certains drones se positionnant au contact de la cible. Le rapport fait état également d'une attaque DDOS massive sur les serveurs du Grand Port Maritime de Guyane, dont les installations vieillissantes sont à Dégrad-des-cannes et à Pariacabo. Les premières constatations des équipiers cyber de la gendarmerie de Cayenne font état de relais wifi et Bluetooth aux alentours des sites visés. Il pourrait s'agir d'un réseau ad Hoc servant à l'extension de la portée et d'aide à la navigation.

Le bilan est uniquement matériel mais le mode opératoire est unique à ce jour et le rapport des équipes de LID et de L2I du COMCYBER est éloquent : les risques d'une nouvelle frappe sont élevés. Plusieurs campagnes de déstabilisation sur les réseaux sociaux ont mené les communautés amérindiennes et brésiliennes à la manifestation. Les bâtiments étatiques et des entreprises françaises ont été les cibles de groupes de casseurs mais les éléments de gendarmerie et de CRS ont réussi à maintenir l'ordre jusque-là. L'attribution de l'attaque n'est pas encore confirmée. Un faisceau d'indices venant de l'activité numérique guyanaise indiquerait que le groupe cyber malveillant Utr3cht est derrière ces attaques. Ce groupe, dont les ramifications techniques et financières sont liées à Brasilia, est né du renforcement idéologique de la communauté amérindienne guyanaise au cours de la dernière décennie. Les revendications sociales et culturelles opposant Paris à la communauté autochtone ont pris une dimension informationnelle en 2024, avec la promulgation de lois de protection du patrimoine forestier et de partage de zones déséquilibrant les zones d'influences ethniques préexistantes. Une montée en tension se traduisant par des actions de manifestations à atteint son paroxysme en 2027 avec le décès d'un gendarme mobile et de cinq manifestants en pleine période électorale. La réponse du président Breton fut le renforcement des éléments de gendarmerie sur le territoire guyanais et une répression des poches de violences identifiées. Spécialisé dans la diffusion de cyber campagnes anti françaises dans la communauté amérindienne, le groupe s'était illustré par la coordination de flashmob

et d'actions de manipulation de l'information ciblant les forces locales en relayant massivement des deep fake sur les positions des groupes d'émeutiers, par post sur les principales plateformes *(Méta, TikTok, Snapchat)*, lors des élections présidentielles de 2027. Surveillé de près depuis ce moment par les IA de détection du COMCYBER, le groupe ne communique plus depuis plusieurs mois.

Le développement du contrôle de flottes de drones n'est pas une technologie nouvelle. Le ministère des armées expérimentait depuis 2011 sur le sujet à travers son projet SUSIE *(Supervision de systèmes d'intelligence en essaim)*. Mais la diffusion en Open Source de proof of concept se basant sur des technologies civiles à bas coût par des chercheurs chinois en 2027 a permis l'accès à cette technologie au plus grand nombre. L'autodestruction de la batterie est une technologie diffusée sur des forums extrémistes du Dark web depuis plusieurs années. La combinaison des deux techniques est qualifiée de première mondiale par le Commandant du COMCYBER. Une fiche descriptive du groupe Utr3cht apparaît à l'écran lorsque le Commandant les évoque, accompagné de photos d'archives des manifestations sanglantes de 2007. Le groupe bénéficie de l'appui de relais narco trafiquants et orpailleurs qui sont les organisateurs de l'immigration brésilienne de la région Manaus, dont l'ampleur est un sujet depuis de nombreuses années. La population guyanaise a ainsi doublé durant les dix dernières années, entraînant des problématiques culturelles, démographiques et sociales.

Le retour de Lula à la présidence en 2022, a renforcé les liens avec Pékin et Moscou, mais a surtout permis de positionner Brasilia comme relais d'influence des BRIC en Amérique du Sud. Le narco trafique de la région de Manaus a également pu se développer sans réel frein ni contrôle gouvernemental. Cette stratégie a eu pour effet de renforcer une filière transfrontalière déjà très puissante et bénéficiant désormais de l'infrastructure logistique des nouvelles routes de la soie. La crise financière de 2024 touchant le pays et accentuant les disparités sociales et ethniques présentes, elle a été un accélérateur du développement de cette économie parallèle dont les ramifications vont désormais jusqu'en Afrique de l'Ouest.

Le Commandant termine son exposé en annonçant un dialogue non établi avec les autorités brésiliennes, faisant écho aux sanctions récentes sur les produits ne venant pas de l'agriculture biologique et touchant l'exportation des produits alimentaires brésiliens comme la viande et les fruits.

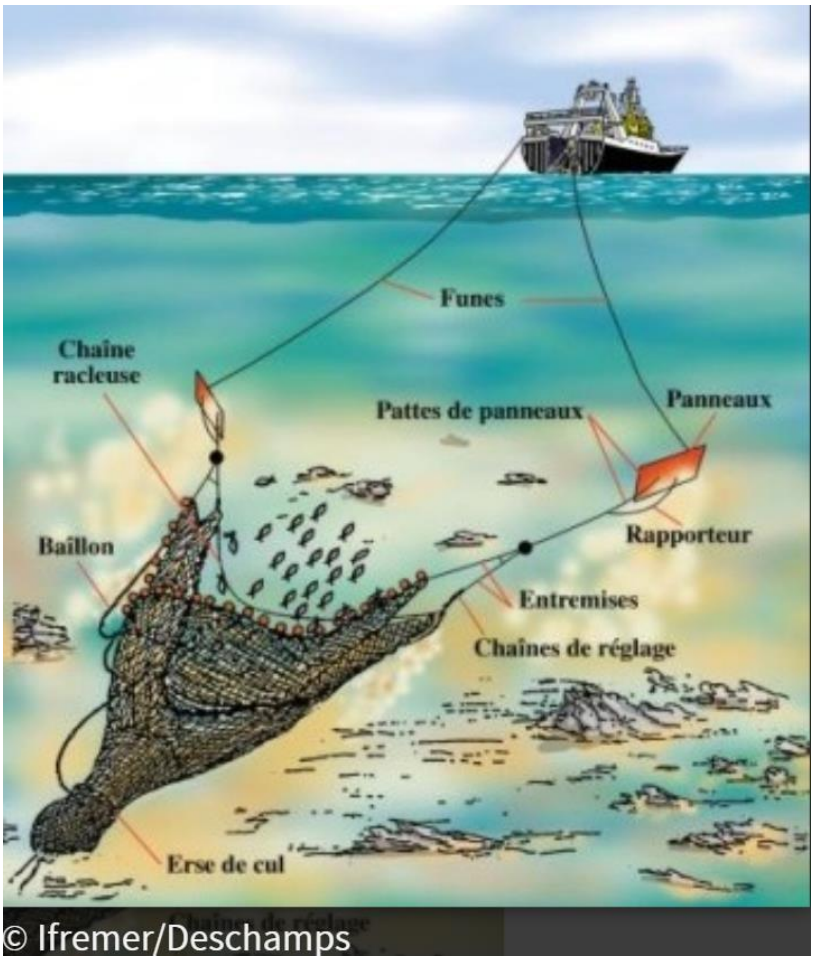
L'assistance se met à échanger le temps que le COMCYBER se coordonne avec son assistant afin de présenter son deuxième sujet. Sur l'écran apparaît les contours de plusieurs îles bien connues de la salle et du président : la Nouvelle Calédonie.

La situation est explosive depuis que le réseau internet de l'île est inopérant. La cause ? Le passage de plusieurs chalutiers-usine japonais sur le passage des deux câbles sous-marins reliant l'île au monde internet deux semaines auparavant. Sauvés par le réseau souverain satellitaire, les autorités locales peuvent continuer leurs missions de services publics, à l'exception des écoles qui ont dû ressortir les feuilles et les stylos. L'investissement massif dans le développement de communications protégées par technologie de chiffrement post quantique et distribution de clés quantiques à destination des services essentiels de l'Etat, a permis à la France d'être un des premiers pays à déployer cette solution à l'échelle. La réaction de l'administration calédonienne pour résoudre les problématiques de traitement de l'eau et d'approvisionnement énergétique a permis d'éviter la catastrophe sanitaire.

La grogne de toute une partie de la population dont l'activité est liée au réseau internet optique monte, aidée en cela par des médias locaux relais d'opinion et agissant comme une caisse de résonance d'un narratif anti-français. Un hashtag #FLNKSisback semble être massivement relayé sur les réseaux sociaux. Les équipes de LID du COMCYBER ont détecté une activité anormale venant de faux comptes

à l'origine de cette campagne informationnelle. La sophistication sur les capacités de dissimulation de la source ne fait aucun doute. Une puissance étatique est derrière cette campagne. L'interception des navires japonais par les forces françaises déployées dans la région, a permis aux équipes forensiques envoyées par Paris de travailler à l'étude approfondie des équipements des embarcations.

Après le recoupement des rapports d'interrogatoires de la Gendarmerie et des recherches des experts forensique en informatique marine embarquée civile, il semblerait que les quatre bateaux incriminés, dont la dernière modernisation correspond à une période allant de 2006 à 2017, ont été touchés par plusieurs attaques ciblant des vulnérabilités non patchées de leurs systèmes Windows XP. Si l'origine de l'infection est encore inconnue à ce jour, les experts sont formels, les instruments de navigation ont diffusé des informations manipulées. Les capitaines de chaque navire auraient suivi un itinéraire sur leur écran, mais leurs navires se seraient dirigés dans une autre direction malgré l'incohérence du compas mécanique. La pression de la marine commerciale chinoise sur la ressource halieutique mondiale a forcé les pêcheurs des pays alentours à chercher de nouveaux territoires.



La pêche par chalutage est la technique la plus dévastatrice pour la faune marine par son absence de mesures de sélection d'espèces et par son efficacité. Véritables laboureurs de la mer, ces bateaux usine traînent plusieurs filets dont la longueur dépasse trois cents mètres, et dont l'ouverture est conditionnée par deux points d'ancrages. Un premier point est le treuil du bateau, le deuxième point est un lest en forme de lame de labour et dont la fonction est de tendre l'autre partie de l'ouverture. Un équilibre entre vitesse et utilisation du sonar permet d'aligner une ouverture du filet optimale avec les masses de poissons détectées. Il semblerait que la navigation et les cibles que suivaient ces équipages aient été faussées.

Dépassant la centaine de mètres et trois mille tonnes, la puissance de traction de ces bateaux est amplement suffisante pour rompre un câble de fibre optique sous-marin au passage de leurs lests tranchants.

Le Commandant du COMCYBER fait référence à une technique vieille de quasiment vingt ans et utilisée lors de l'assaut de Deir Ezzor par l'armée israélienne en 2011, et annonce que c'est en coordination

avec les équipes de l'unité 8200 que la recherche a été effectuée. Les images sous-marines diffusées attestent bien d'une destruction totale des deux câbles.

Il présente ensuite le deuxième point à l'ordre du jour concernant la Nouvelle Calédonie. Une série d'incendies domestiques a attiré les services cyber de la gendarmerie locale par leur double dénominateur commun : l'origine de l'incendie et les personnes touchées. La démocratisation des environnements domotiques connectés était une source de vulnérabilité bien connue, mais les efforts de lobby de la filière ont ralenti les volontés de normalisation pour l'intégration d'une couche sécuritaire dans la conception de leurs équipements. Le doute est levé par les services de gendarmerie après l'investigation de trois affaires et le décès d'une employée de maison. Deux fours et un frigo de dernière génération sont les sources d'incendies ayant mené à l'intervention des services de sécurité incendie. Les équipements incriminés seraient sujets de la même vulnérabilité, qu'un groupe d'Hacktivistes aurait dévoilé un an auparavant, et permettant de contrôler les systèmes de production de chaleur et de froid. Dans le cas du décès, le frigo aurait explosé et mené à l'incendie de la maison en bois où travaillait l'employée. Elle aurait succombé à une intoxication aux fumées de combustion. Issue du peuple Kanak, son décès a déclenché les tensions identitaires qui étaient dormantes.

Les personnes touchées par les incendies ont toutes comme point commun d'appartenir au gouvernement de Nouvelle Calédonie. En une semaine c'est donc plus de dix incendies de maisons de personnels de l'action gouvernementale qui sont victimes de l'incendie de leur maison.

Le Commandant étoffe son propos en citant le rapport d'analyse de son département threat intelligence : les campagnes de dénigrement de la présence coloniale française et invoquant une indépendance de la Nouvelle Calédonie pour le peuple Kanak auraient une signature numérique qui pourrait correspondre à un groupe d'hackers bien connu, APT 41 Double Dragon. Mais il nuance son propos par la poursuite d'investigations dans cette tentative d'attribution. Ces campagnes auraient commencé deux ans auparavant, lorsque le gouvernement Breton aurait initié la stratégie de maintien des réserves stratégiques de matières premières. Un arsenal juridique fut conçu pour renégocier les concessions minières en cours. Les réserves en nickel et cobalt de la Nouvelle Calédonie étaient jusqu'alors exploitées par plusieurs sociétés étrangères. Avançant par rachats, la société Chinalco venait de récupérer les concessions du plus gros gisement. A l'annonce de ce nom, l'assistance comprend qu'une ligne rouge vient d'être franchie et que si l'information est confirmée, la diffusion du renseignement dans l'alliance des seventeen eyes sera indispensable pour maintenir une capacité d'analyse complète. Le Chef d'Etat Major des armées présente un plan d'action de mesures de mitigation puis donne quelques ordres. Le Président fait quelques remarques et se retire en demandant d'être maintenu informé de l'évolution de la situation.
À son départ, l'activité de la salle reprend, les appels reprennent et les claviers sont de nouveau manipulés. L'intelligence artificielle du traitement des flux prend le contrôle de l'écran principal en diffusant un message d'alerte et montre une image thermique d'origine satellitaire. On y distingue un mouvement massif de dizaines d'éléments et l'analyse de l'IA les présente comme une flotte de bateaux, d'hélicoptères et d'avions de l'armée brésilienne. Leur objectif est clair, ils se dirigent vers la Guyane...

Préparer sa résilience

Notre approche centrée sur le territoire français a été fondée sur la volonté d'apporter une pierre à la construction de l'édifice qu'est la résilience de la France face aux menaces endogènes et exogènes. Les particularités spatiales, historiques et ethniques qui font la France, sont autant de challenges à relever dans cette époque d'échanges informationnels infinis et de brassages culturels permanents. Nous avons volontairement choisi de mentionner des technologies actuelles et matures, tout en explorant le champ des possibles que nous apportent les caractéristiques françaises.

Maintenir la proximité temporelle du récit avec les macro-tendances actuelles nous a permis de nous centrer sur des variables qui nous paraissent primordiales pour la construction d'un État cyberrésilient.

Nous avons ainsi voulu mettre en avant l'importance de la dissuasion dans le champ sémantique. Cette dissuasion doit passer par un mix technologique et humain que le COMCYBER semble incarner dans sa genèse et ses objectifs. Il semble cependant qu'un décalage existe avec les moyens mis en place. La place des technologies de ruptures que sont l'IA, le quantique, la blockchain, doivent permettre de combler ce vide. L'écart entre la fiction (avec la création de l'IADMA et de l'IAGDM pour le bien du récit) et la réalité (avec l'initiative ARTEMIS.IA de la DGA) est mince. Les applications potentielles sont nombreuses et seront indispensables pour maintenir un niveau d'efficacité globale d'une force de projection intégrée dans le cadre d'une opération alliée, mais permettront surtout de réduire cet écart entre assaillants [du cyberespace] et défenseurs.

Les vulnérabilités de l'IoT mentionnées dans ce récit, ont étendu la surface d'attaque mondiale de manière exponentielle. Un renfort réglementaire dans le champ de l'IoT est indispensable, sous peine de voir des cas de morts potentiels. Les projets réglementaires dans ce champ sont encore timides et ne prennent pas en compte la dimension sécurisation des vulnérabilités.

L'open source est un espace qui permet des opportunités mercantiles, mais permet également de diffuser des technologies dont la maturité et le cycle de vie sont en déclin. Maintenir une veille technologique est un enjeu important, afin de déterminer les possibles applications malveillantes.

Les drones sont des atouts pour la société dans son ensemble. Le renforcement nécessaire de la sécurité de l'IoT mentionné précédemment, prend d'autant plus son sens lorsque lesdits objets sont en mouvement et peuvent devenir des armes par destinations. La lutte anti-drones est un sujet déjà connu du ministère des Armées, et pris au sérieux. Les capacités des systèmes en développement sont croissantes, mais comme pour tout système de protection, c'est le nombre d'assaillant qui prime dans les rapports de forces. L'utilisation actuelle des drones s'est jusqu'à présent faite dans un cadre tactique (au profit d'armées ou de groupes terroristes), mais comment se préparer à une attaque sur des populations civiles ?

Ce scénario a permis de mettre en évidence des problématiques d'ordre technico-juridique non résolues à l'heure actuelle. Le plus gros challenge pour la France reste le déploiement des moyens de défense sur un territoire partagé sur plusieurs continents, et à la deuxième zone économique exclusive du monde.

CONCLUSION

En traversant l'histoire, la terre, la mer, le ciel et l'espace sont les quatre dimensions que l'homme a appris à maitriser. Un espace est venu s'y ajouter qui est celui informationnel. C'est un lieu de travail, de création de richesse, de divertissements, d'échanges mais aussi sujet à une économie illicite, de la délinquance et de la criminalité organisée. Comme pour toutes les autres zones on s'y affronte également. Cet espace est à la fois un lieu d'affrontement et d'affirmation de la puissance des Etats. Les enjeux de relations internationales qui se jouent dans le monde numérique sont identiques à ceux qui régissent les autres dimensions. Si tous les Etats ont aujourd'hui intégré la dimension cyber dans leur stratégie aussi bien militaire qu'économique, certains ont pris un train d'avance et ont saisi les opportunités d'influence et de pouvoir que le cyberespace leur offrait.

Un cyberespace avec un internet de bien commun et neutre est prôné par les pays démocratiques et ceux dit autoritaires mais dans les faits chacun veut réguler et protéger cet espace et fixe ainsi des règles nationales pour y arriver.

A la différence de la stratégie militaire traditionnelle, la cybersécurité n'est pas uniquement l'affaire de l'Etat ou d'une stratégique gouvernementale, elle est également liée à la responsabilité autant individuelle que collective de la société civile. La cybersécurité et la prévention des cyberattaques passent par le renfort de la résilience des infrastructures, du développement des compétences humaines, réglementaire et technologique adaptés mais surtout à la prise de conscience des risques et préventions de tous les acteurs de la société.

Les risques numériques touchent l'ensemble des couches du cyberespace que ce soient les infrastructures physiques, la couche logique ou les plateformes d'intermédiation. Ces dernières sont sujettes à de nombreuses attaques de cyber influence pour la lutte informationnelle toujours plus sophistiquées. A ce jeu, les Etats-Unis, la Chine et la Russie sont très actives. Les technologies clés que sont l'intelligence artificielle, l'hyperpersonnalisation, les blockchains et la proliférations des fermes à troll seront décisives dans les guerres informationnelles du futur.

Les Etats doivent ainsi prendre en compte toutes ces menaces dans leur capacité de force de frappes offensives et défensives sur le domaine cybernétique. Le développement d'armes cyber puissantes permet de contribuer à la cyber dissuasion. Certains pays n'hésitant pas à attaquer pour montrer leur force mais toujours en dessous du seuil. A la différence des armes nucléaires, ce sont des armes d'emploi.

Comme l'écrivait jadis un fin connaisseur des relations internationales, "veiller à sa propre sauvegarde, ce sera toujours, quoi que l'on pense, que l'on regrette ou que l'on préfère, compter, en dernière raison, sur ses propres armes"

Charles Benoist, Les Lois de la politique française, Paris, Fayard, 1928.

SOURCES

1. Kemp, S. (2023). Digital Report : évolution du numérique en 2023
2. Kempf, O. (2019). Du cyber et de la guerre.
3. Jouvenot, B. (2018). Les incontournables lois pour expliquer et comprendre le digital..
4. Ventre, D. (2017). Guerre, armées et communication - Cyberguerre et communication - CNRS Éditions. https://books.openedition.org/editionscnrs/21114?lang=fr.
5. Mazzucchi, N. (2019). La cyberconflictualité et ses évolutions, effets physiques, effets symboliques. Rev. Déf. Natl. *821*, 138–143. 10.3917/rdna.821.0138.
6. National Cyber Power Index 2022 Belfer Cent. Sci. Int. Aff. https://www.belfercenter.org/publication/national-cyber-power-index-2022.
7. Ceruzzi, P.E. (2012). Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté. Temps Médias *18*, 15–28. 10.3917/tdm.018.0015.
8. Pouzin, L. (2002). Le projet Cyclades (1972-1977). Entrep. Hist. *29*, 33–40. 10.3917/eh.029.0033.
9. La naissance du web | CERN https://www.home.cern/fr/science/computing/birth-web.
10. Définition - Internet | Insee https://www.insee.fr/fr/metadonnees/definition/c1864.
11. Internet au pays des Soviets : épisode 3/8 du podcast Une histoire de… l'Internet, Fr. Cult.
12. La Chine, Internet et la Grande Muraille : épisode 4/8 du podcast Une histoire de… l'Internet Fr. Cult. https://www.radiofrance.fr/franceculture/podcasts/une-histoirede/la-chine-internet-et-la-grande-muraille-4141178.
13. de La Chapelle, B. (2012). Gouvernance Internet : tensions actuelles et futurs possibles. Polit. Étrangère *Eté*, 249–261. 10.3917/pe.122.0249.
14. Nocetti, J. (2018). Internet et sa gouvernance : crispations internationales et nouveaux enjeux. In La Cyberdéfense Collection U. (Armand Colin), pp. 130–135. 10.3917/arco.danet.2018.01.0130.
15. Nocetti, J. (2016). La gouvernance d'Internet, entre émancipation contrariée et nouveaux défis | la revue des médias..
16. Louis-Sidney, B. (2012). La dimension juridique du cyberespace. Rev. Int. Strat. *87*, 73– 82. 10.3917/ris.087.0073.
17. Boyer, B. (2012). Cyberstratégie: l'art de la guerre numérique (Nuvis).
18. Delerue, F., and Géry, A. (2018). Chapitre 3. Les aspects juridique et stratégique de la cyberdéfense. Le droit international et la cyberdéfense. In La Cyberdéfense Collection U. (Armand Colin), pp. 61–70. 10.3917/arco.danet.2018.01.0061.
19. Géry, A. (2018). Droit international et prolifération des cyberarmes. Polit. Étrangère *Été*, 43–54. 10.3917/pe.182.0043.
20. de Wassenaar, L. (2018). La révision de l'arrangement de dans le domaine des logiciels d'intrusion et ses conséquences.
21. Arrangement de Wassenaar (2022). Représentation Perm. Fr. Auprès Organ. Int. N. U. À Vienne. https://onu-vienne.delegfrance.org/Arrangement-de-Wassenaar-971.
22. Evans, R. (2021). Chine : Quelle stratégie dans et pour le cyberespace ?
23. National Cybersecurity Strategy 2023 (2023).
24. Obama ordonne aux États-Unis d'établir une liste de cibles à l'étranger pour les cyberattaques
25. How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last | Ars Technica.
26. Poutine, V. (2021). Décret du Président de la Fédération de Russie n° 400 du 2 juillet 2021
27. Grynszpan, E. (2023). L'empire d'Evgueni Prigojine, patron du Groupe Wagner, mis à nu par des hackeurs.
28. Internet russe, l'exception qui vient de loin, par Kevin Limonier (Le Monde diplomatique, août 2017) https://www.monde-diplomatique.fr/2017/08/LIMONIER/57798.

29. Fokker, J., and Tologonov, J. (2022). Conti Leaks: Examining the Panama Papers of Ransomware.
30. 7 points à retenir de l'enquête Vulkan Files .Washington Post.
31. La fuite des « fichiers Vulkan» révèle les tactiques de cyberguerre mondiale et nationale de Poutine, Cyberguerre | Le gardien.
32. Piratage de TV5 Monde, la piste russe se précise - Le Monde Informatique.
33. Clérot, F., and Mayor, V. (2012). « Jeu de Go dans le cyberespace ». Rev. Int. Strat. *87*, 111–119. 10.3917/ris.087.0111.
34. Niquet, V. (2021). Chapitre 5. La Chine : une modernisation des pratiques de guerre de l'information. In Les guerres de l'information à l'ère numérique Hors collection. (Presses Universitaires de France), pp. 137–158. 10.3917/puf.maran.2021.01.0137.
35. APT Groups and Operations,Google Docs.
36. Romani, R. (2008). Cyberdéfense : un nouvel enjeu de sécurité nationale - Sénat.
37. Plans gouvernementaux | Agence nationale de la sécurité des systèmes d'information.
38. Lasbordes, P. (2006). La sécurité des systèmes d'information : un enjeu majeur pour la France.
39. Delon, F. Défense et sécurité des systèmes d'information : Stratégie de la France.
40. SGDSN La sécurité des activités d'importance vitale.
41. Le commandement de la cyberdéfense (COMCYBER) | ministère des Armées.
42. Politique ministérielle de lutte informatique défensive (2019).
43. Éléments publics de doctrine militaire de lutte informatique offensive (2019).
44. Éléments publics de doctrine militaire de lutte informatique d'influence (L2I) (2021).
45. Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN (2022)..
46. VIGINUM année#1 (2022).
47. Loi de programmation militaire : le Conseil constitutionnel va être amené à se prononcer sur l'étude d'impact | Public Senat
48. Loi de programmation militaire : Cette décision de l'Assemblée est un camouflet inédit pour ce gouvernement.
49. L'essaimage d'anciens de l'ANSSI dans les startups se porte bien - 26/02/2019 - La Lettre A.
50. Des moyens et des hommes | Agence nationale de la sécurité des systèmes d'information.
51. Alsid, levée record pour une start-up française de la cybersécurité, Financement.
52. Rachat d'Alsid par Tenable, une nouvelle perte pour le secteur cyber français - Portail de l'IE https://www.portail-ie.fr/univers/enjeux-de-puissances-et-geoeconomie/2021/rachat-dalsid-par-tenable-une-nouvelle-perte-pour-le-secteurcyber-francais/.
53. Les CSIRT régionaux – CERT-FR https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux/.
54. Meet Babar, a New Malware Almost Certainly Created by France (2015).
55. Quand les Canadiens partent en chasse de « Babar » (2014). Le Monde.fr.
56. Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SOC) (2018).
57. Matania, E., Rapaport, A., and Darmon, C. (2022). Cyberpower: Israël, la révolution cyber, et le monde de demain (les Arènes).
58. Israël répond aux attaques informatiques du Hamas par une frappe aérienne.
59. L'Unité 8200, service d'élite du renseignement israélien et fournisseur officiel de hackers.
60. L'ANSSI et l'Inde renforcent leur coopération en matière de cybersécurité | Agence nationale de la sécurité des systèmes d'information.
61. Cognard, L. (2022). Comment l'Estonie est devenue un pionnier de la cybersécurité.
62. La stratégie de cybersécurité | Bâtir l'avenir numérique de l'Europe.
63. Pétiniaud, L. (2022). Les routes des données, enjeu géopolitique de la guerre en Ukraine: Hérodote *N° 186*, 113–134. 10.3917/her.186.0113.
64. Industry Report | SubTel Forum (2022).
65. Cables télégraphiques, Cité des télécoms.

66. TeleGeography | Home https://www2.telegeography.com/.
67. About | 2Africa Cable https://www.2africacable.net/about.
68. de Dinechin, G. Entretien avec Geoffroy de Dinechin, directeur opérationnel d'Orange Marine.
69. Rapport de la Federal Communications Commission (2016).
70. Picard, R. (2023). Entretien avec Romain Picard, directeur de la cybersécurité du réseau international d'Orange.
71. Morel, C. (2023). Les Câbles sous-marins : Enjeux et perspectives au XXIème siècle (CNRS éditions).
72. Submarine Cable FAQs .
73. Green, M., Drew, S., Carter, L., and Burnett, D. (2019). Submarine Cable Network Security.
74. Arthur, C. (2013). Undersea internet cables off Egypt disrupted as navy arrests three | Internet | The Guardian.
75. Vuillemin, J.-L. (2023). Entretien avec Jean-Luc Vuillemin, ancien directeur du réseau et des infrastructures à l'international d'Orange.
76. Sabotage du gazoduc Nord Stream : l'ONU appelle à éviter d'aggraver les tensions | ONU Info.
77. Edward Snowden, after months of NSA revelations, says his mission's accomplished - The Washington Post.
78. Observatoire du Monde Cybernetique Trimesriel (2013). (Délégation aux Affaires Stratégiques).
79. Greenwald, G., and Ackerman, S. (2013). How the NSA is still harvesting your online data | The NSA files | The Guardian.
80. EXCLUSIF. Comment la France écoute (aussi) le monde https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-franceecoute-aussi-le-monde.html.
81. La Nouvelle-Zélande espionne les îles françaises du Pacifique (2015).
82. NATO - Official text: "NATO 2020 : Assured Security; Dynamic Engagement" - Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO, 17May.-2010.
83. NATO, Rapport annuel du secrétaire général 2018, 14-Mar.-2019.
84. Beckvard, H., and Kono, K. (2019). Strategic importance of, and dependence on, undersea cables. https://ccdcoe.org/library/publications/strategic-importance-of-anddependence-on-undersea-cables/.
85. NATO News: NATO stands up undersea infrastructure coordination cell, 15-Feb.-2023.
86. Salamatian, K. (2020). Trump contre Huawei : enjeux géopolitiques de la 5G. Hérodote *177–178*, 197–213. 10.3917/her.177.0197.
87. Boullier, D. (2014). Internet est maritime : les enjeux des câbles sous-marins. Rev. Int. Strat. *95*, 149–158. 10.3917/ris.095.0149.
88. Convaincre et contraindre : les interférences américaines dans les échanges technologiques entre leurs alliés et la Chine | IFRI - Institut français des relations internationales .
89. La Chine veut construire un câble sous-marin à fibre optique de 500 millions $ pour rivaliser avec les USA (2023).
90. Morel, C. (2022). Le Pacifique insulaire pris dans la toile mondiale ? Géopolitique des câbles sous-marins en Océanie.
91. Digital Realty rachète Interxion pour 8,4 milliards de dollars - ChannelNews.
92. Woody, C. (2017). Russia Increased Naval Activity Worrying NATO About Undersea Cables..
93. Glanz, J., and Nilsen, T. (2020). The Deadly Losharik Submarine Fire and Russia's Secret, Undersea Agenda, The New York Times.
94. Lagneau, L. (2017). La vulnérabilité des câbles sous-marins de communication est un enjeu de sécurité majeur - Zone Militaire.
95. Métayer, L., and Saintoul, A. (2022). 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 les fonds marins.

96. Loi n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (1) - Légifrance.
97. Décret n° 2017-850 du 9 mai 2017 relatif à la composition et à la mise en œuvre de la flotte à caractère stratégique, pris pour l'application de l'article L. 2213-9 du code de la défense - Légifrance.
98. Article L2213-1 Code de la défense, Légifrance.
99. Les armées se dotent d'une stratégie ministérielle de maîtrise des fonds marins | ministère des Armées.
100. Mécanisme pour l'interconnexion en Europe — MIE numérique | Bâtir l'avenir numérique de l'Europe https://digital-strategy.ec.europa.eu/fr/activities/cef-digital.
101. Orange annonce la construction d'un nouveau câble sous-marin entre l'Europe et l'Afrique, co-financé par la Commission européenne - Newsroom Orange Groupe (2023). https://newsroom.orange.com/orange-annonce-la-construction-dun-nouveau-cablesous-marin-entre-leurope-et-lafrique-co-finance-par-la-commission-europeenne/.
102. Rapport d'information (2022). (Assemblée Nationale).
103. Gille, L. (2001). Les satellites dans les réseaux de télécommunications : l'échec des constellations mobiles. Flux *43*, 25–33. 10.3917/flux.043.0025.
104. Satellite Database | Union of Concerned Scientists.
105. Roche, N. (2016). Espace : quels enjeux stratégiques, quelles menaces, quelle dissuasion ? Rev. Déf. Natl. *791*, 99–105. 10.3917/rdna.791.0099.
106. Spacetech: The big business of space on Earth (2023).
107. Satellites - lanceurs : quelles missions et quels outils - Métiers du Spatial https://metiersdu-spatial.com/missions/.
108. Sánchez, I.A., and Fischer, D. (2012). Authenticated encryption in civilian space missions: context and requirements.
109. Quiquet, F. (2020). Description des éléments d'un système de Contrôle-Commande d'un satellite - Space & Cybersecurity Info..
110. Hertzfeld, H. (2016). Conquête spatiale de demain : quel rôle pour le secteur privé ?
111. Davenport, C. (2023). Satellite technology raises new issues for American military - The Washington Post..
112. La cyberguerre des étoiles. - RISKINTEL MEDIA (2022).
113. Gatlan, S. (2022). Viasat shares details on KA-SAT satellite service cyberattack.
114. Thales réalise une première mondiale avec la prise de contrôle inédite d'un satellite de démonstration de l'ESA | Thales Group (2023).
115. Observatoire du monde cybernétique - Lettre mensuelle - mars 2020 (2020).
116. Military and Security Developments Involving the People's Republic of China (2022).
117. Un satellite en 1500 morceaux: le syndrome de Kessler (2021)..
118. Space: EU secure connectivity satellite constellation, IRIS^2.
119. Cattaruzza, A. (2019). Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data (Le Cavalier Bleu).
120. Cattaruzza, A. (2019). Géopolitique des datacenters : puissance en stock. In Géopolitique des données numériques Géopolitique de... (Le Cavalier Bleu), pp. 75–81.
121. L'ANSSI actualise le référentiel SecNumCloud | Agence nationale de la sécurité des systèmes d'information (2016)..
122. Cloud de confiance : nouveau dispositif d'accompagnement vers l'obtention du visa de sécurité SecNumCloud a destination de nos startups et PME | Agence nationale de la sécurité des systèmes d'information.
123. ESCloud – Un label franco-allemand pour les services d'informatique en nuage de confiance | Agence nationale de la sécurité des systèmes d'information https://www.ssi.gouv.fr/actualite/escloud-un-label-franco-allemand-pour-les-servicesinformatique-en-nuage-de-confiance/.
124. Bort, J. (2020). Cisco Is Buying 400-Employee Cybersecurity Startup ThousandEyes.

125. Industroyer 2 : the Russian Cyberattack on Ukraine, Infrastructure (2022)..
126. Israël cherche à créer un “Dôme de fer” contre les cyberattaques - Yoaz Hendel - The Times of Israël https://fr.timesofisrael.com/israel-cherche-a-creer-un-dome-de-fercontre-les-cyberattaques-yoaz-hendel/.
127. ANSSI (2022). Panorama de la menace informatique 2021.
128. Qui sont les OIV - PRIM’X - PRIM’X https://www.primx.eu/fr/culture-tech/tout-savoirsur-les-oiv-ces-organisations-critiques-pour-la-nation/.
129. Cyberattaque : les sites stratégiques français sous la menace ? | TF1 INFO (2022).
130. Vidéo - Les éoliennes de France menacées par les cyberattaques ? | TF1 INFO (2022).
131. Cybersécurité : la défense française veut renforcer ses troupes de cybercombattants (2021)..
132. Fact Sheet : Act Now to Protect Against Potential Cyberattacks | The White House.
133. Camp, C. (2021). Attaque contre le Colonial Pipeline : Piratage dans le monde physique | WeLiveSecurity. https://www.welivesecurity.com/fr/2021/05/19/colonial-pipelineattaque-physique-infrastructures/.
134. Ledieu, A. (2021). La cyberattaque SolarWinds : une (vaste) affaire d’espionnage ? https://technique-et-droit-du-numerique.fr/cyberattaque-solarwinds/.
135. Multiples vulnérabilités dans les produits SolarWinds, CERT-FR.
136. A “Worst Nightmare” Cyberattack: The Untold Story Of The SolarWinds Hack (2021).
137. SolarWinds : ce que l’on sait sur la cyberattaque massive qui touche notamment Microsoft et des agences fédérales américaines (2020).
138. L., A. (2022). WannaCry : tout savoir sur la pire cyberattaque de l’Histoire. https://www.cyberuniversity.com/post/wannacry-tout-savoir-sur-la-pire-cyberattaquede-lhistoire.
139. Objets connectés : les risques à connaître |economie.gouv.fr (2022).
140. Piratage d’objets IoT – Techno Skills https://techno-skills.com/le-piratage-dobjets-iot/.
141. Cochard, S. (2019). Les objets connectés sont une menace de cybersécurité..
142. Mazzucchi, N. (2014). L’économie, cible privilégiée de la guerre informationnelle ? 22– 27.
143. Vanderbiest, N. (2018). Les institutions démocratiques : l’influence des réseaux sociaux durant une élection présidentielle. In La Cyberdéfense Collection U. (Armand Colin), pp. 181–188. 10.3917/arco.danet.2018.01.0181.
144. Wagner en Afrique de l’Ouest : les mécanismes d’une guerre informationnelle (2023). Meilleur Mondes.
145. Mali : l’armée française accuse des mercenaires russes de mettre en scène un charnier pour “décrédibiliser” la France.
146. Dèbes, F., and Madelaine, N. (2022). « L’informationnel est une arme de guerre clé du Kremlin » | Les Echos..
147. Face à la guerre en Ukraine, des réseaux sociaux en ordre de bataille (2022). https://theconversation.com/face-a-la-guerre-en-ukraine-des-reseaux-sociaux-enordre-de-bataille-178662.
148. Sibony, L. (2015). Les réseaux sociaux transforment-ils la guerre ? Rev. Déf. Natl. *784*, 49– 52. 10.3917/rdna.784.0049.
149. Mazzucchi, N. (2021). Chapitre 1. L’arme de l’information dans les conflits armés. In Les guerres de l’information à l’ère numérique Hors collection. (Presses Universitaires de France), pp. 35–54. 10.3917/puf.maran.2021.01.0035.
150. Cyber Front Z : les usines à trolls russes tournent à plein régime.
151. Barraud, B. (2018). La ferme à trolls de Saint-Pétersbourg. Rev. Eur. Médias Numér.
152. Usines à troll, doxing, loups guerriers... Les méthodes agressives de la Chine sur les réseaux sociaux - WE Demain.
153. Un niveau élevé de cybermenaces en 2022 | Agence nationale de la sécurité des systèmes d’information (2022).
154. Guide d’hygiène informatique | Agence nationale de la sécurité des systèmes d’information.
155. Rahmoune, S. (2021). Les indicateurs de maturité, quel cadre pour leur utilisation ? InCyber..

156. Horizon Europe (2023).
157. Shirer, M. (2022). Worldwide Spending on AI-Centric Systems Will Pass $300 Billion by 2026, According to IDC. IDC Prem. Glob. Mark. Intell. Co.
158. France 2030 (2023).
159. Bienert, J., Abbou, D., Cann, V., Handy, P., and Blank, A. (2023). Position Paper on the EU AI Act - Remaining Issues and Current Discussions in the European Parliament.
160. OpenQKD Partners OpenQKD..
161. Martin, K. (2019). Europe et cybersécurité : quelle(s) base(s) industrielle(s) ? Rev. Déf. Natl. *819*, 107–113. 10.3917/rdna.819.0107.
162. Kahmann, M. (2021). Allemagne. L'Industrie 4.0 : vers la digitalisation concertée de l'industrie manufacturière ? Chron. Int. IRES *173*, 33–48. 10.3917/chii.173.0033.
163. mmhaijer (2023). Mieux protéger le Royaume-Uni : explorer l'essor du marché de la cybersécurité britannique. Bus. Fr. Tech.
164. Bancal, D. (2023). Le Royaume-Uni publie une stratégie pour protéger le National Health Service des cyberattaques – Data Security Breach..
165. L'Observatoire de la Confiance Numérique ACN.
166. Cybersécurité, faire face à la menace : la stratégie française (2021).
167. Objectifs LPM 2024-2030 : maîtriser les nouveaux espaces de conflictualité | Ministère des Armées (2023).
168. How it all began ? From Tiger Leap to digital society Educ. Est. /.
169. ESTONIE. Les passions se déchaînent autour du soldat de bronze de Tallin (2007). Courr. Int. https://www.courrierinternational.com/revue-de-presse/2007/04/27/les-passionsse-dechainent-autour-du-soldat-de-bronze-de-tallinn.
170. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.
171. Thiebault, Q., and Loualitene, Y. (2023). France Identité, ou comment récupérer le contrôle des données personnelles sur le cyberespace. Portail IE.
172. Randall, P. (2021). Cybersécurité aux États-Unis : les géants de la tech annoncent une vague d'investissements.
173. National Institute of Standards and Technology (2022). Cybersecurity White Paper: EO Response 10.6028/NIST.CSWP.02042022-2.
174. Rep. Kelly, R.L. [D-I.-2 (2020). H.R.1668 - 116th Congress (2019-2020): IoT Cybersecurity Improvement Act of 2020.
175. House, T.W. (2022). Fact Sheet: Chips and Science Act Will Lower Costs, Create Jobs,
Strengthen Supply Chains, and Counter China. White House.
176. National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (National Institute of Standards and Technology) 10.6028/NIST.CSWP.04162018.
177. Souppaya, M., Scarfone, K., and Dodson, D. (2022). Secure Software Development Framework (SSDF) Version 1.1: (Draft): Recommendations for Mitigating the Risk of Software Vulnerabilities (National Institute of Standards and Technology) 10.6028/NIST.SP.800-218.
178. National Initiative for Cybersecurity Education (NICE) (2016). NIST.
179. National Cyber Investigative Joint Task Force Fed. Bur. Investig..
180. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House.
181. Israeli Cyber Security Industry Continued to Grow in 2021: Record of $8.8 Billion Raised | Israel National Cyber Directorate.
182. De Fontenay, C., and Carmel, E. (2004). Israel's Silicon Wadi: The Forces behind Cluster Formation. In Building High-Tech Clusters, T. Bresnahan and A. Gambardella, eds.
(Cambridge University Press), pp. 40–77. 10.1017/CBO9780511802911.005.

183. Start-Up Nation: Israel spends most money in the world on R&D - WEF - The Jerusalem Post.
184. Cellebrite Sold Phone Hacking Tech to Repressive Regimes, Data Suggests.
185. Dereviankine, E., and Ostashenko, M. (2015). Les obligations des acteurs du commerce électronique en Russie.
186. Zenovina, V. (2016). Президент РФ подписал антитеррористический “пакет Яровой.”.
187. Dobrokhotov, R. (2018). Putin vs the Russian Internet – 0:1 | Science and Technology | Al Jazeera..
188. ASNs by countries - IPinfo.io https://ipinfo.io/countries.
189. Melnikova, J. (2021). City по правилам без ComNews.
190. Galland, J.-P. (2010). Critique de la notion d’infrastructure critique. Flux *81*, 6–18. 10.3917/flux.081.0006.
191. Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d’importance vitale. - Légifrance.
192. Hollande, F., France, and France eds. (2013). Défense et sécurité nationale 2013: livre blanc (Documentation française).
193. Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d’information - Légifrance https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405903.
194. Les États autoritaires intensifient les cyberattaques contre les infrastructures critiques - Microsoft Switzerland News Center (2022).
195. Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog (2023)
196. Van Van Staen, C. (2017). L’Art de la guerre de Sun Tzu (Analyse approfondie) (Profillitteraire.fr).
197. Langlois, J. (2015). Kautilya’s Teachings on How to “Create” Loyal Soldiers in One’s Side but Sedition in the Enemy’s Army In Indigenous Historical Knowledge: Kautilya and His Vocabulary Pentagon Press.
198. Propagande, histoire d’un mot disgracié (2002).
199. Propaganda - The National Archives.
200. Psychological Warfare Division, Supreme Headquarters, Allied Expeditionary Force: an account of its operations in the Western European campaign, 1944-1945. - World War II Operational Documents (1951).
201. de Rochegonde, L., and Tenenbaum, É. (2021). Cyber-influence : les nouveaux enjeux de la lutte informationnelle (IFRI - Institut français des relations internationales).
202. Maurer, T. (2018). Cyber mercenaries: the state, hackers, and power (Cambridge University Press).
203. Le Concept de politique étrangère de la Fédération de Russie 2016 (2016)..
204. Audinet, M. (2019). Comment RT et Sputnik tissent la toile de Moscou à l’étranger | la revue des médias.
205. Patriotic Russians may have staged cyber attacks on own initiative - Putin | Reuters (2017).
206. Auchard, E., and Bate, F. (2017). French candidate Macron claims massive hack as emails leaked | Reuters.
207. China’s Digital Authoritarianism: Surveillance, Influence, and Political Control (2019).
208. Charon, P., and Jeangène Vilmer, J.-B. (2021). LES OPÉRATIONS D’INFLUENCE CHINOISES Un moment machiavélien IRSEM.
209. Arsène, S. (2019). China’s Social Credit System: A Chimera with Real Claws IFRI-Institut français des relations internationales.
210. Palmer, D.A. (2001). Falun Gong : la tentation du politique. Crit. Int. *11*, 36–43. 10.3917/crii.011.0036.
211. Ignoring the Great Firewall of China | SpringerLink.
212. Costello, J., and McReynolds, J. CHINA STRATEGIC PERSPECTIVES 13.
213. Burton, R. The People’s Liberation Army Strategic Support Force.
214. Hong Kong: l’armée intervient pour nettoyer les rues, une présence symbolique (2019).
215. Turla, J. (2012). Understanding the Origins of the China - Philippine Cyber War | Infosec Resources..
216. Les lois sur les « agents de l’étranger » : l’outil multifonction des régimes autoritaires (2021)..

217. Lutte contre la manipulation de l'information : déclarations des opérateurs de plateformes en ligne et questionnaires de l'Arcom | Arcom.
218. Adoption de la recommandation relative à la lutte contre la manipulation de l'information : un pas de plus vers une nouvelle régulation - Le CSA et l'Hadopi deviennent l'Arcom (2019).
219. Taux d'utilisation des réseaux sociaux selon l'âge France 2022 | Statista.
220. Introducing ChatGPT.
221. Hurst, L. (2023). Comment une fausse image de l'explosion du Pentagone sur Twitter a bousculé Wall Street | Euronews.
222. Labro, T. (2018). La cybersécurité impose un nouveau management | Virgule.
223. Blockchain use cases | Stanford Online.
224. Avis de l'ANSSI sur la migration vers la cryptographie post-quantique | Agence nationale de la sécurité des systèmes d'information (2022).
225. Commission de la défense nationale et des forces armées (2022).
226. Red Team Defense - Saison 2 https://redteamdefense.org/.
227. Morel, C. (2019). La mise en péril du réseau sous-marin international de communication. Flux *118*, 34–45. 10.3917/flux1.118.0034.

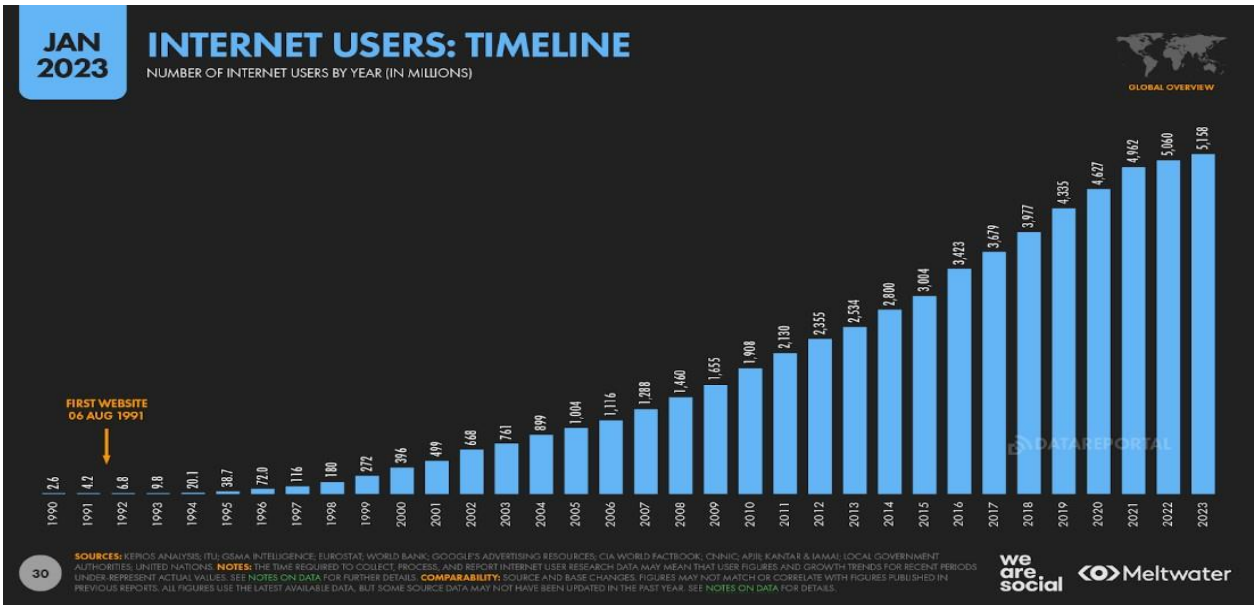
ANNEXES

ANNEXE1 : CYBER POWERS RANK 2022

NCPI 2022: Top 10 Most Comprehensive Cyber Powers Rank 2022 [6]

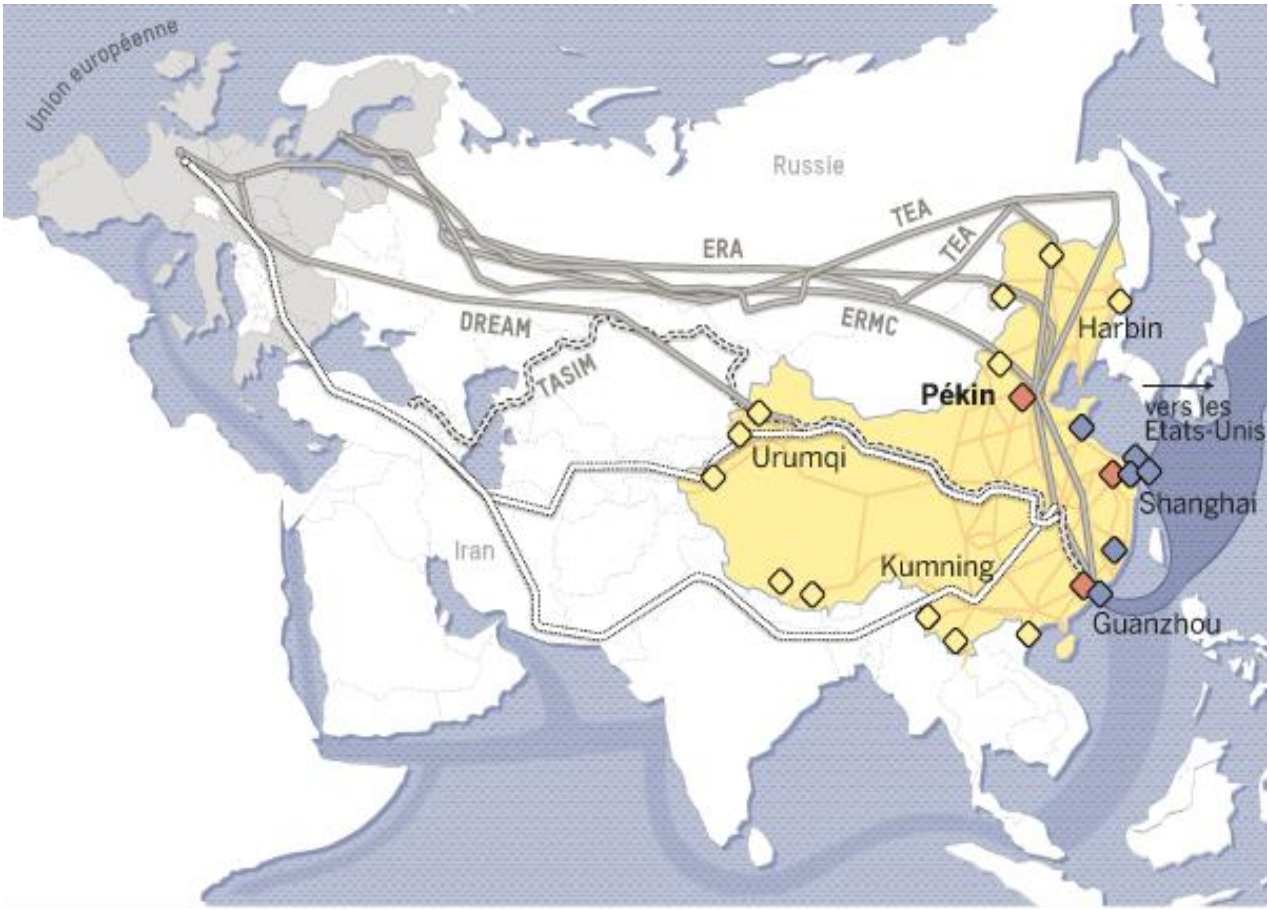
RANK	2022
1	US
2	China
3	Russia
4	Australia
5	Netherlands
6	ROK
8	Vietnam
9	France
10	Iran

ANNEXE 2 : CROISSANCE DU NOMBRE D'INTERNAUTES DE 1990 A 2023



Graphique : évolution du nombre d'internautes depuis 1990

ANNEXE3 : LES POINTS DE CONTROLE DU RESEAU CHINOIS



Cyberespace : la guerre mondiale des données (lemonde.fr)

ANNEXE 4 : ATTEINTES VOLONTAIRES AUX CABLES SOUS-MARINS

Typologie des atteintes volontaires au système sous-marin de télécommunication [227]

Acteur	*Échelle*	*Contexte*	*Action*	*Intention*
État	Infrastructure	Guerre	Coupure de câble	Destruction, isolement
État	Infrastructure	Guerre	Bombardement/ Explosion station	Destruction
État via intermédiaire	Infrastructure	Paix/Crise	Coupure de câble	Déstabilisation
État	Information	Guerre/Crise	Censure	Déstabilisation, avantage stratégique
État	Information	Guerre/Paix/ Crise	Espionnage/ Renseignement	Déstabilisation, avantage stratégique
Acteur non-étatique	Infrastructure	Paix	Coupure de câble/ Endommagement/ vol	Destruction/sabotage/déstabilisation
Acteur non-étatique	Infrastructure	Paix	Explosion stations	Destruction/sabotage
Acteur non-étatique	Information	Paix	Intrusion/hacking système de contrôle	Déstabilisation/dysfonctionnement/ destruction
État via intermédiaire	Information	Paix/crise	Intrusion/hacking système de contrôle	Déstabilisation/dysfonctionnement/ destruction

ANNEXE 5 : TRAME D'ENTRETIEN

Les différentes personnes interrogées dans le cadre des entretiens n'ont pas souhaité avoir une retranscription dans le mémoire. Cette annexe présente un exemple de trame d'entretien utilisée pour l'entretien avec Jean-Louis Le Roux: Directeur général de la société Oinis gérant les infrastructures longues distances, filiale de la société Orange.

- Quelle est la fonction d'OINIS ? Son rôle dans la mise en place et la protection des infrastructures sous-marines et les satellites ?
- Quels risques pèsent aujourd'hui sur la sécurité des réseaux sous-marins et des satellites ?
- Les technologies sous-marines avancées qui sont désormais commercialisées représententelles un risque supplémentaire pour les câbles dans le fond des mers ? possibilité par les constructeurs de distordre la fibre et de capter les données sans alerte sur le système de management ?
- Pensez-vous développer les offres satellites aux clients B2B ou grand public ?
- Existe-t-il une interdépendance entre la France et les Etats-Unis en matière de câble sous-marins, relation avec la Chine ?
- Quels sont, selon vous, les enjeux géopolitiques portés par les câbles sous-marins ?
- Quels sont selon vous les axes de télécommunications sous-marines d'importance et de dépendance de la France ?
- Quelles sont les relations qu'OINIS entretient avec le gouvernement, notamment au regard de l'importance des câbles pour la sécurité nationale ? depuis le sabotage de Nord Stream ? le début du conflit en Ukraine ? Le navire russe Yantar ?
- Que change pour l'industrie du câble sous-marin l'entrée des GAFAM sur le marché ?
- Différents projets de routes alternatives pour la fibre sous-marine devraient voir le jour. Pouvez-vous nous en parler ? non passage pas les US ? Passage par les US et plus le UK ?

ANNEXE 6 : ARCHITECTURE DE L'ORGANISATION DE CYBER INFLUENCE

Schéma n° 3 : Architecture simplifiée de la cyber-influence aux États-Unis

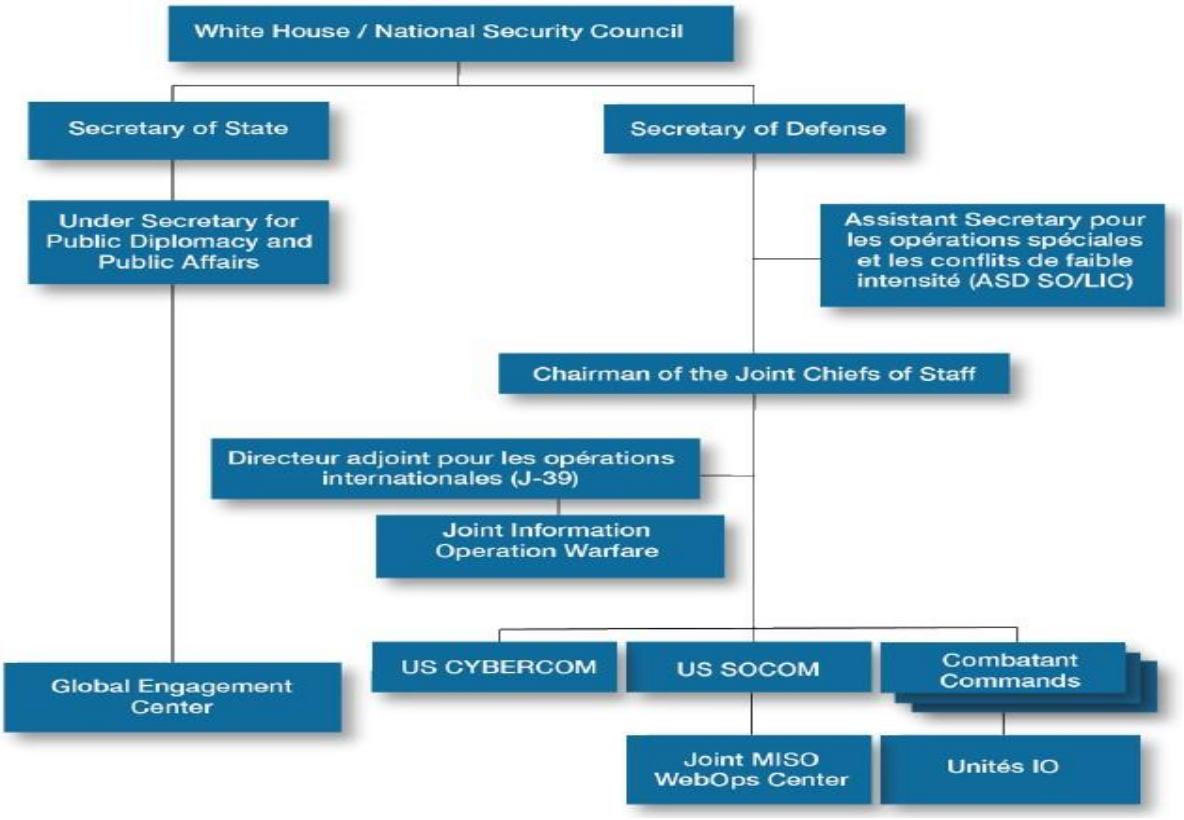


Schéma n° 4 : Architecture simplifiée de la cyber-influence en Russie

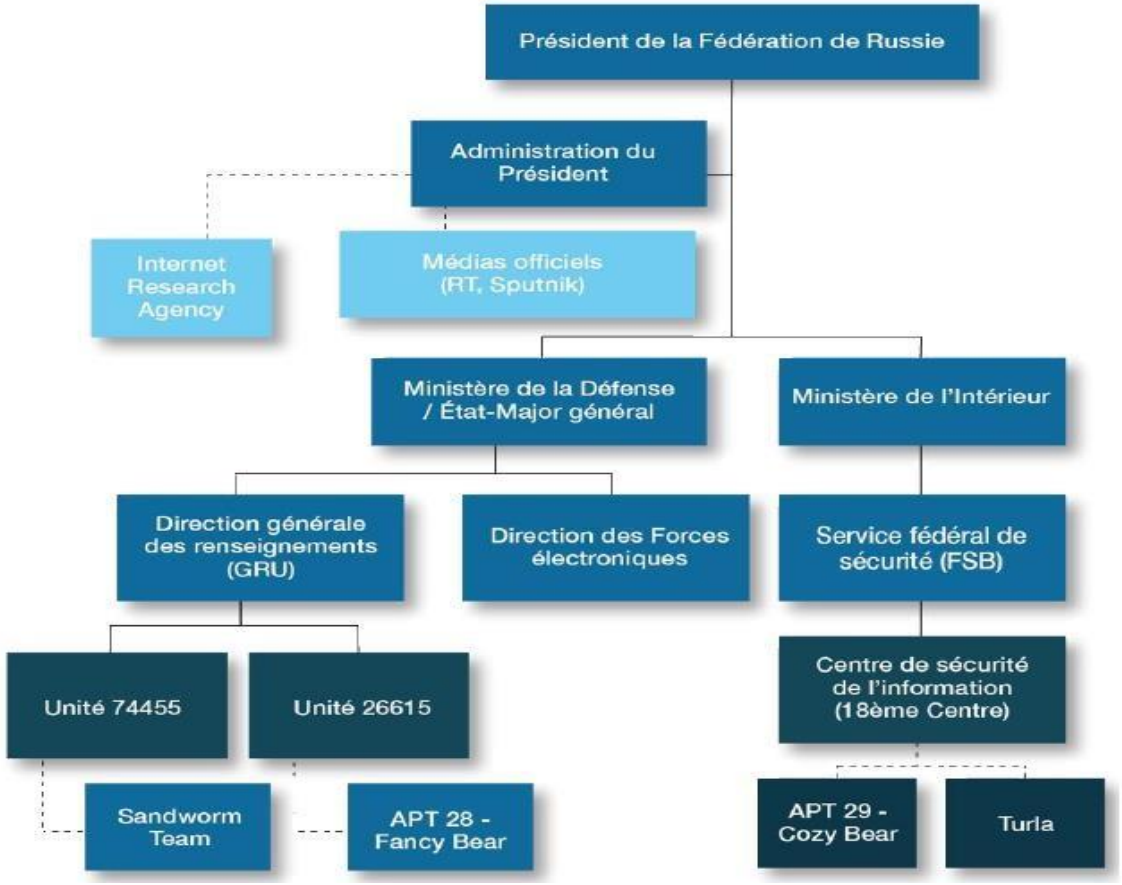


Schéma n° 5 : Architecture simplifiée de la cyber-influence en Chine