Les cyber puissances

Gate HackademINT

Table des matières

1 Introduction

Aujourd'hui l'importance de la cybersécurité n'est plus à démontrer que ce soit au niveau de la défense nationale ou de l'importance économique, technologique et stratégique de ce secteur. Cependant le cyberespace n'a pas été appréhendé de la même façon par tous les Etats ni au même moment ce qui fait qu'il existe aujourd'hui une claire différence entre les capacités des différentes nations.

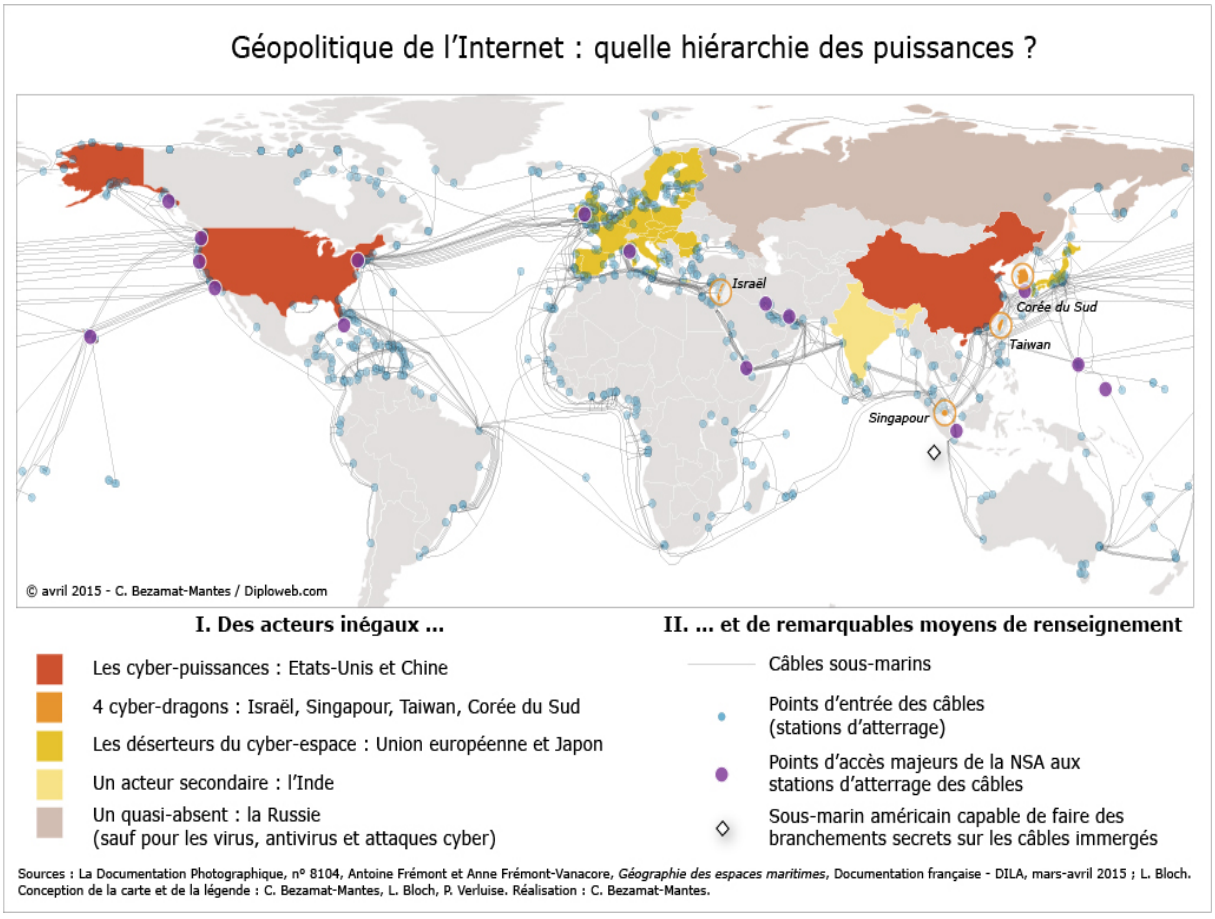
Les Etats-Unis, la Chine, la Russie et Israël ont dès la fin des années 1990 pris pleinement la mesure de l'importance de la cybersécurité et se sont placés comme des acteurs majeurs du cyberespace. Certains pays européen comme le Royaume-Uni ou bien la France ont réellement avoué son importance en 2008 mais restent aujourd'hui compétitifs bien que dépendant technologiquement parlant. Et enfin des pays comme les CyberDragons ou l'Iran sont parvenus à se faire une place soit suite à une prise de conscience datant du milieu des années 2010 pour l'Iran soit à l'aide d'investissements dans des secteurs clés.

A ceci s'ajoute des acteurs non étatiques mais nouant une relation étroite avec des Etats comme les entreprises dans le secteur des technologies de l'information et les groupes criminels mais nous n'en parlerons pas dans cette formation.

Dans cette formation on s'intéresse aux pays les plus influents dans le domaine de la cybersécurité en essayant d'expliciter les raisons de leur avantages avec un aperçu de leur doctrine, leurs capacités militaires et leur puissance économique.

Tout d'abord, lorsque l'on cherche à hierarchiser les cyber-puissances on rencontre différentes propositions qui surprennent voire se contredisent entre elles.

Le premier exemple est le graphique suivant. Il pose l'existence de 2 puissances principales - Etats Unis et Chine - et néglige l'importance de la Russie. Les pays européens sont tous considéré comme en retard, sans distinction entre le Royaume-Uni et le reste de l'Europe. Enfin la place de pays comme le Canada ou l'Australie n'est pas précisée.



Le 2e exemple provient d'un rapport de l'institut de recherche britannique IISS [1], c'est principalement sur ce document que se base cette formation. L'IISS est un institut anglais de recherche en études stratégiques qui est parmi les plus réputés au monde et dont le rapport est destiné à aider la prise de décision nationale.

Les chercheurs anglais de ce Think Tank d'études stratégiques ont classé 15 pays sur leurs cybercapacités. Seuls les États-Unis sont classés en première catégorie, très loin devant la Chine et la France, l'unique pays de l'UE sur cette liste. On remarque également l'absence de l'Allemagne et des Pays-Bas ce qui est assez surprenant. Le classement complet est

— Tiers 1 : Etats-Unis.
— Tiers 2 : Australie, Canada, China, France, Israël, Russie, Royaume-Uni.
— Tiers 3 : Inde, Indonésie, Iran, Japon, Malaisie, Corée du nord, Vietnam.

L'évaluation des capacités de chaque pays s'est faite sur 7 critères :

- ses capacités défensives ;
- ses capacités offensives ;
- ses capacités en cyber-renseignement ;
- sa stratégie et sa doctrine vis à vis de la cybersécurité ;
- sa dépendance notamment technologique ;
- sa place dans les relations internationales liées à la cybersécurité ;
- ses capacitées de gestion et de contrôle.

Si j'ai cité tous les critères c'est pour montrer que la capacité cyber d'un pays ne dépend pas seulement de ses compétences en terme d'attaque et de défense informatique. Ainsi un Etat capable de mener des attaques informatiques complexes et de grande ampleur n'est pas nécessairement une cyberpuissance, il faut aussi tout l'environnement qui va

1. IISS, Cyber Capabilities and National Power: A Net Assessment.

avec comme une stratégie sur le long terme, un contrôle sur les technologies stratégiques ou encore une économie numérique performante. C'est une distinction importante que l'on peut faire entre un Etat et un individu ou un groupe pour lesquels la technique seule représente toutes les capacités.

2 Le trio de tête

2.1 La Chine

Dès les années 1990, la Chine a reconnu l'interêt stratégique des TIC (Technologies de l'information et de la communication) et a su intégrer la dimension cyber dans tous les domaines stratégiques - aussi bien militaire, que politique ou économique [2]. En particulier elle a exploité ces capacités afin non seulement de se prémunir de l'influence occidentale en asseyant son contrôle de l'information mais également pour combler son retard technologique avec les Etats-Unis.

Ce n'est donc pas étonnant si la Chine été désignée en 2021 comme la 2e puissance cyber du monde par le rapport de l'IISS [3].

Doctrine

1. Le numérique ne doit en aucun cas permettre le retour des influences étrangères en Chine, au contraire cela doit être une arme de contrôle.
2. L'action chinoise dans le cyberespace privilégie le domaine économique d'où la volonté de se numériser malgré les risques que cela comporte.
3. Les armes cyber sont principalement utilisées, sur le plan extérieur, pour leur caractère asymétrique qui permet à la Chine de combler son retard vis à vis des Etats-Unis.
4. La vision chinoise est basée sur le long terme et non pas sur de faibles gains improvisés, elle est souvent présentée comme coordonnée et centralisée au plus haut niveau du gouvernement et du commandement militaire [4].

Sur le plan intérieur

A la fin des années 1990, l'arrivée d'Internet en Chine suscitait tout autant l'intérêt que les craintes des instances centrales du Parti Communiste chinois. Dès le début des années 2000, la Chine a fait en sorte de ne pas dépendre technologiquement d'autres nations pour maîtriser au mieux l'information stratégique [5]. Comme l'indique le rapport, la principale préoccupation dans le cyberespace a été d'empêcher la diffusion de la pensée occidentale sur l'internet chinois. Pour ce faire, le « Grand Firewall » ou « Muraille de Chine virtuelle » a été développé par le gouvernement chinois et mis en place à partir de 2003. Il s'agissait de créer un outil permettant de contrôler l'accès des internautes chinois au réseau mondial sans pour autant s'en couper complètement. Le Grand Firewall est donc constitué de pare-feux informatiques et de serveurs proxy qui permettent de filtrer les flux de données en provenance de l'étranger, en particulier les sites d'informations et les réseaux sociaux non-chinois qui sont extrêmement surveillés, voire bloqués notamment les applications américaines comme Facebook, Twitter et YouTube.

Ceci démontre tout le paradoxe chinois : parvenir à instaurer – avec son « Grand pare-feu national » - un système de filtrage d'Internet à très grande échelle tout en devenant sur le plan mondial un acteur majeur de l'économie numérique, capable de concurrencer les GAFA avec ses propres géants que sont les BATX : Baidu, Alibaba, Tencent, Xiaomi. A ceci s'ajoute un moteur de recherche local, Baidu, grâce auquel la Chine a pu construire très tôt son indépendance informationnelle face au géant américain Google. Aujourd'hui,

2. F. DOUZET, Chine : cyberstratégie, l'art de la guerre revisité.
3. IISS, Cyber Capabilities and National Power: A Net Assessment.
4. F. DOUZET, Chine : cyberstratégie, l'art de la guerre revisité.
5. F. DOUZET, Chine : cyberstratégie, l'art de la guerre revisité.

plus de 500 millions d'internautes utilisent quotidiennement Baidu à partir d'une centaine de pays. [6]

Enfin la Chine a clairement intégré les actions cyberoffensives et cyberdefensives sur le plan militaire. Par exemple, en 2015 Xi Jinping a annoncé la création d'une cinquième branche des forces armées : la force de soutien stratégique qui rassemble l'ensemble des capacités spatiales, cyber et de guerre électroniques des forces armées chinoises. Son effectif serait de plus de 175 000 hommes. Cette nouvelle force fait partie du projet de modernisation de l'armée chinoise qui inclue également l'espionnage informatique que nous allons voir dans la section suivante.

Sur le plan extérieur

En plus de garantir sa souveraineté nationale, la Chine a rapidement envisagé la cybersécurité sous l'angle du rattrapage économique. Elle vise à recueillir, par des voies légales ou illégales, de l'information de haut niveau scientifique, technologique, économique mais aussi politique et stratégique [7].

L'affaire la plus médiatisée concerne le vol de documents secret défense sur l'avion de chasse F-35 Lightning II de la société américaine Lockheed Martin. Cela aurait permis le développement de l'avion de chasse chinois Chengdu J-20.

Les attaques informatiques visent généralement un sous-traitant de l'armée américaine afin de récupérer certaines technologies clés. Les entreprises américaines sans lien direct avec le gouvernement ne sont pas épargnées comme l'indiquait en 2013 un rapport de FireEye qui décomptait 141 cibles privées américaines. Le vol des technologies bénéficieraient alors aux entreprises chinoises.

Malgré tous les points forts cités précédemment, la Chine possède également des faiblesses. Plusieurs analystes notent qu'elle se concentre sur le renseignement économique et technologique quitte à négliger sa propre cyberdéfense qui serait bien inférieur à celle de pays comme la France. Ainsi les atouts de la Chine en tant que cyber puissance seraient minés par une sécurité médiocre [8]. D'après le rapport de l'IISS les infrastructures critiques du pays auraient encore des politiques de cyber résilience peu développées.

Enfin sans doute l'élément le plus important expliquant l'écart entre les Etats-Unis et la Chine est la puissance de son économie numérique. La Chine et ses BATX restent encore loin derrière les Etats-Unis et ses GAFAM. Le problème est que les entreprises chinoises du numérique sont pour l'instant concentré sur les parts les plus accessibles de l'économie numérique ce qui empêche la Chine de construire son propre environnement indépendant. Par exemple la Chine dépend énormément d'entreprises comme Microsoft ou IBM. Cela est flagrant quand on compare les BATX et les GAFAM, une seule compagnie américaine n'a pas son équivalent chinois : Microsoft, autrement dit la seule présente dans un secteur stratégique très peu accessible. C'est pour cela que la Chine investit largement dans l'intelligence artificielle, les semi-conducteurs et les ordinateurs quantiques dans le but de se libérer de sa dépendance à l'Ouest vis à vis des technologies critiques [9], dépendance qui est à l'heure actuelle encore très importante.

En 2013, cet article [10] dédié à la cyberstratégie chinoise précisait :

La représentation selon laquelle la Chine pourrait remettre en question la puissance d'une Amérique sur le déclin, repose aussi sur le présupposé que la Chine possède les moyens de ses ambitions, ce qui en matière cyber reste à démontrer. Les révélations sur les programmes de la NSA (affaire Snowden) laissent à penser que les Etats-Unis conservent une longueur d'avance.

6. L. GAYARD, Souveraineté numérique, enjeu géopolitique, Internet sécessionniste.
7. F. DOUZET, Chine : cyberstratégie, l'art de la guerre revisité.
8. IISS, Cyber Capabilities and National Power: A Net Assessment.
9. A. Segal, Seizing Core Technologies: China Responds to U.S. Technology Competition.
10. F. DOUZET, Chine : cyberstratégie, l'art de la guerre revisité.

Or en Juin 2021 le rapport de l'IISS confirme cela : la Chine aurait un retard de 10 ans par rapport aux Etats-Unis. Ce point n'est évidemment pas du tout mis en avant par les Américains qui présentent la Chine comme la menace majeure du cyberespace depuis les années 2010. Elle reste cependant la 2e cyberpuissance dans le monde et est la plus susceptible de rattraper les Etats-Unis.

2.2 La Russie

La Russie est régulièrement désignée comme responsable d'attaques informatiques très agressives qui cherchent notamment à déstabiliser les cibles. Ses capacités cyber seraient équivalentes à celles de la Chine ou des Etats-Unis avec lesquelles elle est souvent comparée. Nous allons voir dans cette section que la Russie présente en fait de larges différences avec ces deux pays et que ces capacités en terme de cybersécurité sont à nuancées.

Doctrine

1. L'action russe dans le cyberespace se concentre principalement sur l'influence, que ce soit pour provoquer une certaine décision ou pour l'empêcher en créant de la confusion.
2. Comme pour la Chine, le numérique est perçu à la fois comme une menace est comme une opportunité : risque d'influences étrangères mais qui permet de compenser un rapport de forces perçu comme défavorable avec l'Occident.
3. La différence avec la Chine est que la Russie utilise le numérique pour ses opportunités cyberoffensives mais quasiment pas pour ses opportunités économiques.

Sur le plan intérieur

Comme dit en introduction, la Russie a très vite mesuré la menace que pouvait représentée le cyberespace notamment vis à vis de sa souveraineté nationale. Ainsi dès 2000, deux mois avant la prise de pouvoir de Vladimir Poutine, l'importance des technologies de l'information était décrite dans la doctrine de sécurité nationale [11]. L'élément le plus frappant de cette doctrine est qu'elle est focalisée sur une chose : l'influence par le biais des technologies de l'information. Cela s'explique par le fait que les élites politiques russes ont très mal vécu l'ingérence américaine dans la politique russe suite à la chute de l'URSS. Ainsi lorsque Vladimir Poutine succède à Boris Eltsine, il cherche à rétablir la puissance de la Russie à l'extérieur et sa souveraineté sur le plan intérieur. Il voit alors le numérique comme un moyen non-létale de promotion des intérêts américains dans la sphère d'influence russe mais comprend aussi les opportunités qu'il pourrait fournir afin de rétablir la puissance russe à l'international.

On comprend alors pourquoi la Russie s'est dôtée d'infrastructures dans l'optique de réduire l'influence américaine. De même que la Chine, la Russie a crée son propre internet afin de contrôler l'information. Il comprend des alternatives aux applications américaines comme l'internet chinois mais il reste moins stricte que ce dernier étant donné que les applications américaines ne sont pas interdites. On peut citer par exemple le moteur de recherche Yandex qui concurrence Google sur le secteur du référencement intérieur russe puisqu'il détient en 2022 près de 44% des parts du marché national [12], à titre de comparaison Google représente 92% des parts de marchés en France.

Sur le plan extérieur

Comme dit précédemment, l'activité russe dans le cyberespace est concentrée sur l'influence. Cette arme non conventionnelle a été théorisée sous le nom de *contrôle réflexif* qui peut être résumé par :

11. J.-L. Gergorin, L. Isaac-Dognin, Cyber : La guerre permanente.
12. StatCounter, Search Engine Host Market Share Russian Federation Jan 2021 - Jan 2022.

> L'influence des décisions de l'ennemi à travers l'utilisation des connaissances profondes de sa politique, idéologie, doctrine militaire, objectifs, l'état de ses forces, organisation, psychologie, les qualités du personnel clé, ses relations mutuelles, et l'état émotionnel [a].
>
> *a.* D. KOLESNYK, Du contrôle réflexif.

Ce concept permet de mieux comprendre les opérations de cyberinfluence menées par la Russie notamment l'ingérence dans les élections américaines de 2016. Cette opération menée par le GRU - la direction générale des renseignements de l'état-major russe - démontre bien les deux facettes du contrôle réflexif. La facette la plus évidente est l'influence exercée via une campagne massive sur les réseaux sociaux mais il ne faut pas négligé la confusion que cette cyber-ingérence a engendré dans le gouvernement américain en semant un doute sur la légitimité de l'élection. Cet intérêt porté au caractère asymétrique des armes cyber est bien représenté dans un rapport du chef d'état-major russe, le Général Valéri Guérassimov, qui écrivait en 2013 :

> Au XXIe siècle, nous avons constaté une tendance à l'effacement des lignes de séparation entre la guerre et la paix.
> L'utilisation des moyens non militaires pour atteindre des objectifs politiques et stratégiques a cru, et dans bien des cas leur efficacité a surpassé celle de l'utilisation des armes.
> L'espace informationnel offre de larges capacités asymétriques pour réduire la capacité de combat de l'ennemi. [a]
>
> *a.* J.-L. Gergorin, L. Isaac-Dognin, Cyber : La guerre permanente.

Le développement des capacités offensives russes est tel que la Russie possède désormais une capacité de nuisance qui ne peut pas être négligée.

Cependant malgré cette prise de conscience rapide des problématiques cyber, la Russie ne possède pas la capacité industrielle de la Chine ni même l'économie numérique de la France [13]. Comme indiqué dans le livre *Cyber : La guerre permanente* [14], bien que très innovante dans sur le plan offensif et défensif dans le cyberespace, la Russie s'engage cependant dans la cyberguerre avec un handicap monumental : la faiblesse de son économie entrepreneuriale dans le domaine du numérique. Autrement dit, la composante cyber a été vue principalement sous l'angle militaire tandis que l'angle économique a été négligé [15]. C'est sans doute la différence la plus importante entre la stratégie chinoise et la stratégie russe. La Chine a choisi de se numériser, même si cela la rend plus sensible aux attaques informatiques, afin d'avoir un tissu économique puissant. De son côté, la Russie a d'abord été largement méfiante vis à vis du secteur du numérique, irrémédiablement associé à l'influence américaine, avant de commencer à investir dedans en 2017 soit très tardivement.

13. IISS, Cyber Capabilities and National Power: A Net Assessment.
14. J.-L. Gergorin, L. Isaac-Dognin, Cyber : La guerre permanente.
15. T. BERTHIER, Maîtriser la donnée : enjeux et défis géopolitiques.

2.3 Les Etats-Unis

Au début des années 1990, les Etats-Unis dominent le secteur du numérique avec des empires comme IBM, Microsoft, Intel et Oracle. Les responsables politiques et militaires américains ont alors estimé que « la domination américaine de l'industrie numérique allait se traduire par une hégémonie similaire dans le cyberespace leur permettant à la fois un accès totale à toutes les informations par les interceptions et pénétrations de la NSA et la neutralisation des Etats voyous par leurs capacités cyber-offensives » [16]. D'après cette idée, la supériorité économique des Etats-Unis dans ce secteur aurait pour conséquence la maitrîse absolue des nouvelles technologies ce qui permettraient d'assurer l'hégémonie américaine grâce à des capacités inégalables en terme de renseignement, de contrôle, de commandement et de communication.

Evidemment cela ne s'est pas passé comme prévu. De nombreuses puissances sont parvenues à développer des capacités suffisantes pour constituer une menace pour les Etats-Unis tout en n'étant pas aussi vulnérables que voulu. Il apparaît alors que les Etats-Unis ne sont finalement pas - ou plus - maître du cyberespace même s'ils restent le pays le plus puissant dans ce secteur.

Doctrine

1. Le commandement cyber américain - US Cyber Command - a nommé le rapport de 2018, dans lequel il délivre sa vision stratégique, *Achieve and maintain cyberspace superiority.*
2. Ce même rapport indique que les Etats-Unis considèrent les cyber-opérations offensives comme l'un des outils principaux pour accomplir leurs objectifs nationaux.
3. C'est sans doute le pays dans lequel le renseignement cyber est le plus développé. Les révélations d'Edward Snowden ont montré que les services de renseignement américains disposaient de capacités très sophistiquées et de grande ampleur.

Capacités

Tout d'abord, qui gère la cybersécurité dans le gouvernement américain ? Contrairement au système français que nous verrons dans la suite, le gouvernement américain dispose de nombreux départements et agences impliqués dans la gestion de la question cyber. Les éléments les plus importants de ce système sont le Conseil de sécurité nationale (NSC), la NSA et le Cyber Command.

La NSA est l'agence la plus médiatisée notamment du fait des révélations de Edward Snowden qui ont délivré une vision précise des capacités offensives Etats-Unis. Les objectifs de la NSA, les informations sur son budget ainsi que des détails sur certaines opérations font partie des documents dévoilés par Snowden. Par exemple l'organisation aurait effectué 231 cyber opérations offensives rien qu'en 2011 et elle aurait coordonné l'installation d'implants sur de nombreux systèmes informatiques permettant non seulement l'accès à toute l'information mais aussi la paralysie du système . Toutes ces informations tendent à montrer que les Etats-Unis ont probablement les capacités cyberoffensives les plus importantes du monde.

Ces mêmes documents ont aussi dévoilé l'ambition des services de renseignement américains : la surveillance de l'intégralité des communications mondiales. En particulier c'est la surveillance des citoyens américains ainsi que celle des alliés des Etats-Unis comme la France ou l'Allemagne, qui ont été révélateurs des capacités d'interception de la NSA. Ces capacités proviennent notamment de la coopération entre les Etats-Unis et 4 autres pays. Cette alliance, nommée Fives Eyes, consiste en la coopération des services responsable

16. J.-L. Gergorin, L. Isaac-Dognin, Cyber : La guerre permanente.

du renseignement d'origine électromagnétique de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. La puissance de cette alliance ainsi que les autres coopérations qu'entretiennent les Etats-Unis avec certains pays comme Israël - sur laquelle nous reviendrons - prouvent que les Etats-Unis ont les meilleurs capacités de cyber renseignement du monde. C'est aussi un des avantages que les Etats-Unis ont sur la Chine et la Russie qui sont en comparaison relativemment isolées.

Finalement en terme de sécurité des systèmes d'information les Etats-Unis ont la même faiblesse que beaucoup de pays développés à savoir la protection des infrastructures critiques. En effet, comme nous l'avons vu dans le cas de la Chine, une économie numérisée a l'inconvénient d'être extrêmement vulnérable aux attaques informatiques. C'est pourquoi les Etats-Unis investissent énormément dans la protection des infrastructures critiques du pays. Cependant la dépendance du pays à l'économie numérique est telle que cela ne suffit pas à empêcher les nombreux sabotages et vol d'informations perpétrés par des nations étrangères sur les infrastructures vitales du pays. Ce dernier reconnait la difficulté à protéger ses infrastructures et sait qu'en cas de conflit direct, elles seraient immédiatement visées et sévèrement endommagées. Il n'en reste pas moins le pays le plus avancé en terme de protection des infrastructures nationales avec une stratégie reposant sur 3 points :

1. **Shape Behavior** : constuire des partenariats que ce soit entre les pays - notamment avec le Royaume-Uni - ou entre le gouvernement, l'industrie et le secteur académique sur la cyberstratégie à adopter.
2. **Deny Benefits** : améliorer la protection des infrastructures.
3. **Impose Costs** : dissuader les ennemis potentiels d'attaquer en mettant en avant les capacités de ripostes des Etats-Unis.

Finalement tous ces éléments font des Etats-Unis la seule superpuissance de premier plan d'après l'IISS.

3 Les Fives Eyes et l'Europe

Maintenant que nous avons posé les bases des 3 puissances dominantes dans le cyberespace, nous pouvons nous intéresser aux autres nations qui sont moins mentionnées alors qu'elles disposent de moyens conséquents notamment du fait de leurs alliances.

3.1 Les Fives Eyes

L'alliance des Fives Eyes désigne la coopération des services responsable du renseignement d'origine électromagnétique de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Cet accord inclut donc naturellement les activités liés à la cyberdéfense. Il permet notamment un partage accru des activités, des fruits du renseignement technique et des interceptions de chaque pays [17]. Il stipule également que les pays s'engagent à ne pas s'espionner mutuellement. C'est cela qui explique les liens particuliers qui existent entre la NSA et les agences nationales de cybersécurité des Fives Eyes.

D'après l'IISS, qui est on le rappelle un institut de recherche britannique, le Royaume-Uni est l'Etat le plus «cyber-capable» des Fives Eyes après les Etats-Unis. Si l'on cherchait à comparer grossièrement les pays restants en terme de cybersécurité, on placerait ensuite le Canada puis l'Australie et enfin la Nouvelle-Zélande. A l'exception de ce dernier, tous ces pays sont classés en tant que Tiers 2. Ils ont des économies numériques avancés, des capacités cyberoffensives importantes et ont clairement établie leur cyberstratégie ce qui fait des Fives Eyes une alliance très puissante.

En matière de cybersécurité, les pays européens sont loin d'avoir adopter une posture commune. Alors que la plupart sont totalement dépassés, trois pays européens sont parvenus à devenir des puissances importantes du cyberespace. C'est le cas du Royaume-Uni, de la France et de l'Allemagne.

Tout d'abord, France, Allemagne et Grande-Bretagne disposent chacune d'une agence nationale de cybersécurité de grande qualité, respectivement l'ANSSI, le BSI et le NCSC. Celles-ci disposent d'une capacité de protection des infrastructures majeures probablement meilleures que celles des États-Unis, mais dont les moyens en la matière sont trop fragmentés. Les trois grands pays européens ont également chacun des capacités de renseignement technique d'excellente qualité mais quantitativement bien inférieures à celles des trois cyber-superpuissances. Enfin France, Allemagne et Grande-Bretagne ont chacun un commandement chargé à la fois de sécuriser les équipements et infrastructures informatiques des forces militaires et de mener des opérations cyber offensives contre tout type d'agresseur, étatique ou non. Là aussi, les moyens nationaux déployés, bien qu'en croissance continue, sont très inférieurs à ceux des Etats-Unis, de la Chine et de la Russie.

17. J.-L. Gergorin, L. Isaac-Dognin, Cyber : La guerre permanente.

3.2 Le Royaume-Uni

Le Royaume-Uni dispose de grandes capacités en terme de cybersécurité. L'organisme principal est le Government Communications Headquarters (QCHQ) qui a la particularité d'être à la fois l'agence de renseignement du Royaume-Uni - rôle qui est assuré par la DGSE en France - et la maison mère du National Cyber Security Center (NCSC) qui est l'agence en charge de l'ensemble de la cybersécurité britannique - rôle assuré par l'ANSSI.

Doctrine

1. La stratégie britannique met l'accent sur les relations avec le secteur privé en établissant des partenariats pour le partage d'informations sur les tactiques de piratage et les stratégies de défense.
2. Le Royaume-Uni accorde une grande importance au renseignement comme le montre le fait qu'il soit membre des Fives Eyes et que le NCSC soit subordonné à un service de renseignement.
3. Le Royaume-Uni est l'un des 3 pays - avec les Etats-Unis et l'Australie - qui a reconnu publiquement qu'il utilise ses capacités cyberoffensives.

Capacités

Le Royaume-Uni n'hésite pas à investir massivement dans le secteur de la cybersécurité avec £1.9 billion alloué entre 2016 et 2021. Une part notable est investit dans le renseignement cyber, bien plus que les investissements de la France.

De plus, il à l'une des économies les plus numérisées au monde ce qui est un atout mais qui signifie qu'elle est d'autant plus vulnérable. Cela explique que le gouvernement britannique souhaite coopérer avec le secteur privé pour favoriser la résilience des entreprises.

Enfin, le Royaume-Uni a des capacités cyberoffensives très importantes, supérieures à celle de la France d'après l'IISS et également les meilleurs capacités en cryptographie du monde. Par exemple, le GCGQ serait - d'après des documents révélés par Edward Snowden - à l'origine de nombreuses techniques cyberoffensives. La coopération Etats-Unis - Royaume-Uni et plus particulièrement NSA - GCHQ est aussi révélateur des capacités du Royaume-Uni. Les 2 pays parlent de protéger les intérêts anglo-saxons et n'hésitent pas à évoquer la dissuasion collective. Cela est important car les pays anglo-saxons ont quasiment le monopole des coopérations aussi avancées sur le cyber, ce qui pose la question des capacités de l'Europe. Par exemple, Bernard Barbier, ancien directeur technique de la DGSE s'inquiète :

> Est-ce que l'Europe veut créer une capacité combinée de cyber dissuasion ? Si l'Europe ne réagit pas rapidement, nous serons encore plus totalement dépendant du couple UK-USA : les GAFAM plus NSA-GCHQ [a].
>
> *a.* M. RAFFRAY, Washington et Londres brandissent la cyberdissuasion.

3.3 La France

Bien que la France a réagit tardivement comparé aux 4 pays cités en introduction, la réaction a été très importante à partir de la publication du livre blanc en 2008 durant le mandat de Nicolas Sarkozy. Ce livre blanc a conduit à la création de l'ANSSI en 2009 et du commandement de la cyberdéfense COMCYBER en 2017. La stratégie française de cybersécurité possède alors 3 composantes :

- l'ANSSI qui supervise la sécurité numériques des services gouvernementaux, administratifs ainsi que des opérateurs d'importance vitale ;
- la DGSE qui est chargé du renseignement cyber ;
- le COMCYBER qui est chargé de la protection des réseaux informatiques de l'armée et des actions cyberoffensives.

Ce modèle séparant les missions offensives et défensives s'oppose au modèle anglo-saxon notamment celui du Royaume-Uni où le GCHQ est chargé des opérations offensives et de la cyberdéfense de l'Etat.

Doctrine

1. Accent mis sur la défense avec l'ANSSI qui a beaucoup de pouvoir.
2. Volonté de développer la coopération européenne sur la cybersécurité sans nuire à la souveraineté nationale.
3. La France s'autorise à répondre - de manière proportionnée - aux attaques informatiques.
4. La France souhaite la mise en place d'une règlementation internationale de la cybersécurité s'appliquant aux Etats et aux acteurs privés.
5. La France est spécialiste des plans de continuité d'activité cyber en cas de crises.
6. Importance donnée à la prévention de la cyberingérence étrangère.

Capacités

L'ANSSI est l'autorité nationale en terme de cybersécurité et a donc de larges capacités d'action :

- comme on l'a vu elle est en charge de la défense et de la sécurité des systèmes d'information de l'Etat ;
- elle dispose d'un pouvoir réglementaire lui permettant de fixer les règles devant être mises en œuvre par les opérateurs d'importance vitale en matière de protection de leurs systèmes d'information ;
- elle possède un pouvoir de certification et qualification des produits et services ;
- elle peut, en cas de crise majeure, imposer des mesures à ces opérateurs.

L'ANSSI a donc à la fois un rôle de prévention et un rôle de règlementation vis à vis des entreprises. Grâce à cela la France est le leader en Europe en terme de résilience cyber i.e. la capacité à supporter les attaques informatiques et a continuer son activité. Cela est dû à une obligation réglementaire pour beaucoup d'entreprises et explique le fait que les entreprises françaises sont - en Europe - celle qui dédie la plus grande part de leur budget informatique à la cybersécurité. Bien que la France n'investisse pas autant que le Royaume-Uni dans le renseignement cyber, elle profite de nombreuses alliances dont elle dispose que ce soit avec l'Allemagne, le Royaume-Uni, les Etats-Unis ou ses anciennes colonies.

Pour ce qui est de l'Allemagne, l'agence allemande, le BSI, possède énormément de points communs avec l'ANSSI. Leurs fonctions et effectifs sont similaires et d'ailleurs les 2

agences coopèrent régulièrement. Cependant, l'Allemagne a la particularité d'avoir l'une des agences nationales dédiée à la cybersécurité la plus ancienne avec la création de la BSI en 1991. C'est paradoxale quand on sait qu'elle n'a constitué une branche militaire dédiée au cyber qu'en 2017 soit après la France et le Royaume-Uni. C'est peut-être l'une des raisons qui fait qu'elle ne figure pas dans le rapport de l'IISS.

4 Israël et l'Iran

4.1 Israël

Du fait des tensions permanentes avec ses pays voisins, Israël a toujours cherché à avoir un clair avantage sur ceux-ci en termes de capacité militaire et de renseignement. En effet cet Etat part du postulat que les États arabo-musulmans ne veulent pas seulement la défaite d'Israël mais sa destruction totale et que par conséquent il doit absolument avoir l'avantage sur les cyberarmes.

Doctrine

1. Israël a d'abord perçu le cyberespace comme une menace envers la sécurité nationale.
2. L'Etat considère comme vital le maintien de son avance technologique sur ses voisins. Ces priorités sont le renseignement et la protection de ses réseaux informatiques.
3. L'investissement dans l'industrie est nécessaire pour maintenir une cyberdéfense de haute qualité.
4. Il y a une forte coopération entre le gouvernement, le secteur privé et le secteur académique.

Capacités

Israël part du postulat que les États arabo-musulmans ne veulent pas seulement sa défaite mais sa destruction totale. Dans de nombreux scénarios qu'ils ont imaginés, la guerre est précédée d'attaques informatiques paralysant les systèmes d'information du pays, c'est pourquoi le pays accorde une importance toute particulière à l'amélioration de leur protection. Cela vise d'abord à protéger les réseaux militaires puis dans un second temps, les infrastructures nationales critiques.

Comme dit en introduction, Israël a commencé à développer ses capacités de renseigement cyber dès les années 1990. L'organisation principale du renseignement cyber est l'unité 8200 qui en charge du renseignement électromagnétique au sein du renseignement militaire israélien (AMAN). Cette unité a un rôle similaire à celui de la NSA et du GCHQ et est parvenue à atteindre un niveau d'excellence dans le domaine. C'est cette unité qui a participé au développement du virus Stuxnet. La qualité de ce service est en partie liée à la coopération étroite entre la NSA et le renseignement israélien qui comprend des échanges d'informations et d'équipements.

Israël ne fait cependant pas partie des alliés les plus proches des Etats-Unis qui sont, on le rappelle, les Five Eyes. Ainsi d'après *The Guardian*[18], Israël serait considéré par les Etats-Unis comme un allié très précieux mais dont il faut se méfier. Preuve de ceci, il est classé dans ce même article comme le 3e service de renseignement le plus aggressif envers les Etats-Unis. De plus les révélations de Snowden ont montré à la fois que le GCHQ surveillait les diplomates israéliens et que le gouvernement israélien était mis sous écoute par la NSA.

Sur le plan économique, Israël est l'un des leaders mondiaux de la cybersécurité. Le rapport de l'IISS indique que lorsque l'on fait le top 500 des entreprises de cybersécurité les plus importantes, Israël se retrouve classé 2e mondial avec 42 entreprises, derrière les Etats-Unis qui en compte 354. La fertilité de l'industrie israélienne de cybersécurité est notamment due aux relations étroites qu'il y a entre le gouvernement, le secteur privé

18. G. Greenwald et al., NSA shares raw intelligence including Americans' data with Israel.

et le secteur académique. En effet, le secteur académique a pour rôle de sélectionner les meilleurs candidats qui iront remplir les rangs des agences gouvernementales comme l'unité 8200. A la fin de leur carrière militaire les agents rejoignent souvent le secteur privée notamment les start-ups de cybersécurité. Cela a pour conséquence un échange important de technologie entre le gouvernement et l'industrie ce qui permet notamment de tester les nouvelles technologies directement sur le champ de bataille avant de les introduire sur le marché.

Pour finir sur cette partie, voici quelques données comparatives :

Pays	**Effectif dans le cyber**	**Investissement dans les start-ups cyber par an**
France	3500 (DGSE)	100 millions €
Royaume-Uni	7000 (NCSC)	300 millions €
Israël	>6000 (Unité 8200)	1 milliards €
Etats-Unis	50000 (NSA)	3 milliards €

TABLE 1 – Investissement et effectif dans le secteur de la cybersécurité en 2018

4.2 Iran

L'Iran a connu un développement de ses capacités cyber offensives assez impressionante. En effet bien que quelques groupes de cyber activistes iraniens liés au gouvernement se soient déclarés entre 2000 et 2010, c'est véritablement la découverte du virus Stuxnet au printemps 2010 qui accélère cette mise en place.

Doctrine

1. L'Iran se concentre essentiellement sur les capacités offensives et de renseigement. Ses attaques visent principalement les Etats-Unis, les États arabes du Golfe et Israël.
2. Le gouvernement n'hésite pas à contrôler Internet avec notamment la possibilité de déconnecter les internautes iraniens du reste du monde.

Capacités

Pour comprendre le développement de l'Iran dans le domaine de la cybersécurité, il est nécessaire de revenir sur Stuxnet et son impact.

En 2006, l'accélération du programme iranien d'enrichissement de l'uranium inquiète grandement les puissances occidentales. Le gouvernement israélien cherche alors à convaincre le président américain de lancer une attaque contre les installations iraniennes. George W.Bush refuse mais pour éviter que son allié ne décide d'une action militaire unilatéral, le Pentagone propose une opération de cybersabotage de l'usine iranienne d'enrichissement d'uranium. C'est ainsi que la NSA et l'unité 8200 vont collaborer sur l'opération Olympic Games qui donnera entre autres le virus Stuxnet. Ce virus, probablement introduit par une clé USB sur les serveurs isolé de l'installation nucléaire iranienne, a modifié la vitesse de rotation des centrifugeuses afin de les détruire tout en effaçant toute alerte sur les panneaux de contrôle. C'est l'entreprise russe Kapersky qui a découvert ce virus et qui déclara qu'il était si sophistiqué qu'il ne pouvait qu'être l'oeuvre d'un Etat avec des capacités technologiques importantes. Finalement l'opération Olympic Games aurait retardé d'un an le programme iranien.

C'est donc après cette attaque que l'Iran prend conscience de sa vulnérabilité face aux attaques informatiques et décide d'investir dans ce secteur.

La réponse ne se fait pas attendre car dès dès le premier semestre 2011, 46 établissements financiers new-yorkais sont paralysés par un DDOS. Cela a eu une conséquence très importante dans la vision des Etats-Unis. Alors que, comme nous l'avons vu, les Américains s'imaginaient pouvoir paralyser n'importe quel adversaire grâce à leurs capacités cyber, il se trouve que des pays bien moins puissants peuvent infliger des dommages non négligeables au pays notamment via l'intrusion dans les systèmes des infrastructures critiques. Cela a 2 conséquences majeures. Premièrement cela montre qu'une attaque informatique n'est pas aussi gratuite qu'elle semble être, du fait de la potentielle riposte de la cible. Deuxièmement c'est une nouvelle preuve de l'importance du potentiel asymétrique du cyber. On a vu précédemment que la Chine et la Russie l'avaient remarqué dès les années 1990 et aujourd'hui des pays encore moins puissants comme l'Iran ou la Corée du nord usent de cela pour attaquer leurs adversaires malgré un retard colossale dans le domaine militaire.

Bien que l'Iran soit aujourd'hui reconnu comme un des pays avec d'importantes capacités cyber offensives, il reste très loin derrière Israël ou les pays occidentaux cités précédemment. Cela est notamment dû au fait que ses attaques restent relativemment basiques et de faible ampleur. A cela s'ajoute des problèmes économiques importants ainsi qu'un budget en R&D bien plus faible que ses concurrents.

5 Bibliographie

Références

[1] IISS, Cyber Capabilities and National Power: A Net Assessment.

[2] F. DOUZET, Chine : cyberstratégie, l'art de la guerre revisité.

[3] L. GAYARD, Souveraineté numérique, enjeu géopolitique, Internet sécessionniste.

[4] A. Segal, Seizing Core Technologies: China Responds to U.S. Technology Competition.

[5] J.-L. Gergorin, L. Isaac-Dognin, Cyber : La guerre permanente.

[6] StatCounter, Search Engine Host Market Share Russian Federation Jan 2021 - Jan 2022.

[7] D. KOLESNYK, Du contrôle réflexif.

[8] T. BERTHIER, Maîtriser la donnée : enjeux et défis géopolitiques.

[9] M. RAFFRAY, Washington et Londres brandissent la cyberdissuasion.

[10] G. Greenwald, L. Poitras, E. MacAskill, NSA shares raw intelligence including Americans' data with Israel.

[11] A. Géry, La stratégie française de cyberdéfense.

[12] LeMonde, Quand les Canadiens partent en chasse de « Babar ».

[13] D. A. Fulghum, Why Syria's Air Defenses Failed to Detect Israelis.