Chapitre 7

La cyber-guerre

En 2007 l'Estonie, pays déjà très connecté, a mis un genou à terre suite à une attaque informatique massive de la part de la Russie probablement.

En 2010 un virus *a priori* israélo-américain détruisait les centrifugeuses du programme nucléaire iranien et retardait ainsi de quelques années le programme. C'était probablement la première fois qu'une cyber-attaque détruisait une cible physique.

En mai 2019, l'aviation d'Israël bombardait un immeuble de Gaza pour arrêter une cyber-attaque en cours. C'était probablement la première fois qu'une attaque physique était utilisée contre une attaque dans le monde virtuel.

La cyber-guerre est bien réelle et déjà utilisée par de nombreux pays. La frontière entre le monde physique et le monde virtuel n'a plus beaucoup de sens dans nos sociétés hyper-connectées aussi c'est sans surprise que les polices, les services secrets et les armées sont entrés dans la danse et qu'on parle de plus en plus de cyber-guerre.

Mais de quoi parle-t-on ? Où commence la cyber-guerre ? Est-ce que le piratage des données d'un ministère d'un pays étranger est un acte de guerre ou simplement d'espionnage ? Est-ce que casser l'infrastructure informatique d'une entreprise majeure est un acte de cyber-guerre ? Est-ce que la propagande entre dans la guerre ? Est-ce que perturber significativement une élection dans un pays étranger peut être considéré comme un acte de cyber-guerre ?

On voit que la définition n'est pas simple tant elle dépend de l'intention, de la réussite et de la portée de l'acte. Mais une ligne rouge existe.

> *Une attaque informatique majeure, par les dommages qu'elle causerait, pourrait ainsi justifier l'invocation de la légitime défense au sens de l'article 51 de la Charte des Nations Unies.*
>
> Revue stratégique de défense et de sécurité nationale 2017

La difficulté ne s'arrête pas là car si l'acte est défini comme un acte de cyber-guerre ou de guerre, deux questions restent en suspense : comment réagir et contre qui ? Une réaction physique avec destruction peut sembler disproportionnée et pourtant les dégâts d'une cyber-attaque peuvent

être bien plus importants que ceux d'un bombardement. Enfin trouver qui est à l'orgine d'une attaque est nettement plus difficile dans le monde virtuel que dans le monde physique.

Tout ces aspects font que la cyber-guerre est non seulement nouvelle structurellement puisqu'elle touche de l'immatériel, mais aussi dans son mode opératoire. Lorsque l'aviation a été utilisée comme une arme, il ne s'agissait, comme pour les autres armes, d'approcher de une cible physique pour la détruire. La bombe atomique, qui a soulevé bien des problème dans son usage, fonctionne aussi suivant le même principe. Mais ce n'est pas le cas des cyber-attaques qui touchent à distance l'immatériel lequel contrôle de plus en plus notre économie, nos modes de vie mais le monde physique voire nos vies. La cyber-guerre comme la guerre économique peut mettre un pays à genou sans l'attaquer physiquement [1] mais elle peut aller plus loin.

Dans ce chapitre nous commençons par regarder des exemples de cyber-attaques qui peuvent être assimilées à de la cyber-guerre. Puis nous regarderons d'autres attaques qui sont plus proches de la propagande mais que certains, comme les russes ou les chinois, intègrent dans une définition plus large de la cyber-guerre.

La seconde partie de ce chapitre se concentre sur les moyens mis en œuvre par les différents pays pour mener cette guerre. Pour commencer nous verrons que s'il est à la portée de presque tous les États de développer une cyber-force pour attaquer les infrastructures de l'ennemi, peu peuvent espérer couvrir l'ensemble du spectre des cyber-armes. Enfin nous regarderons les cyber-forces mises en place par différents pays.

7.1 Histoires de cyber-guerre

Depuis premier ver [2] lancé sur Internet en 1988 [3] l'histoire des agressions sur Internet a largement évolué pour arriver au niveau des armées qui préparent toutes les formes d'agressions possibles.

> *[Le cyberespace est un] lieu d'immense violence [dans lequel] tous les coups sont permis. [...] Le cyber est une arme d'espionnage, mais [c']est aussi une arme que des Etats utilisent pour déstabiliser, manipuler, entraver, saboter.*
>
> Florence Parly, ministre des armées – 2019

De fait, les attaques sont nombreuses et leur évolution montre l'implication de plus en plus importante des États. Le rapport impact/prix imbatable de ces attaques et l'importance grandissante d'Internet dans nos sociétés en sont les raisons premières. À cela s'ajoutent les innovations possibles dans l'usage de cette nouvelle arme. Aussi il n'y a pas de raison que la cyber-guerre baisse en intensité, pas tant que le rapport impact/prix ne chute au niveau de celui des armes conventionnelles, pas tant que les défenses et réponses des attaqués ne feront pas exploser le prix d'une cyber-attaque, pas tant que l'indentification de l'attaquant ne sera pas efficace.

1. ce qui se passe actuellement, en 2019, avec les États-Unis qui interdissent à toutes les entreprises mondiales de commercer avec l'Iran en est un exemple.
2. Un ver est un programme informatique malveillant qui se propage tout seul sur Internet.
3. Le ver de l'étudiant Morris qui a fait très mal à Internet à l'époque, à un niveau jamais atteint depuis heureusement. L'ironie est que ce ver n'était pas conçu pour faire mal mais un bug l'a rendu dangereux.

7.1.1 Estonie 2007

L'Estonie est un ancien pays du bloc soviétique d'un peu plus d'un million d'habitants.

En avril 2007 le gouvernement estonien décide de déplacer la statue du *Soldat de bronze* qui représente la libération du joug nazi par l'Armée rouge en 1944. Cette statue en plein centre ville n'était pas trop apprécié par les lituaniens qui y voyaient plus le symbole de l'occupation russe que celui d'une libération. Par contre pour la forte minorité russophone d'Estonie, environ 25% de la population, cette statue représente le combat soviétique contre les nazis.

La décision a donc soulevé des vagues de protestations tant de la part de la minorité russophone que des russes. Le 26 avril des manifestations font un mort et de nombreux blessés. Le lendemain les cyber-attaques commencent.

Les cyber-attaques

Les cyber-attaques utilisées en Estonie ont été principalement des dénis de service [4]. On a pu compter des centaines de milliers de botnets de plus de 50 pays, dont les États-Unis, ont envoyé des attaques sur les serveurs estoniens.

Les dénis de service peuvent être aussi de simples mails envoyés par millions à des adresses bien déterminées comme celles des députés listées dans un document partagé avec tout ceux qui désirent participer à l'attaque, voir figure 7.1.

Les cibles de la cyber-attaque de 2007 contre l'Estonie ont été :

- le parlement, les sites ministériels, le parti politique au pouvoir ;
- les journaux principaux ;
- les deux plus grandes banques, la Hansabank et la Eesti Ühispank ;
- des universités ;
- les infrastructures télécom du pays, le FAI [5] du gouvernement.

Dans un pays aussi connecté que l'Estonie cela a eu des conséquences terribles. Ainsi les clients de l'Hansabank n'avait plus accès à leur compte via Internet, service utilisé par 97% des clients,

4. Denial of Service en anglais, DoS, à savoir interroger un serveur (web par exemple) depuis des milliers voire millions de machines en même temps pour qu'il s'effondre, ne pouvant pas répondre à tous. On parle aussi de Distributed DoS, DDoS. Pour avoir un tel nombre de machine à sa disposition on pirate des machines sur lesquelles on installe des programmes dormants qui feront les attaques lorsqu'on leur demandera. Ces programmes, les *bots*, sont groupés en *botnets* pour synchroniser les attaques.

5. Fournisseur d'Accès Internet

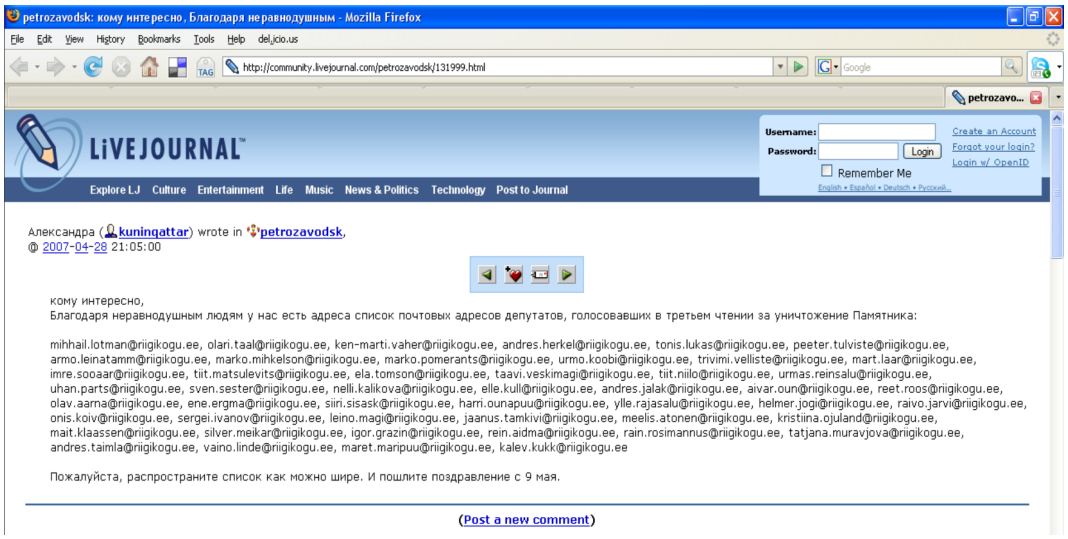


FIGURE 7.1 – Mails des députés estoniens publiés sur un site russe

mais aussi le système de vérification des transactions était hors service ce qui a perturbé fortement le fonctionnement des distributeurs de billets et a bloqué les connexions avec les banques à l'étranger donc interdit aux clients de cette banque à l'étranger d'utiliser leur carte de paiement. Les services institutionnels étaient bloqués pour un grand nombre et l'infrastructure télécom elle même a été touchées à des endroits pourtant pas connus du grand public normalement.

La défense estonienne a mis en place une cellule de crise pour gérer la défense. Cette cellule a obtenu l'aide de pays étrangers comme l'Allemagne, l'Italie ou l'Espagne et bien des pays baltes voisins la Lituanie et la Lettonie. Elle a aussi été assistée par les FAI étrangers qui ont bien voulu couper la communication aux ordinateurs les plus agressifs qui passaient sur leur réseaux. Mais surtout, après 3 semaines d'attaques et de chaos, le gouvernement estonien a pris la décision de couper les connexions à l'international ce qui a coupé l'Estonie de l'Internet mais ce qui a réussi à réduire assez les attaques pour réagir et remettre en état le réseau.

Le 19 mai les attaques ont arrêté.

Les responsables

Si la coordination des attaques était visible sur des sites web russe où il était indiqué les adresses IP des cibles et les dates des attaques, rien n'indiquait a priori que le gouvernement russe était aux commandes. Des activistes auraient pu être à l'initiative des attaques comme, plus tard, les Anonymous l'ont fait lors de l'Operation Payback contre les entreprises ayant, de leur propre initiative, bloqué les comptes de Wikileaks.

Cependant l'ampleur de l'attaque et son excellente coordination rendent plus probable l'implication des autorités russes avec a priori au moins un accord implicite de la présidence. Le gouvernement estonien a déclaré avoir relevé des adresses IP d'ordinateurs de l'administration centrale russe parmi les attaquants. Pour l'Estonie, l'implication de la Russie est évidente.

m.à.j. sur http://www.ricou.eu.org/e-politique.html

Mais aujourd'hui il n'y a toujours pas de preuve formelle du niveau d'implication des autorités russes. De plus ces dernières ont toujours déclaré officiellement ne pas être liées à ces attaques. Seuls des officiels russes ont déclarés en leur nom que tel ou tel groupe d'activistes avait mené l'attaque avec eux, mais rien de convainquant a priori.

On trouve ici une caractéristique de la cyber-guerre à savoir la difficulté de nommer l'agresseur et surtout d'apporter les éléments qui le prouvent. Dans certains cas l'agresseur peut désirer qu'on sache que c'est lui sans toute fois qu'on puisse le prouver. Dans notre cas on peut supposer que les russes ne sont pas mécontents que l'Estonie les considère responsables de l'attaque.

Les réactions

La statue a été transférée dans le cimetière militaire conformément à la volonté des autorités estoniennes.

L'Estonie a profité de l'ampleur de l'attaque pour s'afficher en victime et bénéficier de la sympathie occidentale. Elle a pu également se servir de l'évènement pour pousser sa demande de cyber-défense au niveau de l'OTAN.

En 2008 le Centre d'Excellence de Coopération en Cyber Défense de l'OTAN a été créé à Tallinn. Les pays qui ont aidé l'Estonie durant la crise ont rejoint le centre dès le début. Les États-Unis l'ont rejoint en 2011, la France et l'Angleterre en 2014. Son but est de partager entre ses membres les connaissances en cyber-défense.

Tant à travers ce centre que par des accords avec les entreprises privées et les citoyens, l'Estonie a depuis développé sa cyber-défense. Un des éléments visibles est la réserve citoyenne d'informaticiens certifiés par l'OTAN qui peut être mobilisée en cas de nouvelle cyber-guerre.

7.1.2 Géorgie 2008

En 2008 la Géorgie décide d'attaquer la région d'Ossetie du sud qui fait preuve de sécessionisme mais la Russie choisit de protéger cette dernière et envahit la Géorgie. La région d'Abkhazie profite de l'occasion pour se rebeller et trouve aussi le soutien de la Russie. La guerre a duré 9 jours, du 7 au 16 août 2008 pour finir sur la sécession *de facto* de l'Ossetie du sud et de l'Abkhazie.

L'intérêt de cette guerre dans le cadre de la cyber-guerre est qu'elle est la première guerre qui couple l'attaque cyber à l'attaque physique. On a pu noter non seulement une concordance temporel, des cyber-attaques ont commencé en même temps que les mouvements de troupe, mais aussi géographique avec des cyber-attaques localisées. Le but était non seulement de rendre le réseau internet géorgien inopérant mais aussi de le détourner dans un but de propagande.

FIGURE 7.2 – Cartographie de la deuxième guerre d'Ossétie du Sud – 7-16 août 2008
source : Wikipedia – 2019

Les cyber-attaques russes

On retrouve le même mode opératoire que pour l'Estonie à savoir des DoS (Dénis de services) probablement lancé par les personnes externes au gouvernement russe [6] et probablement coordonnées par le gouvernement russe. Le site `stopgeorgia.ru` a apporté son aide aux attaques en offrant au téléchargement des logiciels d'attaques. Ainsi toute personne à travers le monde qui désirait aider la Russie pouvait le faire très simplement. Ce recrutement gratuit couplé au faible coût d'achat de cyber-attaques fait que cette campagne de DoS a eu un coût ridiculement faible (un expert a chiffré l'ensemble de la campagne au prix d'une chenille de char).

Une autre attaque a consisté à pirater le réseau géorgien et rediriger ses connexions sortantes vers la Russie et la Turquie où elles étaient bloquées. Ainsi la Géorgie n'avait plus accès au reste du monde.

Cependant la Géorgie étant nettement moins connectée que l'Estonie, l'impact a été moins fort. La perte pour le gouvernement géorgien de ses canaux numériques de communication n'était pas vitale tant vis à vis de ces citoyens que de l'étranger.

Les autres cyber-attaques entrent dans le cadre de la guerre de l'information. Il s'agit de justifier l'invasion de la Géorgie en dénigrant l'adversaire (on notera en particulier la comparaison du président géorgien avec Hitler figure 7.3) tout en soulignant l'aide qu'apporte la Russie aux

6. Le groupe de pirate Russian Business Network basé à St Pertersbourg a été montré du doigt.

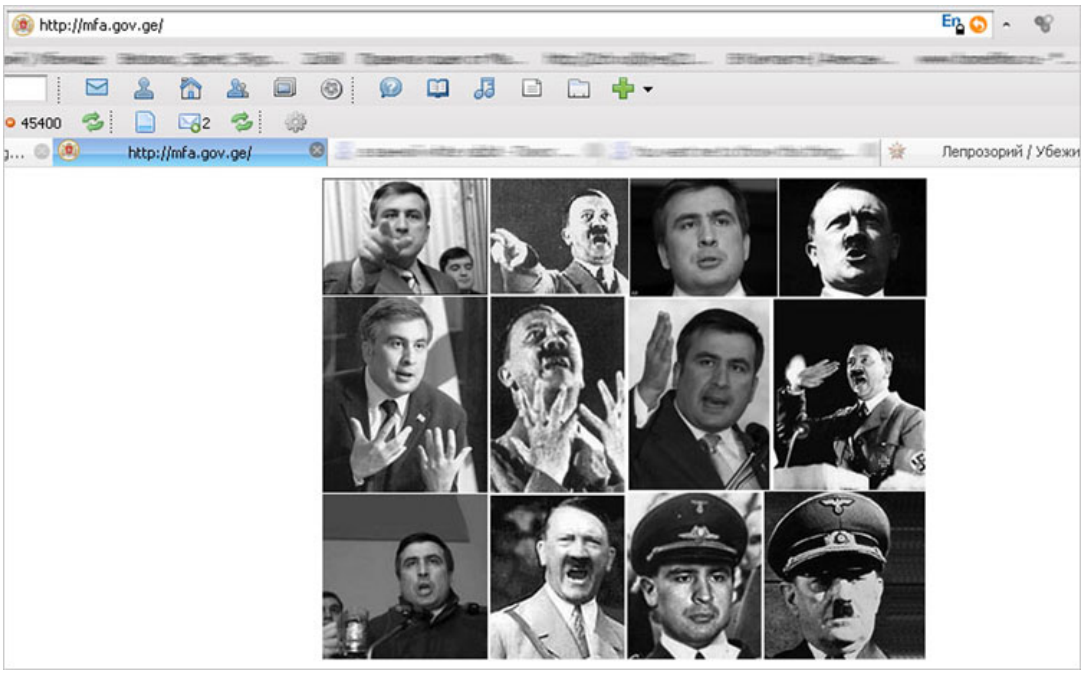


Figure 7.3 – Le site de l'assemblée nationale géorgienne piraté
Le président de la Géorgie, Mikheil Saakashvili, comparé à Hitler.

peuples d'Ossetie et d'Abkhazie. Pour la Russie cette guerre de l'information est un des piliers de la cyber-guerre.

Les cyber-attaques géorgiennes

Les russes ont aussi déclaré avoir été piratés et ont accusé les géorgiens. Le premier site à avoir été piraté par les géorgiens semble être celui de l'agence de presse d'Ossetie du sud, OSInform News Agency, qui a vu son contenu remplacé par celui d'une agence favorable à la Géorgie. L'agence de presse russe RT a aussi déclaré avoir été attaquée ainsi que des sites web russes officiels.

Mais ce qui a le plus marqué les russes, ce sont les attaques sur leur réseau militaire de communication. Il semblerait qu'avec l'aide des américains, les géorgiens aient réussi à perturber suffisamment ce réseau pour que des officiers russes doivent utiliser leurs téléphones personnels pour communiquer.

D'autre part l'armée russe a clairement fait preuve d'un manque d'équipement numérique dans cette guerre comme l'usage de drones pour éviter de tomber dans des embuscades.

Ces points négatifs pour les russes sont à l'origine de la prise de conscience de l'armée russe du besoin d'intégrer en son sein la cyber-guerre et de ne plus la laisser exclusivement aux services secrets.

7.1.3 Iran 2010

L'attaque des installations nucléaires de l'Iran a été une véritable surprise. Pour la première fois des pays ont utilisé un virus pour détruire des appareils d'un pays ennemi. On a découvert que le virtuel pouvait être utilisé pour détruire du matériel physique ultra protégé.

Avant d'examiner la cyber-attaque regardons le contexte géopolitique. En 2010 l'Iran est un pays en marge de la communauté internationale qui affirme vouloir détruire Israël. Les tensions avec les États-Unis et Israël sont très fortes. L'Iran cherche à se doter de l'arme nucléaire, seule protection efficace en cas de guerre contre ces pays et probablement la seule façon de rayer Israël de la carte [7].

Pour les États-Unis et Israël il faut agir avant que l'Iran ait la bombe atomique. Les israéliens aimeraient lancer des bombardements aériens comme ils l'ont fait jadis contre la centrale nucléaire syrienne, mais l'Iran est nettement plus loin, plus grande et ses centres nucléaires sont dispersés et fortement protégés.

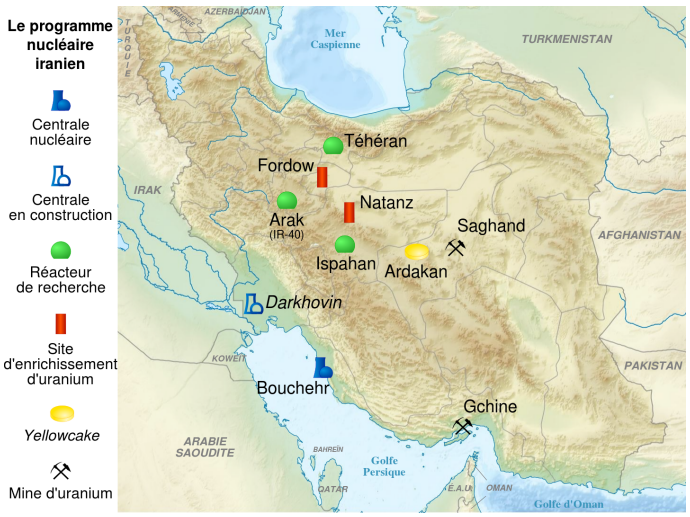


FIGURE 7.4 – La programme nucléaire iranien
source : Wikipedia – 2012

De son coté, la communauté internationale cherche une solution qui ne dégénère pas en guerre.

Stuxnet

Une cyber-attaque directe contre les installations nucléaires iraniennes n'était pas possible pour la simple et bonne raison que ces installations n'étaient pas reliées à Internet. Pour les toucher il fallait donc déposer dans le réseau local un programme qui puisse attaquer, un virus. Si ce virus peut se débrouiller tout seul pour se diffuser et dans, notre cas trouver le réseau local des centres nucléaires visés, c'est encore mieux. C'est le principe du ver. Dans le cas d'un réseau non

7. Officiellement l'Iran développe un programme nucléaire civil.

connecté à Internet, un ver passe le plus souvent par des clefs USB qui ont été connectées aux deux réseaux.

L'attaque est donc d'un ver qui a probablement été conçu vers 2005 mais qui n'a été découvert qu'en 2010 par l'entreprise de sécurité informatique Kaspersky Lab. Ces ingénieurs ont découvert le ver sur Internet sans rien comprendre initialement de ce programme très sophistiqué qui n'avait aucun comportement agressif. Ce ver appelé Stuxnet est un programme de très haute qualité :

— son code est très dense et très difficile à comprendre ;
— il n'a pratiquement pas de bug ;
— il exploite 4 failles de sécurité dites *zero-day* à savoir inconnues, une pour se diffuser via USB, une pour exécuter du code à distance et deux pour obtenir des privilèges d'exécution ;
— il a été signé par des certificats officiels de Microsoft, lesquels certificats ont été volés, *a priori* physiquement, dans des entreprises taïwanaises.

Le coût pour développer un tel ver est énorme, tant par le temps humain nécessaire pour le développer, 27 hommes/an d'après Microsoft, que par la valeur marchande des failles *zéro-day*, ½ M$ sur le marché noir, et le besoin d'intervention physique pour le vol des certificats. Il semble donc qu'il s'agisse d'un programme étatique ou d'une organisation criminelle de grande envergure.

Pour les ingénieurs de Kaspersky, tant que la cible de ce ver inoffensif n'était pas trouvée, il était difficile de connaître son origine. Cela pouvait être une bombe à retardement dans le but de faire un chantage à grande échelle, une attaque tellement bien ciblée qu'on ne la voit pas si on n'est pas la cible, ou encore autre chose.

En analysant le code, la cible a finalement été trouvée, il s'agissait de contrôleurs industriels bien spécifiques fabriqué par Siemens, les contrôleurs qui commandaient les centrifugeuses iraniennes de leur programme d'enrichissement de l'uranium. Une fois que Stuxnet avait trouvé sa cible, il s'activait pour faire tourner les centrifugeuses trop vite jusqu'à ce qu'elles cassent, tout en indiquant aux différents appareils de contrôle un comportement normal.

Figure 7.5 – Centrifugeuses inspectées par le président Ahmadinejad

Une fois la cible découverte, les coupables ont rapidement été désignés à savoir les États-Unis via la NSA et le Cyber Command avec les Israëliens via leur unité 8200 spécialisée dans le cyber. Bien sûr ces pays nient leur participation.

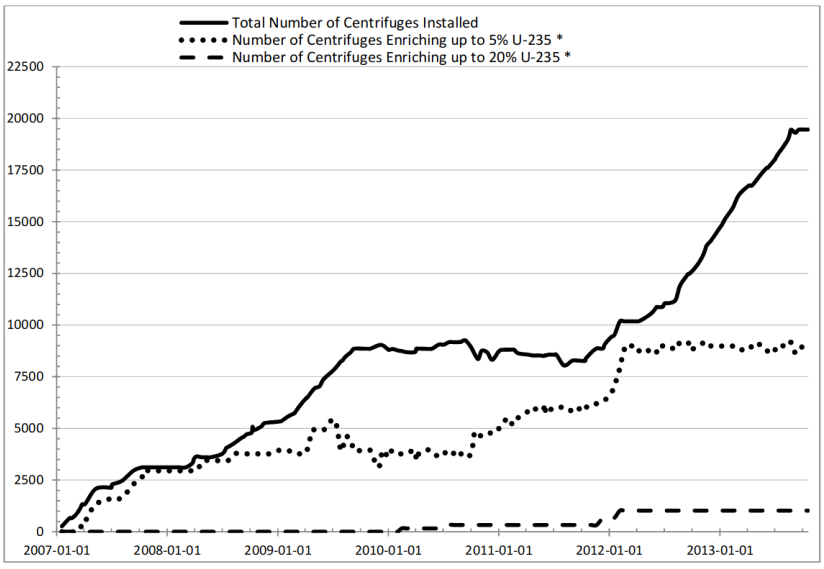
Conséquences

Stuxnet a eu de nombreuses conséquences. Tout d'abord c'est un succès militaire puisque plus d'un cinquième des centrifugeuses ont été détruites ce qui a fortement pénalisé le programme nucléaire iranien. On soupçonne d'ailleurs la démission en juillet 2009 de M. Aghazadeh, responsable du programme nucléaire iranien, d'être due aux retards générés par Stuxnet.

La seconde conséquence est la découverte publique qu'on peut faire du sabotage physique via le monde virtuel.

La troisième conséquence a été l'accélaration de l'installation de de centrifugeuses par l'Iran afin de combler le retard comme le montre la figure 7.6. Si Stuxnet a pu retarder le programme nucléaire iranien, il ne l'a pas arrêté.

Figure 1: Status of Centrifuges in Iran



Note 1: Centrifuges involved in R&D activities are not included.
**Not all of the centrifuges fed with UF_6 may have been working.*

FIGURE 7.6 – Évolution et affectation des centrifugeuse d'enrichissement d'uranium en Iran
source : Agence Internationale de l'Energie Atomique – 14 nov. 2013

La quatrième conséquence a été le cyber armement de l'Iran. Deux ans après la révélation de Stuxnet, des cyber-attaques ont visé la Saudi Aramco qui a eu 30 000 ordinateurs effacés soit 75% de son parc informatique avec toutes les répercussions imaginables en termes de production. La même année, en 2012, l'opération Ababil a bloqué la Bank of America, JP Morgan, Citigroup, US Bank, Wells Fargo et PNC aux États-Unis. Sans se déclarer à l'origine des attaques, l'Iran a pu faire passer le message de l'équilibre de la terreur à savoir "Moi aussi je suis armé maintenant".

7.1.4 États-Unis – 2016

L'histoire retiendra peut-être que le 45ième président des États-Unis a été choisi par les russes.

On a vu dans le chapitre sur la communication comment la Russie a acheté des publicités sur Facebook pour pousser certains groupes à voter (les catholiques traditionalistes qui n'appréciaient pas que Trump ait divorcé deux fois) et certains groupes à rester chez eux (les afro-américains votent démocrate généralement), cf 7.7. L'enquête effectuée après l'élection a révélé que plus de cent millions d'américains ont été touchés par ces publicités ciblées.

Figure 7.7 – Publicités russes sur Facebook durant l'élection aux E.U. en 2016

Ces messages sur Facebook ne sont bien sûr pas la seule action imputée aux russes. Les fuites sur le contenu des e-mails d'Hilary Clinton révélées par Wikileaks avant les débats avec Donald Trump sont probablement des documents piratés par les services russes. Les informations s'y trouvant ont eu un poids important dans le premier débat mettant la candidate démocrate dans une situation délicate. Voici deux exemples qui montrent comment l'impact que peuvent avoir de telles fuites.

Hilary Clinton a indiqué dans un de ces documents fuités qu'elle approuve la phrase de Lincoln dans le film du même nom, qui indique que parfois les politiciens doivent avoir des discours différents en privé et en public. Lors du débat un des modérateurs lui demande s'il est acceptable pour un politicien de jouer un double-jeu. Sachant que la candidate avait déjà refusé d'évoquer des discours privés, son image d'hypocrite en était renforcée.

Dans un autre document elle indique rêver d'un espace nord américain ouvert commercialement et sans frontière. Lorsque durant le débat Donald Trump l'accuse de vouloir ouvrir les frontières et donc favoriser l'immigration elle s'en défend mais le modérateur cite ce document ce qui sous-entend qu'elle ment.

On voit comment des documents privés révélés au bon moment peuvent aider le candidat adverse. Les MacronLeaks, à savoir les boites mails de son équipe de campagne piratées et diffusées juste avant le débat du second tour allaient dans le même sens.

L'élection présidentielle 2016 était particulièrement serrée avec un taux d'indécis très élevé, 15% une semaine avant l'élection. Sachant que Donald Trump a gagné de justesse, des universitaires [8] et officiels [9] pensent que la Russie a réussi à faire basculer l'élection.

Dans cet exemple le terme de cyber-guerre est moins évident. Il n'y a pas eu de dégradation du réseau informatique américain ni de destruction matérielle, pourtant l'impact est immense. Il est évident que les américains ont été pris par surprise et qu'ils feront tout pour que ce genre de situation ne se reproduise pas. Toute la question est de savoir ce que ce *tout* va couvrir. Si cela peut mener à des représailles guerrières, on pourra considérer que manipuler une élection de cette importance est un acte de cyber-guerre.

7.1.5 La suite

À travers ces exemples on a vu différents types d'agression avec différents buts :

- des DoS pour paralyser le réseau ennemi,
- du piratage pour la même raison (mais aussi pour espionner dans d'autres cas),
- de la propagande pour justifier une opération miliaire traditionnelle,
- un virus utilisé comme arme pour détruire du matériel ennemi,
- de la manipulation d'opinion pour faire basculer une élection.

On retrouve ces types d'attaque et d'autres en dehors des cas présentés. Par exemple l'Ukraine, en guerre larvée avec la Russie depuis 2014, est un terrain de cyber-guerre actif et a déjà accumulé un bon nombre de cyber-attaques (sabotage du réseau électrique, le virus NotPetya pour bloquer les réseaux informatiques de nombreuses entreprises ukrainiennes, propagande en ligne pour l'élection sur le rattachement de la Crimée à la Russie…).

Un des points qui ressort de ces différentes attaques est que la notion de cyber-guerre n'a pas la même portée suivant les pays. Pour les russes et les chinois, la guerre de l'information fait partie de la cyber-guerre ce qui n'est pas le cas pour les occidentaux qui se focalisent sur les infrastructures. L'information est un enjeu bien plus critique pour les régimes autoritaires en particulier en interne, mais l'exemple de l'élection américaine de 2016 montre qu'un bon contrôle de l'information et savoir manipuler l'opinion est aussi une force d'attaque contre d'autres pays.

La suite va vers une militarisation de l'Internet. Les grands acteurs préparent le terrain pour d'éventuels conflits. Cela se fait en prenant le contrôle d'ordinateurs, en cartographiant l'architecture des réseaux ennemis, en "minant" le réseau :

> *Ce qui nous préoccupe le plus aujourd'hui, ce sont des attaques où l'on ne voit pas quel est l'objectif. Ce n'est pas de l'espionnage, du détournement de données personnelles. Ce n'est pas encore du sabotage, [mais] des gens de très haut niveau qui préparent les*

8. Voir le livre de la chercheuse K.H. Jamieson "Cyberwar. How Russian Hackers and Trolls Helped Elect a President - What We Don't, Can't, and Do Know".
9. J. Clapper, directeur du renseignement national d'alors, a affirmé que la Russie a fait basculé l'élection.

conflits de demain.

Guillaume Poupard, directeur de l'ANSSI – 2018

La cyber-guerre se prépare aussi en isolant son réseau de l'Internet. Les chinois sont connus pour leur muraille virtuelle appelée aussi le grand parefeu de Chine [10] et les russes sont en train de faire de même. Une loi dite de sécurité informatique oblige l'infrastructure Internet russe à être autonome et donc de ne pas dépendre de serveurs étrangers, y compris du DNS ou de nuages non russes. Cette loi doit entrer en vigueur en novembre 2019.

Les États-Unis étant à l'origine de l'Internet et ayant de facto le contrôle dessus, on peut donc diviser l'Internet actuel en trois zone, la chinoise, la russe et l'américaine, l'Europe étant un vassal des américains.

7.2 L'armement cyber

Les exemples de cyber-guerre présentés permettent d'avoir une idée des armes utilisées mais il ne s'agissait que d'armes relativement basiques en dehors de Stuxnet. Regardons ce qui permet à un pays de développer une cyber-force de qualité.

7.2.1 Niveau 1 : pirates et virus

La première cyber-arme est relativement accessible, peu chère et efficace. Vous embauchez une vingtaine de bons informaticiens, vous leur donnez une bonne connexion et vous avez votre commando prêt à faire plein de choses terribles à travers toute la planète. Il n'existe pas d'arme qui soit plus rentable. Alors pourquoi s'en priver ?

C'est probablement ce que se disent les dirigeants. D'ailleurs en 2019 on compte déjà plus de 30 pays qui ont annoncé avoir une cyber-force. Bien sûr tout le monde n'est pas au même niveau. Les grandes puissances et les pays les plus développés sont déjà bien équipés tout en étant aussi les plus vulnérables car les plus connectés.

En effet Internet a changé notre monde, en particulier dans les pays les développés. Nous sommes devenus numériques et interconnectés. Cela a changé fondamentalement nos façons de travailler, les interactions entre les entreprises, avec l'administration. Sans Internet nos économies s'effondreraient.

La logique voudrait que ces acteurs/pays se protègent. Malheureusement la défense est chère et pas suffisamment efficace. Aussi la majorité met en place des mesures de sécurité raisonnablement efficace contre des pirates occasionnels mais rarement suffisantes contre des experts motivés. Pour le monde économique le réseau doit fonctionner. Le coût de se couper de l'Internet à des fins de protection est bien trop élevé par rapport au coût du risque d'une cyber-attaque [11].

10. The Great Firewall of China

11. Le coût du risque étant le coût des dégats infligés par l'attaque multiplié par la probabilité d'être attaqué avec succès. On peut l'assimiler au prix d'une assurance tout risque.

Aussi avoir une cyber-armée pour attaquer tout ces acteurs économiques mal protégés est très tentant. Que cela soit pour du simple espionnage, pour du sabotage plus ou moins léger ou pour mettre hors jeu l'adversaire, l'arme cyber s'intègre parfaitement dans la guerre économique. Et lorsqu'on n'attaque pas, on peut préparer le terrain.

Dans ce domaine les américains sont les rois. Depuis la fin de la guerre froide en 1989, ils ont réaffecté leurs capacités d'espionnage à la guerre économique. On a vu qu'avec l'avènement de l'Internet cet espionnage a pris de plus en plus d'importance et a permis une surveillance globale non seulement des gouvernements et des acteurs économiques mais aussi des citoyens. La NSA de la guerre froide est devenu le Big Brother mondial pour le plus grand bénéfice des États-Unis.

La Chine aussi est accusée d'utiliser Internet afin de pirater des entreprises occidentales pour récupérer leurs secrets industriels. L'administration Trump a déclaré en 2019 que la Chine lui vole entre 200 et 600 milliards de dollars par an de secrets technologiques.

7.2.2 Niveau 2 : savoir

L'information est le nerf de la guerre et c'est doublement vrai sur Internet, premier outil d'information.

Les GAFAM sont connus pour être des monstres économiques mais ils sont aussi les gestionnaires de nos vies numériques. Ils savent ce nous faisons en tant qu'individu mais aussi en tant que groupe de personnes. Ils ont une vision comme peu ont de l'activité de nos sociétés, des modes, des maladies, des évolutions. Ils ont aussi pour certain la vision du fonctionnement de l'Internet.

Ce dernier point est un véritable atout stratégique en cas de cyber-guerre puisqu'il permet de connaître le terrain de combat. Les points précédants sont aussi importants puisque le but d'une cyber-guerre est de toucher un pays ennemi et pour cela, la compréhension des comportements humains et sociétaux permet non seulement de mieux toucher sa cible mais aussi d'anticiper les réactions de l'ennemi et de son propre peuple.

Comme aucune armée n'a les moyens de developper ses GAFAM, on comprend qu'au niveau d'un pays, avoir de telles entreprises chez soi offre un avantage évident. Bien sûr faut-il que les entreprises collaborent avec les autorités mais c'est toujours le cas. Ainsi les services secrets des États-Unis, grâce au programme PRISM, peuvent légalement accéder aux données des GAFAM avec une facilité qu'aucun autre pays n'a.

En Chine ce sont Baidu, Alibaba, Tecent et Xiaomi, les BATX, qui sont les équivalents des GAFAM. Elles aussi sont liées à leur État et doivent lui transmettre les informations dont il a besoin. La domination totale de ces entreprises en Chine lui offre une bonne connaissance de sa population et de son réseau tout en réduisant la capacité de forces étrangères d'avoir accès à ces informations.

La Russie, avec Yandex et VK, est dans le même cas que la Chine avec néanmoins une pénétration des GAFAM significative d'où la volonté des autorités russes d'avoir un contrôle local sur ces entreprises américaines.

L'Europe enfin est dans la situation la plus délicate. Ses citoyens et entreprises reposent essentiellement sur les GAFAM mais ces dernières répondent à la justice des pays européens. Ainsi la police peut obtenir auprès des GAFAM l'accès à des informations nécessaires à une enquête mais

la procédure sera nettement plus compliquée que pour les autorités américaines et ne pourra probablement pas répondre aux besoins des armées européennes. Par contre en cas de tensions entre l'Europe et les États-Unis, l'Europe peut perdre tout contrôle sur ces données.

Les câbles

L'accès à l'information peut aussi se faire en interceptant les communication directement sur le réseau, aux points d'interconnexion ou directement sur les dorsales de l'Intenet. Les fibres sous-marines par lesquels passent la quasi totalités de communication entre les continents voire pays sont des éléments stratégiques de première importance.

Dans ce domaine encore les États-Unis ont une longueur d'avance. En plus d'avoir sur leur sol la majorité des câblo-opérateurs et donc de pouvoir les contraindre à permettre l'interception des communications, ils ont aussi la capacité d'aller écouter les câbles au fond de l'eau. Notons que les russes savent aussi aller espionner les câbles au fond de l'eau.

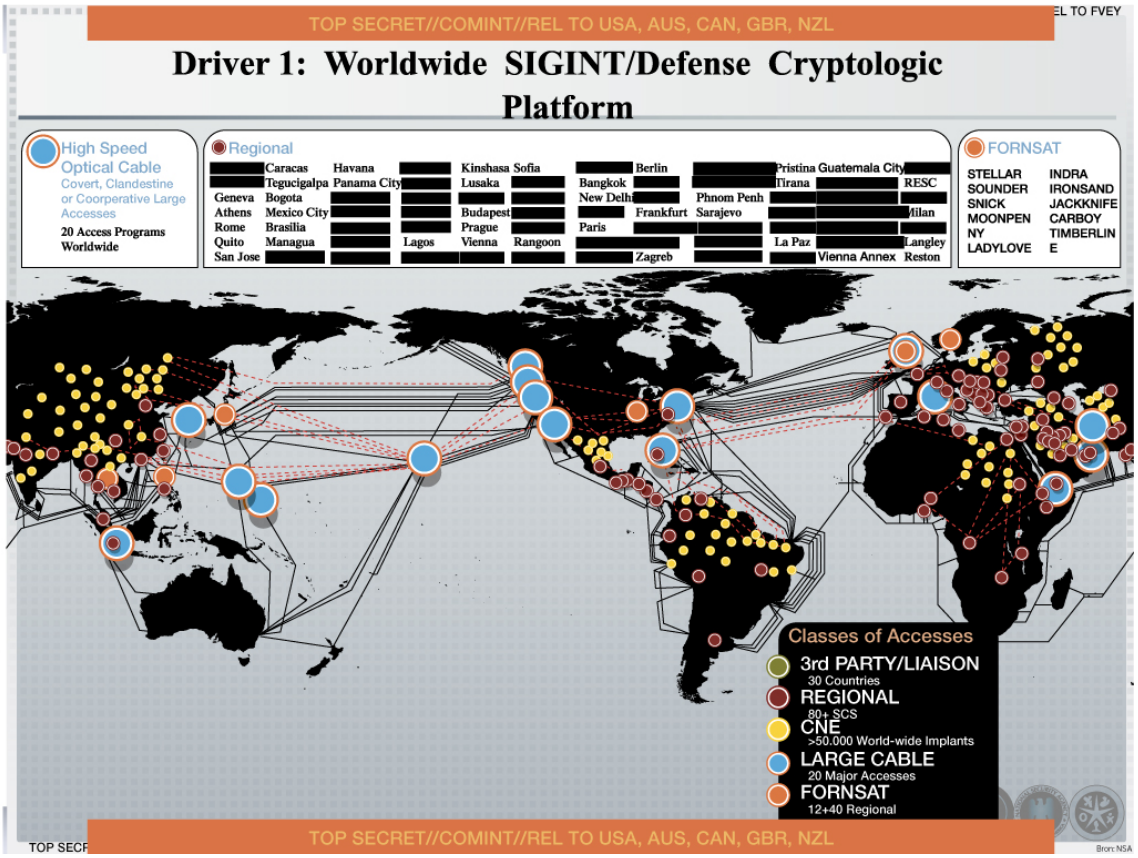


Figure 7.8 – Point d'écoute de la NSA en 2012
source : Edward Snowden – 2013

Cela étant espionner les câbles est plus difficile que d'utiliser la loi pour demander à ses GAFAM de fournir les données. Il faut pouvoir poser des appareils d'espionnage sur chaque câble, être capable de déchiffrer ce flux d'information et pouvoir organiser et stocker cette quantité astronomique d'information pour l'exploiter. On n'est plus du tout dans les mêmes ordres de grandeur

en terme de coût par rapport à la petite équipe d'informaticiens.

Si les câbles sont intéressants pour obtenir de l'information, ils sont aussi une source de vulnérabilité. Casser un câble est relativement simple et l'impact est tout de suite très important. Pour certains pays qui n'ont pas de redondance, la perte d'un tel câble revient à être coupé de l'Internet [12]. Pour les autres, la redondance les protège des accidents mais en cas de guerre, on voit mal comment protéger tout ces câbles, sachant qu'il n'est pas nécessaire de les couper tous pour saturer Internet.

7.2.3 Niveau 3 : pirater le matériel

Si des informaticiens peuvent infiltrer des réseaux informatiques et y déposer des bombes ou simplement écrire des virus qui feront le travail tout seul, il est possible de faire nettement mieux. Il est possible de contrôler le matériel informatique.

La crise actuelle sur la 5G et le choix américain d'interdire à Huawei l'accès à son marché en est l'illustration [13]. Le contrôle des infrastructures informatiques est devenu vital pour les pays, ce qui fait passer les considérations économiques au second rang. Même si Huawei présente la meilleure solution technique pour le prix le plus faible, le risque que son matériel puisse être activé à distance par la Chine pour espionner ou saboter le pays client devient trop grand étant donné l'importance d'Internet dans nos sociétés. Le coût du risque devient significatif voire trop important par rapport à la différence de prix entre une technologie locale et celle d'une compagnie étrangère en laquelle on n'a pas confiance. Pour l'Europe, le coût de refuser le matériel de Huawei pour la 5G est estimé à 55 G€ et 18 mois de délais par Reuters [14].

Cette guerre de la 5G est visible mais elle n'est pas la première dans le domaine matériel. Les États-Unis d'Obama avait déjà banni cette entreprise chinoise et sa consœur ZTE des réseaux filaires américain. L'Australie avait déjà refusé un marché de fibre sous-marine à Huawei pour des raisons de sécurité.

Le contrôle du matériel informatique dans une cyber-guerre est bien sûr un atout de luxe mais dont le coût est nettement moins abordable puisque le pays doit avoir des entreprises compétitives dans le domaine. De fait seuls les États-Unis, la Chine et l'Europe semblent en mesure de jouer sur ce terrain.

Il est possible d'aller plus loin dans le contrôle du matériel. On peut mettre des instructions pour détruire un processeur ou permettre d'en prendre le contrôle à distance. Sachant que les appareils informatiques d'un réseau en ont un très grand nombre, il devient possible de tuer voire de contrôler ces appareils et donc le réseau à distance. Ainsi il suffit de fabriquer un des processeurs d'un appareil pour pouvoir au moins abimer ce dernier à distance. On soupçonne l'aviation israélienne d'avoir utilisé un tel procédé pour rendre inopérant les radars syriens lors d'une attaque aérienne en 2007.

12. En 2017 la Somalie a été ainsi coupée du monde pendant 3 semaines après qu'un porte-conteneurs a coupé le câble sous-marin qui reliait le pays à Internet. Le coût de la perte d'accès à Internet a été évalué à 9 M€ par jour soit presque la moitié de son PIB journalier.

13. En juin 2019, le Japon, l'Australie et la Nouvelle-Zélande avaient déjà emboité le pas des USA et banni Huawei pour la 5G.

14. Nokia, solution de remplacement à Huawei, estime que le coût serait nettement inférieur.

Là où l'affaire devient terrible c'est qu'un processeur peut être modifié à l'insu de ses concepteurs. Cela peut avoir lieu lors de la fabrication, l'usine peut modifier discrètement le processeur sans rien changer des fonctionnalités attendues. Dans un monde où la majorité des processeurs sont fabriqués en Chine, le risque devient immense pour les autres pays.

Enfin, après que le processeur ait été fabriqué, des modifications peuvent encore être effectuées à l'aide de faisceaux ioniques. Snowden a montré que la NSA intercepte du matériel informatique pour y placer des mouchards avant livraison. Elle pourrait aussi intecepter des livraisons de processeurs pour y mettre des portes dérobées. Les pays peuvent aussi vouloir modifier des processeurs du grand public avant de les intégrer dans du matériel sensible vendu à l'étranger.

On est donc dans une situation où :

— une faille logicielle permet une intrusion voire le contrôle ;
— une porte dérobée d'un appareil permet son contrôle à distance ;
— un processeur peut être conçu pour altérer l'appareil qui le contient ;
— un processeur peut être piraté pour permettre au pirate d'en avoir le contrôle.

7.2.4 Niveau 4 : l'intelligence artificielle

Si les humains ne peuvent pas appréhender ce qui ce cache derrière des flux de données et réagir immédiatement, les ordinateurs peuvent le faire à condition d'avoir l'algorithme qui permet de traiter les données et d'indiquer comment réagir. Écrire un tel algorithme pour analyser des données qui peuvent être aussi variées que du texte, du son, des images, des films, des codes binaires, des données chiffrées et plus est mission impossible. La seule possibilité d'y arriver semble être d'utiliser l'intelligence artificielle (IA).

Les progrès de l'IA depuis le début des années 2010 sont fulgurants. Alors qu'un ordinateur ne pouvait pas comprendre ce qu'il y a dans une image en 2010, l'IA permet aujourd'hui de décrire une scène en indiquant ce qui s'y trouve. L'IA commence aussi à comprendre le sens des phrases ce qui permet non plus de rechercher le mot "bombe" dans tous les mails mais de lui demander si elle détecte une volonté de préparer une attaque terroriste comme pourrait le faire un humain qui lirait tous les mails. Mais là où l'IA devient indispensable c'est pour lire les données binaires qui circulent sur Internet afin de repérer les virus ou autres formes d'attaques numériques.

L'IA ne s'arrête pas à l'analyse, elle peut aussi apprendre à agir. Les voitures autonomes en sont l'exemple le plus connu mais les majordomes virtuels, les publicités en lignes, les drônes autonomes sont autant d'exemples d'IA qui agissent. Aussi il est tout à fait envisageable de laisser le contrôle des cyber-attaques et de la défense à des IA [15]. Leur vitesse d'exécution et leur capacité à analyser des flux d'information énormes devrait pouvoir dépasser les capacités humaines. Le monde des jeux stratégiques a déjà montré la supériorité de la machine pour de plus en plus de jeux. La marche suivante ne semble pas inaccessible.

15. Mais aussi laisser à l'IA le contrôle des armes conventionnelles et développer des blindés, avions, navires, soldats et généraux autonomes.

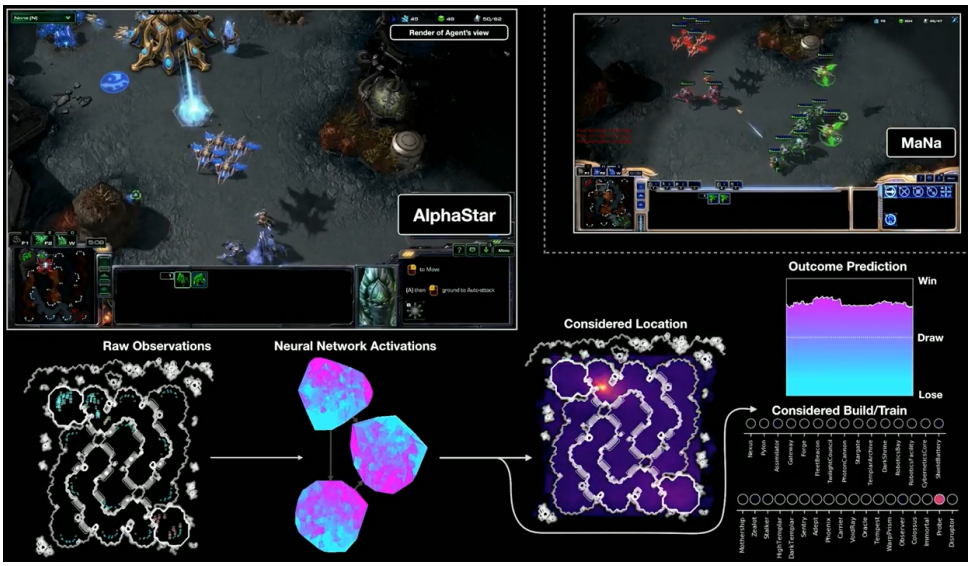


FIGURE 7.9 – Victoire facile d'Alphastar, l'IA de Google, contre un des meilleurs humains

Si on combine l'avantage stratégique qu'offre l'intelligence artificielle à l'avantage économique, on comprend que sa maîtrise soit considérée comme de toute première importance par les pays. Dans ce domaine les États-Unis et la Chine sont en position favorable mais les pays européens ainsi que la Russie affichent aussi leurs ambitions.

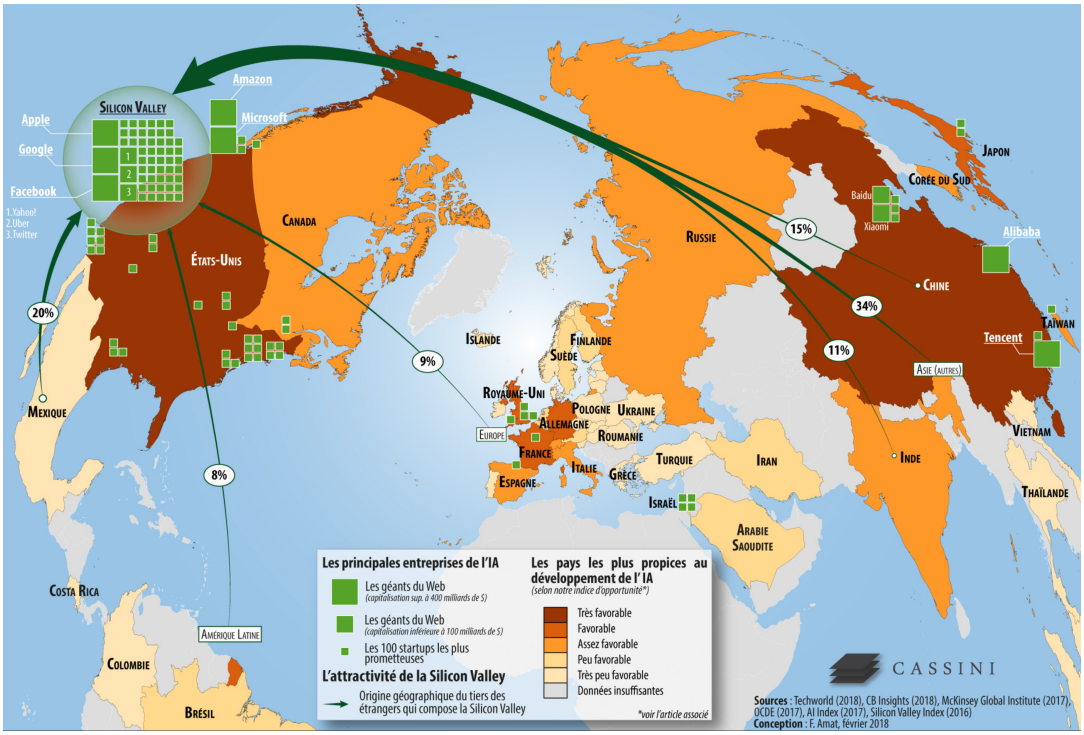


FIGURE 7.10 – Chances des pays dans la course à l'intelligence artificielle
source : Florent Amat et Cassini Conseil – 2018

7.3 Les cyber-armées

Cette dernière partie est la plus délicates car les informations sur les cyber-armées sont bien sûr protégées. Aussi on peut extrapoler des déclarations, des budgets demandés, des analyses faites par les autres pays. On peut ainsi connaître l'existence de cyber-forces mais il est difficile d'en connaitre les détails.

7.3.1 Les États-Unis

Sans surprise les États-Unis sont considérés comme la cyber-force la plus importante. Non seulement ils ont créé Internet et ils en contrôlent une bonne partie, mais aussi ils ont la plus grande armée conventionnelle. Les États-Unis ont dépensé 650 G$ en 2018 pour leur armée contre 250 G$ pour la Chine, 64 G$ pour la France et 61 G$ pour la Russie.

Il est difficile de connaître le budget dédié à la cyber-guerre tant par les aspects secrets des budgets dédiés au renseignement que par la dispersion de la cyber-arme US. Si le commandement, le USCYBERCOM, est un des 10 centre de commandement unifié des États-Unis, ses unités [16] sont en partie intégrées aux autres armes comme le montre l'organigramme figure 7.11. Son budget personnel n'est que de 600 M$ en 2019 à comparer au 190 G$ de chacune des trois armes principales, l'armée de terre, la marine et l'aviation.

Figure 7.11 – Organigramme de la cyber-armée des États-Unis – 2019

Cette dispersion, tout comme la dispersion des unités de renseignement, se comprend dès lors qu'on ne pense pas qu'attaque mais aussi cyber-défense. Pour cela il est important que le cyber intègre tous les niveaux des armées dès lors qu'il y a communication et données numériques, c'est à dire partout aujourd'hui.

16. unités sous double commandement

Si on pense uniquement en capacité d'attaque, il est probable qu'en 2019 la principale cyber-force des États-Unis soit encore la NSA [17].

7.3.2 La Russie

La Russie est probablement le pays qui a utilisé le plus visiblement la cyber-arme en particulier lors d'attaques globales contre d'autres pays [18]. En même temps la Russie mène des cyber-opérations plus discrètes mais pas toujours heureuses comme l'a montré l'arrestation du cyber-commando chargé d'infiltrer le réseau de l'Organisation pour l'interdiction des armes chimiques (OIAC) à La Haye.

Une spécificité supposée de la Russie est d'avoir utilisé à plusieurs reprises des groupes de pirates autonomes pour mener ses cyber-attaques. Outre le gain économique d'utiliser des mercenaires, cela a permis aussi au gouvernement russe de jouer les innocents. Dans le monde cyber où il n'est pas simple de savoir qui fait quoi, passer par des organismes indépendants sans laisser de trace complique la tâche de la victime pour dénoncer l'agresseur. Il est aussi possible que le gouvernement russe manquait de moyen pour lancer des cyber-attaques en 2007 et 2008.

Il est probable que la Russie continue d'utiliser des cyber-mercenaires mais elle a aussi développer des cyber-forces en interne. Le FSB, le successeur du KGB [19], semble avoir été la première force a intégrer l'arme cyber. Si le FSB est chargé principalement des affaires intérieures, il inclut également le Service fédéral des communications et informations gouvernementales (FAPSI), impliqué dans la surveillance électronique à l'étranger. D'autre part la notion d'intérieur est assez souple pour intégrer les anciens membres de l'URSS. Enfin notons que le FSB semble aussi chargé de la guerre de l'information, domaine que les russes intègrent dans la cyber-guerre [20].

La seconde composante de la cyber-guerre russe est le GRU, service d'espionnage de l'armée. Après la guerre de Géorgie en 2018, l'armée a décider de coupler la guerre de l'information avec la guerre physique.

> *Net wars have always been an internal peculiarity of the Internet—and were of no interest to anyone in real life. The five-day war showed that the Net is a front just like the traditional media, and a front that is much faster to respond and much larger in scale. August 2008 was the starting point of the virtual reality of conflicts and the moment of recognition of the need to wage war in the information field too.*
>
> Sharov et Shevyakov [21]– 2009

De ce point de vue l'annexion de la Crimée en 2014 a été un véritable succès pour les russes. Le GRU a su utiliser les réseaux pour promouvoir leurs discours et faire de sorte qu'ils soient acceptés par la plus grande partie possible en y intégrant les contextes culturels nécessaires pour chaque groupe visé. Le vote qui a suivi sur le rattachement de la Crimée à la Russie a montré le

17. cf chapitre sur la démocratie pour la présentation de la NSA
18. L'Estonie, la Géorgie et l'Ukraine pour les plus grands.
19. avec le SVR et SFO, cf figure 7.12
20. cf Russia's Approach to Cyber Warfare – 2106 – https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf
21. cités dans le livre "Inside Cyber Warfares" de Jeffrey Carr

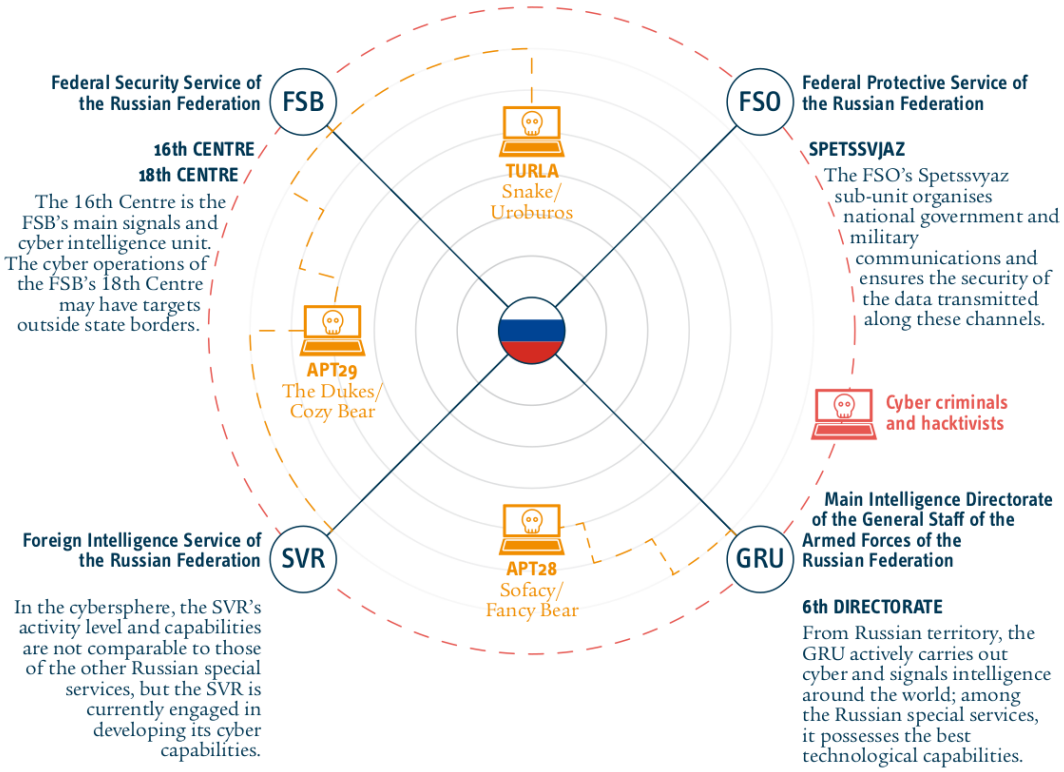


Figure 7.12 – Organisation des cyber-forces russes
source : Estonian Foreign Intelligence Service – 2018

succès de la propagande russe (ou sa capacité de défense sur le terrain des idées suivant le camps où on se trouve).

Mais le GRU ne fait pas que de la guerre de l'information. Il agit aussi à l'étranger dans une cyber-guerre à l'occidentale avec des piratages de réseaux. Ainsi il est reproché au GRU d'avoir piraté les données du parti démocrate pour les faire fuiter lors de l'élection présidentielle américaine de 2016. En 2018, le Royaume-Uni a accusé le GRU d'avoir mener de nombreuses cyber-attaques à travers le monde, y compris en Russie, et croit voire une volonté d'ébranler la stabilité mondiale [22]. Le GRU est aussi montré du doigt pour le piratage de nombreuses organisations internationales en particulier dans le domaine sportif.

Toute cette suractivité déplait aux occidentaux.

> *La Russie doit cesser son comportement irresponsable, incluant l'usage de la force contre ses voisins, des tentatives d'immixtion dans des processus électoraux et des campagnes massives de désinformation.*
>
> Déclaration du chef de l'OTAN dans un communiqué de 2018

22. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

7.3.3 La France

Comme tous les pays occidentaux, la France développe des forces cyber tant au niveau civil que militaire depuis les années 2000. Bien sûr il s'agissait de cyber-défense puisque la doctrine militaire de la France est basée sur la défense [23]. Ainsi l'ANSSI a pris la suite de la DCSSI en 2009 pour protéger les réseaux informatiques civils

En 2017 l'armée a intégré le cyber au plus haut niveau en créeant le Commandement de la cyberdéfense, COMCYBER, placé directement sous les ordres de l'état-major des armées.

Cepeandant en 2018 la France a affiché sa volonté d'agir aussi de façon offensive dans le cyberespace à traver sa nouvelle doctrine. Elle acte le fait que le cyber est une arme à part entière et s'autorise le droit de l'utiliser aussi pour attaquer tant dans le cadre d'opérations militaires que pour répondre à les offensives cybers [24].

Dans le cadre d'opérations militaires le but offensif est d'obtenir du renseignement, de perturber le bon fonctionnement du matériel adverse ainsi que de l'induire en erreur.

Aujourd'hui les cyber-forces françaises s'articulent donc autour de l'ANSSI pour le civil et du COMCYBER pour le militaire. Plus secrètement les services de renseignement, la DGSE pour l'extérieur et la DGSI pour l'intérieur, ont développés leurs capacités cyber. La direction technique de la DGSE est l'équivalent français de la NSA.

L'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Cela comprendre la protection des réseaux informatique des administrations mais aussi d'apporter son expertise aux entreprises et au particuliers. Dans ce cadre l'ANSSI a aussi une mission pédagogique.

Pour mener à bien ses missions elle dispose, en plus de ses ressources propres, d'une autorité sur les entreprises stratégiques. Elle peut imposer aux opérateurs d'importance vitale des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques. De plus ces entreprises ont obligations de tenir l'ANSSI informée des incidents constatés sur leurs systèmes informatiques.

L'ANSSI résume sa mission en quatre points :

- faire de la France une des première puissance mondiale de cyberdéfense ;
- garantir la liberté de décision de la France ;
- renforcer la cybersécurité des infrastructures vitales nationales ;
- assurer la sécurité dans le cyberespace.

L'ANSSI est rattaché au secrétariat général de la défense et de la sécurité nationale sous l'autorité du premier ministre. En 2018 son effectif était de 600 personnes et son budget de 100 M€.

23. cf Le livre blanc sur la Défense et sécurité nationale de 2013
24. cf https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-de-florence-parly/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive

Le COMCYBER

Le commandement des forces de cyberdéfense des armées françaises, COMCYBER, est l'unité opérationnelle commandant, de façon organique ou fonctionnelle, l'ensemble des forces de cyberdéfense des armées françaises. Placé sous l'autorité directe du chef d'état-major des armées, le COMCYBER est responsable de la manœuvre cyber globale.

Créé en 2017, le COMCYBER exerce une tutelle opérationnelle sur près de 3 400 cyber-combattants au sein du ministère en 2019 [25].

Pour l'exercice de ses missions, le COMCYBER dispose d'un état-major et a une autorité sur trois organismes interarmées :

- **CALID** Centre d'analyse en lutte informatique défensive
  Crée en 2006, basé à Paris & Rennes
- **CASSI** Centre d'audits de la sécurité des systèmes d'information
  Crée en 2008, basé à : Maisons-Laffitte, Brest, Orléans, Toulon & Rennes.
- **CRPOC** Centre de la réserve et de la préparation opérationnelle de cyberdéfense
  Crée en 2015, basé à Rennes, il gère 4400 réservistes

7.3.4 La Chine

Durant les années 80 les dirigeants chinois ne connaissaient pas Internet au point d'avoir coupé toutes les communications vers l'extérieur durant les événements de Tiananmen en 1989, toutes sauf Internet ce qui a permis aux quelques étudiants ayant Internet d'informer le monde. Depuis les choses ont bien changé et la Chine a su développer son Internet pour devenir la pays ayant le plus d'internautes et possédant des entreprises majeures dans le domaine. À l'extérieur elle a su aussi pleinement utiliser Internet, aux point de se faire une grande réputation de cyber-voleuse de secrets industrielles auprès des occidentaux.

Aujourd'hui la Chine est une puissance majeure du cyber-espace. Elle contrôle parfaitement de qui se passe dans l'Internet chinois et dispose d'une frontière bien gardée. À l'étranger son arme principale réside dans ses appareils qui inonde le monde en particulier ses ordiphones Huwai, Oppo et Xiaomi.

Du point de vue militaire, la Chine a réorganisé son armée en 2015 pour établir la Force Stratégique de Support (战略支援部队) au plus haut niveau de l'organigramme, voir figure 7.13. Cette force opère suivant trois axes : le spatial, le cyber-espace et le domaine de l'électromagnétique. Son département des systèmes réseaux (网络系统部) est en charge de la guerre cyber, électronique et psychologique (dans la veine de la guerre de l'information). Comme pour les armées des autres pays, des cyber-forces se retrouvent aussi dans les armées de terre, air et mer.

25. source : https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation

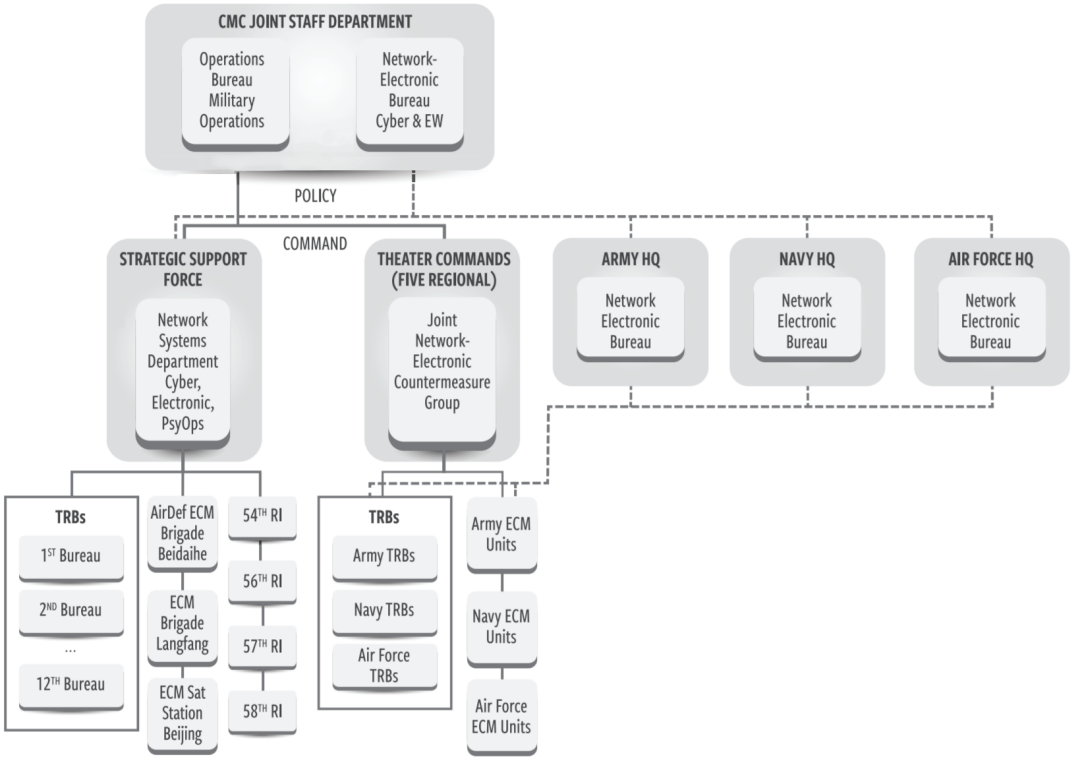


FIGURE 7.13 – Organigramme de la cyber-armée de la Chine – 2017
source : Elsa B. Kania et John K. Costello – 2017

La raison d'être des cyber-forces chinoises est clairement de participer pleinement à un guerre conventionnelle, avec les missions de reconnaissance et de cyber-attaques usuelles. Cependant, pour les chinois comme pour les russes et probablement comme pour les occidentaux de plus en plus, le cyber-espace est un espace-temps différent de l'espace physique :

> *Le jeu stratégique dans le cyber-espace n'est pas limité dans l'espace ou dans le temps, il ne fait pas la différence entre la paix et la guerre, [et] n'a pas de ligne de front et de bases.*
>
> Ye Zheng, Stratège de l'armée chinoise – 2013

Plus

- Les publications du CCDCOE de l'OTAN, https://ccdcoe.org/library/publications/
- La revue de cyber-défense de West Point, https://cyberdefensereview.army.mil/