État des lieux des risques et menaces cyber

Laurent Prosperi

prenom.nom@ens-paris-saclay.fr

17 octobre 2020

« La menace d'origine cyber ne cesse de croître dans ses formes et dans son intensité » [1] avec le passage à une échelle mondiale en 2017 suite aux deux vagues de rançongiciels Wannacry et NotPetya. Les acteurs, étatiques ou non, se multiplient et montent en compétence. Leurs attaques visent des cibles toujours plus critiques et peuvent entrainer des effets létaux. Le coût pour la société de cyberattaques est en croissance rapide. Il est passé de 0.62% du PIB mondial en 2014 (soit 445 milliards de dollars) à 0.80% en 2017 [2] (soit plus de 600 milliards de dollars). Aussi il nécessaire de procéder à un état des lieux des risques et menaces pour affiner la compréhension domaine cyber. Cela nous amène à cartographier les vulnérabilités de la société et de l'État avant de plonger dans une rétrospective de la construction de la menace cyber, de faire émerger les tendances en actuelles et de dessiner les concours des évolutions probables.

1 Évaluation des vulnérabilités

Pour le SGDSN, « l'état sécuritaire est insuffisant » [3] au sein de la société française, exception faite des opérateurs d'importance vitale OIV, de l'armée et des administrations spécialisées. Cet état résulte de l'ensemble de la chaîne, du développement de logiciels jusqu'à la prise en compte de la menace par les différents acteurs en passant par le maintien en condition de sécurité, couplé à des vulnérabilités croissantes (numérisation de la société, des armées, de l'État, inter-connectivité

1. SGDSN. *Revue stratégique de cyberdéfense*. 2018.
2. James Andrew Lewis. *Economic Impact of Cybercrime—No Slowing Down Report*. CSIS - Center for strategic & International studies, février 2018, p. 28.
3. SGDSN, op. cit., p. 27.

et interdépendance croissante entre les aires géographiques et les systèmes). Les entreprises comme les administrations ne disposent que rarement de systèmes d'information robustes, sécurisés à l'état de l'art et maintenus en condition de sécurité tout au long de leur cycle de vie. Il faut compter un délai moyen de près de six mois pour que 90% des appareils touchés soient mis à jour après la publication d'un correctif [4]. L'industrie est séparée en deux groupes, celui rassemblant les acteurs du numérique, de la finance, de l'assurance où le délai est de 10 jours pour atteindre 90% de couverture et celui des médias et de la santé où il faut près de 500 jours pour atteindre le même niveau. La situation est pire du côté des systèmes, le temps médian est de huit semaines et il faut compter près de dix mois pour atteindre les 90%. Les secteurs industriels sont partitionnés de la même manière, même le meilleur groupe ne peut être considéré comme un bon élève. De plus, la prise en compte et la compréhension de la menace sont insuffisantes du fait d'une grande faiblesse de l'hygiène numérique [5]. La prise de conscience se fait lentement, au fur et à mesure des incidents, la gouvernance n'est pas assez sensibilisée, ce qui entraine une faible légitimité des services de sécurité informatique pour agir en prévention et un manque de ressources engagées. En effet, les ressources allouées sont faibles comparativement aux dégâts provoqués, les cyberattaques ont coûté près de 6000 milliards de dollars à l'échelle mondiale en 2018 pour seulement 1000 milliards investis dans la sécurité [6]. A l'aspect financier s'ajoute une pénurie de moyens humain [7], en particulier pour irriguer les collectivités locales, les administrations et les TPE/PME non spécialisées dans le cyber, pénurie due à une forte tension sur les effectifs en raison de la concurrence avec les grands groupes étrangers et des faibles perspectives de carrière au sein de ces entités [8]. Malgré une lente prise de conscience, l'état sécuritaire se dégrade avec une transition numérique non maitrisée et l'arrivée massive des objets connectés qui combinent une faible prise en compte de la menace avec une expansion importante et un morcèlement de la surface d'attaque en fractions détenues par des acteurs différents.

Les vulnérabilités des systèmes cyber peuvent être classifiées selon trois axes [9] :

4. L. Bilge. « Invited Keynote : Is Proactive Security even Possible ? » In : *13th European workshop on Systems Security*. 2020.

5. Les collaborateurs sont les premières portes d'entrée des attaques subies

6. SGDSN, op. cit.

7. *Entretien réalisé le 16/06/2020 avec avec un reponsable du comité stratégique de filière industries de sécurité.*

8. SGDSN, op. cit., p. 133.

9. S. Taillat. « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33, p.28.

1) les couches du cyberespace dans lesquelles elles résident, 2) le degré d'ouverture du système 3) les logiques géopolitiques à l'œuvre. Les vulnérabilités liées aux hardwares (ou au cœur de réseaux) sont souvent difficilement détectables et difficilement exploitables mais peuvent compromettre une grande gamme de systèmes et nécessitent des moyens importants pour les réduire (et une temporalité longue, jusqu'au changement du matériel). Les vulnérabilités logicielles sont à la fois les plus faciles à exploiter (par exemple avec des outils achetés sur étagère) et à corriger. Enfin, l'ingénierie sociale (ou plus rarement un action volontaire) permet le plus souvent d'introduire la charge utile directement à l'intérieur du réseau de l'entité visée. Ensuite vient le degré d'ouverture qui mesure le niveau d'interaction d'un système d'information avec l'environnent numérique extérieur. Par exemple si le système est connecté ou non à Internet, si la séparation est physique ou logique et aussi en fonction des mesures de sécurité physique (type contrôle d'accès) mises en place. Enfin, à l'échelle d'un État ou d'un géant du numérique, le contexte géopolitique entre en jeu notamment du fait de la dépendance ou non à certains câbles océaniques (et au pays de transit de ceux-ci), à la position des datacenters.

1.1 Comment les prévenir ?

Une meilleure résilience des systèmes passe, dans un premier temps, par une adaptation organisationnelle de l'entité [10] et par une intégration du cyber dans la Direction pour accroitre la légitimité de la personne en charge. Une meilleure connaissance de la technologie actuelle, des modes opératoires et des attaques en cours permet de s'adapter aux nouvelles vagues d'attaques. Pour ce faire, il est nécessaire de mettre en place une veille active, un développement de bases de données de signatures afin d'améliorer et automatiser la détection. Éventuellement, la mise sur pied d'un centre de veille permanent permet d'anticiper en temps réel les attaques non ciblées qui se propagent en fonction des fuseaux horaires [11]. Troisièmement, il est nécessaire de monter en puissance techniquement pour assurer la sécurité tout au long de la durée de vie d'un système, ce qui inclut une intégration des questions de sécurité dès la conception et une phase de vérification conditionnant la mise en service. Ensuite, le maintien en condition de sécurité et la détection des attaques doivent être assurés pendant l'exploitation du système. A cela, il faut ajouter les

10. SGDSN, op. cit.

11. Intervention de Nathalie Mombelli le 16 octobre 2019 lors du séminaire Géopolitique du risque : technologies et responsabilité organisé par J. Peter Burgess et Sarah Perret dans le cadre de la Chaire Géopolitique du risque de l'ENS.

capacités de réaction aux attaques. Enfin, les entités ayant des moyens techniques suffisants [12] mettent en place des moyens de défense active soit en plaçant des "pots de miel" pour attirer les assaillants vers une cible fictive soit en étudiant in situ une attaque avant d'y répondre [13]. Enfin, une culture du "hack-back", c'est à dire une riposte cyber, se développe au sein des entreprises étrangères. En France, c'est une méthode proscrite pour les organisations privées [14].

2 Construction de la menace

Les premiers cas d'agression cyber remontent aux années 1980 [15] (Cuckoo's egg en 1986, Morris Worm en 1988). Des attaques plus évoluées commencent à voir le jour dans les années 1990 : la première attaque par déni de service a lieu en 1995 et le département américain de la défense a subi sa premier agression d'origine cyber en 1998. Cependant, les cyberattaques sont restées l'affaire de quelques spécialistes (les plus connus étant allemands, américains, ou russes) jusqu'à la fin de la décennie. Les années 2000, ou phase de maturation, voient émerger une structuration de la menace en groupes de plus en plus organisés pour donner naissance dans les années 2010 [16] à la notion d'Advance Persistent Threat (APT), c'est à dire de menaces persistantes souvent mises en œuvre par des groupes structurés utilisant un ensemble de techniques et outils de hauts niveaux.

Nombre d'APT servent de proxies à des États. En effet, ceux-ci sont de plus en plus impliqués dans la déstabilisation du cyberespace (plus de 28 États sont suspectés de mener ou de commanditer des actions cyber [17]) directement ou à travers des proxies (APT, groupes cybercriminels, activistes). La multiplication des acteurs et des nationalités entraine une dilution de la notion de souveraineté et de frontière [18] d'autant plus qu'il n'y a pas de gouvernance ni de régulation internationale du

12. En France, principalement l'ANSSI, le COMCYBER, les services de renseignement et les entreprises de cybersécurité.

13. Cette dernière méthode est controversée car elle est souvent mise en place sans que les utilisateurs du système concerné ne soit avertis.

14. SGDSN, op. cit., p. 35.

15. O. Kempf. « Du cyber et de la guerre ». In : *Fondation pour la recherche stratégique* (Note n°17/2019 12 septembre 2019), p. 3.

16. SGDSN, op. cit.

17. *Cyber Operations Tracker*. Council on Foreign Relations. URL : `https://www.cfr.org/interactive/cyber-operations` (visité le 09/12/2019).

18. Taillat, op. cit. ; A. Cattaruzza. « Chapitre 1. La construction politique de l'espace numérique. Penser l'espace numérique comme un espace stratégique ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 19-25, p. 32, 83.

cyberespace. Par ailleurs, la puissance étatique est battue en brèche par le secteur privé en terme de capacités techniques, de ressources mais aussi par les positions prises dans la construction de la gouvernance et de la régulation internationale du cyberespace.

Par ailleurs, notons que les attaques cyber ne cadrent, jusqu'à présent, que partiellement avec les critères de la violence des conflits armés. Les conséquences physiques, létales ou non, contre les individus sont encore indirects, résultant souvent d'effet de bord. Cette situation évolue rapidement car les menaces contre les systèmes de sécurité et de santé (cryptovirus ayant entrainé la paralysie du NHS en 2017) sont en expansion. Les logiques sous-jacentes sont incertaines, les objets difficiles à définir et une certaine retenue de la part des états peut être constatée [19].

3 Phase de prolifération ou complexification de la menace

Plus généralement, les menaces se complexifient par le passage d'une échelle locale à une échelle régionale voire mondiale (propagation due à l'échelle mondiale des acteurs ou à l'interconnexion des réseaux et systèmes), par une polyvalence et une réversibilité accrues des outils qui peuvent être utilisés à la fois pour défendre et pour attaquer. Un marché noir de services offensifs sur le *darkweb* permet à un commanditaire de sous-traiter une attaque à un individu ou à un groupe. L'utilisation de ces services ne nécessite pas de compétences techniques élevées du donneur d'ordre, facilitant ainsi les attaques et complexifiant d'autant plus l'attribution. L'incertitude est accrue par une recrudescence d'attaques à objectifs multiples, comme par exemple l'utilisation d'un ransomware effectuant aussi de l'exfiltration de données, et par le détournement de cyberarmements développés par d'autres à l'image du vol en 2015 des outils de l'APT Equation Group, une probable émanation de la NSA.

Pour Julien Nocetti, les menaces cyber sont rentrées dans une phase de « prolifération » [20] comme avec l'attaque massive par le botnet Mirai de la société Dyn (fournissant un service DNS) en octobre 2016, vue comme l'un des tests successifs ciblant l'architecture physique d'Internet avec une utilisation à une échelle encore jamais atteinte d'objets connectés. Au printemps 2017, le rançongiciel Wannacry infecte près 300 000 ordinateurs dans 150 pays, dans la foulée un autre malware se

19. Taillat, op. cit., p. 27.

20. J. Nocetti. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27, p.18.

propage, initialement appelé Petya puis rebaptisé NotPetya car il agissait en surface comme un rançongiciel en chiffrant les données mais n'était pas destiné à collecter des rançons mais à détruire. Cette thèse est corroborée par plusieurs sources : l'expert en sécurité connu sous le pseudonyme de « the grugq », les sociétés de cybersécurité ComaeTechnologies et Kasperky [21]. En février 2018, les Five Eyes attribuent NotPetya à la Russie, dans une volonté de frapper l'Ukraine. La transition des rançongiciels à des programmes purement destructeurs est un glissement « du cybercrime vers l'arme cyber » [22] mais aussi un changement de finalité en passant d'un but financier à un but politique. Il est intéressant de remarquer que Janus, le créateur de Petya, s'est dissocié de NotPetya via Twitter et, plus généralement, les hackers connus ou suspectés d'avoir participé à la conception de ce type de malwares ont fait de même. NotPetya n'est pas pour autant le premier du genre à effectuer un tel glissement mais c'est celui qui a frappé le plus durement les pays occidentaux. Déjà en 2012 Shamoon, probablement d'origine iranienne, a perturbé l'industrie pétrolière saoudienne (notamment Aramco, les estimations parlent de 35 000 ordinateurs infectés) et dans une moindre mesure celle du Qatar.

Durant l'exercice 2018, l'ANSSI a été amenée à traiter 78 attaques informatiques ayant touché des ministères français [23]. 31 se sont révélées mineures au sens où un engagement minimal a été requis pour leur traitement, 32 ont demandé l'emploi d'expertises particulières, alors que 15 se sont avérées majeures, nécessitant l'engagement de moyens à long terme de la part de l'ANSSI, trois d'entre elles ont fait l'objet d'une opération de cyberdéfense. L'ANSSI a dû dépêcher des équipes sur place pour faire cesser l'attaque et reconstruire les réseaux. Les ministères les plus attaqués, en terme de volume, sont dans l'ordre l'éducation nationale, la défense et les affaires étrangères. En intensité, les ministères des armées et des affaires étrangères [24] ont été les plus touchés.

Les rançongiciels représentent actuellement l'une des menaces principales pour les entreprises et institutions par le nombre d'attaques quotidiennes et par leur impact potentiel sur la continuité d'activité. L'ANSSI a traité 69 incidents [25] en 2019

21. *L'officier au service de la Nation dans le monde du XXI e siècle.* LesCahiersdelaRevueDéfenseNationale. 2018, p. 72, p. 59.

22. Ibid.

23. O. CADIC et R. MAZUIR. *Projet de loi de finances pour 2020. Direction de l'action du gouvernement :coordination du travail gouvernemental : SGDSN, ANSSI, cyberdefense, INHESJ, IHEDN.* Note de synthèse N° 46 (2019-2020). Sénat, novembre 2019.

24. Ibid.

25. Les collectivités territoriales et le secteur de la santé étant les plus touchés. Cette surreprésentation peut être expliquée par un biais dans la sur-représentation des signalement faits à l'ANSSI dans ses secteurs ou cela peut montrer l'intérêt des attaquants pour des entités réputées

sur son périmètre [26] soit presque autant d'incidents que pour l'année 2018 tous types confondus. Depuis la fin 2019, certains groupes d'attaquants s'emploient à exfiltrer de grandes quantités de données présentes sur le système d'information compromis avant le chiffrement de celles-ci afin d'exercer une pression supplémentaire sur les victimes. Ce fut notamment le cas, en mai 2019, lorsque les opérateurs du rançongiciel RobbinHood ont divulgué des documents appartenant à la ville de Baltimore, alors compromise par ce rançongiciel. Cette menace sur la confidentialité des données peut avoir des implications légales, notamment en Europe dans le cadre du RGPD, qui entraine à minima l'obligation d'informer la CNIL ainsi que les utilisateurs ou clients concernés par le vol de leurs données.

La complexité du cyberespace, comme des menaces, est à l'origine de l'émergence de risques systémiques [27] pouvant prendre racine dans des dommages collatéraux non maitrisés à très large échelle ou dans un emballement entre attaques et ripostes facilité par de possibles attributions erronées. Cet aspect systémique peut se concrétiser par des phénomènes imprévisibles de grande ampleur comme des coupures d'électricité à l'échelle d'un pays voire à une échelle régionale du fait de l'interconnexion des réseaux et de la dépendance au cyber. Ces risques sont renforcés par des interactions cyber-physiques toujours plus fortes (pacemaker connecté, voiture connectée, gestion intelligente de l'énergie) qui tendent à augmenter la létalité potentielle des futures attaques. L'archétype en est la "révolution" des objets connectés entrainant une multiplication du nombre d'appareils, faiblement sécurisés pour l'instant, et contrôlant une part croissante de l'activité humaine.

3.1 Menace contre les systèmes industriels

Depuis les années 2000, les entreprises industrielles ont entrepris une migration vers des systèmes Ethernet et TCP/IP, et plus récemment vers ce qu'on appelle l'industrie 4.0, tout en ne prenant pas suffisamment en compte les problématiques de cybersécurité [28]. Initialement, les installations étaient déconnectées d'Internet et la technologie de niche souvent propriétaire et peu connue des hackers. Aujourd'hui, la technologie s'uniformise, les systèmes industriels sont reliés aux systèmes d'information et mis en réseaux. En 2010, est dévoilé Olympic Games, la première attaque

faiblement défendues ou qui ne peuvent se permettre une rupture d'activité.

26. ANSSI. *Etat de la menace rançongiciel à l'encontre des entreprises et des institutions.* 5 février 2020, p. 3.

27. SGDSN, op. cit., p. 28.

28. Yugo Neumorni. « La 'taupe' venue du réseau électrique ». In : *Observatoire FIC* (24 juillet 2019). (Visité le 13/04/2020).

d'ampleur contre des systèmes industriels. Cette opération, menée en collaboration par les États-Unis et Israël, visait à ralentir le programme nucléaire iranien à l'aide du virus Stuxnet afin d'endommager les centrifugeuses. La charge utile a été introduite directement par une clé USB et elle a exploité un certain nombre de failles des systèmes SCADA. Cette opération marque le glas de l'immunité des systèmes industriels. L'année 2015 fut témoin de la réussite de la première cyberattaque ayant permis de déconnecter une partie d'un réseau électrique (en Ukraine) depuis l'étranger. La porte d'entrée de l'attaque a été le réseau d'entreprise, compromis par des attaques classiques à base phishing et d'exploitation de vulnérabilités non protégées de la suite Microsoft Office. Puis, la latéralisation a été possible grâce au vol des moyens d'authentification nécessaires et à la convergence TCP/IP entre réseaux d'entreprise et industriels. Enfin, l'exploitation s'est faite par la prise de contrôle de convertisseurs Série/Ethernet, chainons critiques pour la sécurité, utilisés dans la plupart des systèmes critiques et souvent faiblement durcis car n'étant souvent pas conçus pour être exposés sur un réseau public. Ces dernières années, le Department of Homeland Security des États-Unis [29] dénonce l'infiltration de postes de contrôle de centrales électriques sur le sol américain. En 2016, le directeur de la NSA a soulevé le problème du prépositionnement de cyberarmes adverses dans les réseaux de distribution d'électricité, d'eau et de gaz. En 2019, les Américains ont annoncé s'être infiltrés dans le réseau de distribution d'électricité de la Russie afin d'y prépositionner des charges permettant de répondre aux cyberattaques russes.

3.2 Les infrastructures critiques en première ligne

Les infrastructures critiques sont devenues des cibles de choix. Dans le secteur de l'énergie, des attaques ont ciblés Aramco [30] en 2012 et 2017. Les réseaux électriques sont régulièrement attaqués [31], le 5 janvier 2003, le virus Slammer infecte la centrale nucléaire Davis-Besse dans l'Ohio par une connexion entrante passant à travers le pare-feu de la centrale. Les deux systèmes « Safety Parameter Display System » (le système d'affichage des paramètres de sécurité) et « Plant process computer » (l'ordinateur industriel gérant une partie des processus de la centrale) sont désactivés pendant plusieurs heures. La centrale étant à l'arrêt, la sécurité des populations

29. Ibid.

30. Saudi Aramco est la compagnie nationale saoudienne d'hydrocarbures

31. A. PALLE. *Vulnérabilité et protection des réseaux électriques : Approches comparées Union européenne - Etats-Unis*. Note de recherche 62. IRSEM, 28 septembre 2018, p. 18. (Visité le 16/04/2020).

n'a pas été compromise. L'année 2012 est témoin de la première cyberattaque de près de cinq jours contre un opérateur de réseau européen, 50Hertz (gestionnaire de réseau allemand). Celle-ci est sans gravité pour la stabilité du réseau et la sécurité d'approvisionnement. Suite à la révolution orange, l'Ukraine devient un terrain d'expérimentation cyber. Le 23 décembre 2015 près de 70 000 foyers sont privés d'électricité par l'emploi du malware BlackEnergy contre des centrales électriques. Le secteur financier est largement ciblé pour l'appât du gain ou de données personnelles [32], notamment avec l'attaque emblématique contre JP Morgan en 2014 qui s'est soldée par un vol de données massif de près de 83 millions de comptes [33] représentant près de 7 millions de commerces ainsi que les deux tiers des ménages américains clients de la banque. Plus récemment ce sont les plateformes gérant les cryptomonnaies qui sont ciblées. Les médias ne sont pas non plus en reste, dans le cas français l'affaire de TV5 Monde a défrayé la chronique en 2015, M6 a aussi été frappée dans une moindre mesure en 2019 [34]. Les systèmes de santé sont régulièrement la cible de rançongiciel, le NHS britannique a été très fortement perturbé par la vague WannaCry et NotPetya. En novembre 2019, le CHU de Rouen a été fortement secoué par une attaque qui a nécessité l'intervention de l'ANSSI [35].

La politique énergétique [36] de l'Union Européenne tend à favoriser l'apparition de risques systémiques dans le domaine de l'approvisionnement électrique par l'interconnexion des différents réseaux nationaux. Le traité de Lisbonne promeut une intégration des réseaux d'énergie pour faire émerger un grand marché commun et pour réaliser des économies d'échelle. Le dernier grand black-out européen, en 2006, a pour origine un incident sur une ligne allemande et a touché 15 millions de consommateurs dans 12 pays de l'Union et du voisinage proche. L'ouverture des réseaux au numérique, dans le cadre de la transition énergétique et de la modernisation des infrastructures, tend à renforcer la vulnérabilité du secteur de l'énergie au profit d'une recherche de l'efficience des systèmes en adaptant le réseau en temps réel. Cette politique entraîne par exemple la connexion de certaines infrastructures à Internet, démultipliant ainsi la surface d'attaque des systèmes. En Europe, la gestion des risques cyber et physiques est traitée de manière séparée tandis qu'elle est intégrée

32. Nocetti, op. cit., p. 19 note 12.
33. T. S. Bernard. « Ways to Protect Yourself After the JPMorgan Hacking ». In : *The New York Times* (3 octobre 2014). (Visité le 21/05/2020).
34. M. Untersinger. « Une attaque informatique perturbe le fonctionnement du groupe M6 ». In : (octobre 2019).
35. « Après la cyberattaque au CHU de Rouen, l'enquête s'oriente vers la piste crapuleuse ». In : *Le Monde* (26 novembre 2019).
36. PALLE, op. cit.

dans un même plan de réponse aux États-Unis, ce qui facilite la réponse.

« A l'avenir le plus à redouter » [37] ce sont les actions de sabotage contre les systèmes de sécurité (communication, transport, énergie) de par leur létalité directe. Aujourd'hui, un petit nombre d'États est en mesure de mener de telles actions mais ce nombre est appelé à croître et à se diversifier en incluant des acteurs non étatiques. Certaines attaques ont montré qu'il était possible d'entraver des investigations judiciaires (cas de la compromission des laboratoires Eurofins Scientific) et des postes de police. « Il est tout à fait envisageable dans le futur que des groupes cybercriminels (ou le crime organisé en général) puissent s'appuyer sur ce moyen afin de faire pression sur la justice. » [38] En outre, la surface d'attaque des système de défense est en croissance rapide [39], les transformant eux-mêmes en cible de choix pour des assaillants qualifiés. Leur complexité s'est accrue du fait de l'extension de leur capacité de détection des événement non connus (pour sortir de la dépendance aux bases de signature et pour réduire le temps de détection). Une boucle de détection classique s'appuie sur deux systèmes de détection : l'un par base de signatures traitant des menaces connues, l'autre collectant des traces (réseaux notamment) et utilisant des outils d'apprentissage statistique en temps réel [40] afin de faire de la corrélation de fait et de la détection d'anomalie en temps réel. Les incidents et anomalies détectés sont transmis à un humain expert chargé de faire la part des choses avec les faux positifs. Les nouvelles menaces sont alors ajoutées à la base de signatures et le cycle se poursuit. De nombreuses attaques ont vu le jour pour empoisonner les modèles d'apprentissage ou pour passer outre leur capacité de généralisation.

3.3 Menace contre l'infrastructure d'Internet

Au niveau national, les réseaux de télécommunication sont devenus l'une des clés de voûte de nos sociétés, s'ils sont perturbés ou mis hors service, les secteurs critiques que sont la santé, l'énergie, les transports seront fortement impactés sans compter les sinistres économiques et sociaux. Seuls quelques services s'appuyant sur des réseaux PMR ou sur des réseaux dédiés devraient pouvoir continuer à fonctionner [41]. Au

37. L. Gautier. « Cyber : les enjeux pour la défense et la sécurité des Français ». In : *Politique étrangère* Été.2 (2018), p. 29-42, p. 33.

38. ANSSI, op. cit., p. 17.

39. *Entretien avec un architecte réseau d'Orange.*

40. C'est à dire s'appuyant sur des outils faisant partie de la sphère du BigDate et l'IA. Notons que la démocratisation de ces outils n'est pas synonyme d'un personnel qualifié en nombre pour les utiliser.

41. *Entretien avec un architecte réseau d'Orange.*

niveau international, l'infrastructure d'Internet, bien que décentralisée, joue le rôle des réseaux de télécommunication nationaux. Elle sert à interconnecter les différents sous-réseaux entre eux. Nous allons étudier les menaces pesant sur deux points critiques à deux niveaux, ce lui de l'infrastructure d'interconnexion international (câbles sous-marins et continentaux) et celui de l'infrastructure logique permettant son utilisation (le routage).

Un rapport détaillé publié par le centre de réflexion britannique Policy Exchange en 2017 [42] montre la dépendance actuelle aux câbles sous-marins mais aussi leur grande vulnérabilité, que ce soit en mer ou sur la terre ferme, contre des attaques provenant d'États voire d'organisations non étatiques. L'infrastructure sous marine est vitale à notre société numérique, 97% des communications mondiales et l'essentiel des transactions financières (soit près de dix mille milliards de dollars par jour en 2017) y transitent. En 2017, le réseau sous-marin est constitué de près de 213 câbles courant sur près de 900.000 km. La perte d'un câble peut entrainer l'augmentation de latence, et ainsi compromettre certains services fonctionnant en temps réel, voire priver une région d'accès au reste d'Internet et perturber fortement l'ensemble des services régionaux nécessitant des ressources externes (notamment des données stockées dans des datacenters à l'extérieur de la zone concernée). En 2014, la rupture d'un câble sous-marin a réduit de près de 80% le trafic extérieur de l'Algérie [43] entrainant une coupure massive d'Internet pendant près de 48 heures. L'une des particularités de l'infrastructure physique est que les câbles sont posés, détenus et opérés par des opérateurs privés. Ces infrastructures sont souvent négligées par les États et la réglementation internationale (principalement la United Nations Convention onthe Law of the Sea (UNCLOS)) n'est que faiblement protectrice [44] par rapport à la place centrale qu'occupent ces infrastructures aujourd'hui. Par exemple, elle ne donne pas la possibilité de protéger les câbles à terre (en dehors du territoire national), ni d'intercepter les navires suspects et les promulgations nationales ne sont pas forcément cohérentes entre elles.

Les câbles sont des cibles physiques de choix lors d'opérations militaires conven-

42. R. Sunak et J. Stavridis. *Undersea cables : indispensable, insecure*. Policy Exchange, 2017, p.22, rapport ratifié par l'amiral James Stavridis, US Navy (Ret), ancien commandant suprême des Forces alliées en Europe SACEUR, ; par Robert Hannigan, ancien directeur du GCHQ jusqu'en 2017 et par le général Lord Houghton, ancien Chef d'état-major des armées (Royaume-Uni) jusqu'en 2016.

43. C. Morel. « Les câbles sous-marins : un bien commun mondial ? » In : *Études* Mars.3 (2017), p. 19-28, p.14.

44. Sunak et Stavridis, op. cit., Chapitre 2.

tionnelles pour paralyser l'adversaire [45] ou lors de conflits hybrides afin de mettre en place une bulle d'exclusion informationnelle. L'une des premières opérations russes en Crimée fut de couper l'unique câble la reliant au reste du monde. Même sans volonté de nuire, les câbles sont très vulnérables à des dommages physiques accidentels en mer, les Nations Unis estiment que plus d'une centaine de câbles sont endommagés chaque année le plus souvent du fait de la pêche [46]. Ils sont fortement exposés à des opérations de faible envergure à terre car ils sont souvent fortement concentrées et faiblement protégés avec un tracé publiquement connu (et ce pour presque tous les câbles existants) facilitant les actes hostiles d'acteurs non étatiques, par exemple en 2007 Al-Qaïda a projeté d'attaquer le London Internet Exchange (LINX), un Internet Exchange Point (IXP). Les réseaux nationaux sont tous aussi vulnérables, en mai 2020 la destruction à la disqueuse de câbles dans le Val-de-Marne a entrainé des perturbations pour près de 100 000 clients d'Orange [47]. Enfin, des attaques cyber contre les réseaux de contrôle et les IXP pourraient permettre de menacer la connectivité de régions entières (pour les moins bien desservies) ou de fortement perturber les échanges. En mer, la barrière d'entrée pour réaliser des attaques est assez faible (ne nécessitant que des vecteurs et de la technologie facilement accessibles), bien que la sous-marinade soit la plus grande menace.

La menace étatique est croissante. En avril 2017, dans son étude prospective *Chocs futurs*, le SGDSN a souligné que les « câbles sous-marins assurant les communications numériques deviennent par exemple de potentielles cibles dans le jeu des puissances. » Les forces russes comme occidentales développent leurs capacités d'action pour perturber les communications, isoler une zone (comme lors de l'annexion de la Crimée) ou pour poser des bretelles sur les câbles afin de faire du renseignement. La Russie a lancé un développement capacitaire de premier plan pour sa marine à horizon 2030 qui inclut des navires de guerre électronique de classe Yantar et sous-marins auxiliaires pouvant permettre d'opérer contre des câbles sous-marins. Les Américains disposent aussi de capacités d'action pour la collecte de renseignement notamment avec le sous-marin USS Jimmy Carter spécialement conçu pour des opérations clandestines et de renseignements comme l'écoute de câbles sous-marins. Depuis 2015, des opérations « agressives » [48] d'origine russe ont été dénoncées par

45. Déjà en 1914, la Royale Navy a coupé les cinq câbles sous-marin reliant l'Allemagne à l'Amérique.

46. Sunak et Stavridis, op. cit., p.22.

47. « En Ile-de-France, l'accès au réseau téléphonique et Internet d'Orange perturbé par la destruction de câbles en fibre optique ». In : *Le Monde* (6 mai 2020).

48. Sunak et Stavridis, op. cit.

les Américains dans la mer de Norvège ou dans l'océan Atlantique. La place des États-Unis est particulière, la concentration des infrastructures sur leur sol ou entre les mains d'entreprises américaines fait d'eux la plaque tournante des échanges internationaux et favorise ainsi leur capacité d'écoute notamment avec les programmes Upstream et Tempor de la NSA, dévoilés en 2013, ciblant les câbles transitant sur le territoire américain et les points d'échange. Ceci se traduit par un très net avantage américain au niveau logique du "cœur" d'Internet. Les communications reposent sur le principe de la commutation de paquets (ou routage), les données échangées sont découpées en blocs (appelés paquets) disposant de méta données qui permettent à l'infrastructure logique de rediriger le paquet vers sa destination. Internet est composé d'un ensemble de réseaux interconnectés par des routeurs de sortie qui vont orienter les paquets suivant un certain protocole, le plus connu étant Border Gateway Protocol (BGP) permettant un routage décentralisé et initialement "neutre". Si plusieurs routes sont disponibles, la meilleure selon certains critères (notamment de performance) transfèrera les données, ce qui fait que les États-Unis sont l'une des plaques de transit les plus importantes même si les données sont échangées entre deux nations tierces.

Des routes alternatives ont vu le jour notamment à destination de l'Asie. Le Transit Europe-Asia (TEA), inauguré en 2008, permet de connecter l'Europe à la Chine en suivant le tracé du Transibérien et désenclave ainsi la Russie tout en accroissant son poids géopolitique face à l'Union Européenne. Les BRICS [49], en partenariat avec une vingtaine d'états africains, ont même lancé en 2012 le projet de leur propre câble sous-marin de 34 000 km, afin de les interconnecter sans passer par les États-Unis [50] ; le projet a été abandonné en 2014 faute d'accord commun. Dans la foulée de son enterrement, un câble reliant le Brésil à l'Europe a vu le jour. Les révélations d'Edward Snowden en 2013 à-propos des programmes XKeyscore et Prism ont servi de catalyseur à la remise en question de la position dominante des États-Unis.

« Le routage apparait comme un enjeu géopolitique majeur aujourd'hui » [51] et pose la question du routage national, pour que les données issues et à destination d'un même territoire ne sortent pas de celui-ci. Nombre de pays non européens (Malaisie, Australie, Corée du Sud ou encore le Brésil) se sont saisis de l'affaire. En 2014, Deutsche Telekom, en coopération avec d'autres fournisseurs d'accès al-

49. Russie, Chine, Inde, Afrique du Sud, Brésil

50. A. Zyw Melo. « Un câble pour les BRICS : un défi stratégique insurmontable ». In : *Hermès, La Revue* 79.3 (2017), p. 145-149.

51. Cattaruzza, op. cit., p. 37.

lemands, lance l'initiative *Email made in Germany* visant à garantir que les mails envoyés entre deux clients ne traversent pas les frontières nationales ; bien qu'intéressante, la mesure ne vise que les clients de Deutsche Telekom. Les routages nationaux les plus avancés sont ceux de la Chine et de l'Iran, ils s'inscrivent dans les "boucliers numériques" mis en œuvre pour les isoler de l'extérieur (le *Great Firewall* pour la Chine et l'*Internet halal* pour les iraniens). La mise en place d'un routage national n'est pas sans conséquence, cela participe à la territorialisation des données et modifie en profondeur la nature d'Internet qui devient moins décentralisé, moins neutre et plus politisé, à l'opposé de sa conception initiale visant à s'affranchir des frontières et de la régulation étatique. Lors de la création d'Internet, les réseaux sont sans mémoire afin de garantir un traitement égalitaire (avec des variations de performance) des terminaux, indifférent à la topologie du réseau ou au contenu échangé. Actuellement, la tendance est à la modification de la logique des réseaux afin que le routage tienne compte de critères géographiques, politiques voire aussi économiques (sur fond de bataille juridique aux États-Unis pour la neutralité du Net). Pour Andreas Baur-Ahrens [52] cela entraine trois changements : 1) le renforcement de la position des fournisseurs d'accès, 2) une puissance accrue pour les autorités gouvernementales en terme de facilités d'intervention sur les réseaux ou en terme de contrôle de l'information, enfin, 3) la transition vers un réseau plus directif entrainant une plus forte passivité et dépendance de l'utilisateur, tendance déjà à l'œuvre avec l'avènement des grandes plateformes et le principe des outils as a service proposés par les grands acteurs du cloud.

La question du routage national ne traite que l'aspect géographique, l'autre aspect étant la place des géants du numérique (principalement les deux géants du Cloud : Google et Amazon) dans l'infrastructure d'Internet. Durant la dernière décennie, ils sont entrés massivement dans le marché câblier ce qui avantage technologiquement leur service car ils disposent notamment de câbles dédiés. De plus, ils gagnent aussi un avantage géopolitique par l'exploitation de ces câbles, principalement quand ils désenclavent numériquement certaines régions. Pour l'instant, la pose se fait en partenariat avec des entreprises existantes (comme Orange Marine) car même s'ils disposent des capacités financières nécessaires « ils ont encore besoin des capacités techniques des opérateurs historiques. » [53]. En 2020, Google dispose

52. M. Leese et S. Wittendorp. *Security/mobility : Politics of movement*. Manchester University Press, 2017, p.51.

53. C. d'études stratégiques de la marine. « Les câbles et les GAFAM ». In : *Brèves Marines - Technologie* 205 (novembre 2017).

de 4 câbles à titre privé et a investi dans une dizaine d'autres [54]. Facebook a investi dans une dizaine de câbles mais n'en possède pas en propre. Amazon en possède deux.

L'Espace est en passe d'entrer dans le cœur de réseaux d'Internet avec le lancement de plusieurs constellations de mini satellites destinées à fournir une couverture mondiale. Ces projets sont aussi le fait d'acteurs privés, qui sont soit des géants du numérique (Google et Amazon) soit des acteurs du New Space (avec les projet Starlink de SpaceX et OneWeb). L'infrastructure spatiale sera autant exposée, si ce n'est plus, à des accidents du fait de la multiplication des débris spatiaux, à de l'interception (ou à des perturbations) électromagnétique et même à des frappes cinétiques, les grandes puissances se dotant de capacités antisatellites.

Conclusion

La menace, et le rapport de force, s'étendent sur l'ensemble des couches du cyberespace. Au niveau matériel, le cœur de réseaux est l'enjeu le plus visible, les ressources, notamment les capacités de traitement de l'information (des datacenters et supercalculateurs), se concentrent aux États-Unis et entre les mains des géants du numérique. Une menace indirecte pointe à travers le marché des équipements avec le risque de portes dérobées dans les équipements réseaux (polarisation du débat autour de la 5G) ou dans les composants (tel les microprocesseurs). Les portes dérobées introduites volontairement par les équipementiers ou les éditeurs de logiciels constituent le cinquième niveau de menace (sur six) de l'échelle élaborée par le Départent de la Défense des États-Unis [55]. Par ailleurs, l'élongation de la chaine de sous-traitance au niveau des prestataires des fournisseurs d'accès accroit la problématique de la présence de portes dérobées dans les réseaux nationaux [56]. Au niveau de l'infrastructure logique, le routage et la convergence des systèmes industriels vers la technologie Ethernet et TCP/IP sont à l'origine de menaces majeures en facilitant la latéralisation d'un système d'information vers un système industriel. Plus généralement, la dominance des systèmes et logiciels fournis comme des services par les acteurs du Cloud (les géants du numérique étant les plus gros) tend à accroitre la puissance géopolitique des quelques plateformes et pays (Chine et États-Unis).

54. W. Qiu. *Complete List of Google's Subsea Cable Investments - Submarine Networks*. 9 juillet 2019. URL : `https://www.submarinenetworks.com/en/insights/complete-list-of-google-s-subsea-cable-investments` (visité le 21/05/2020).

55. *L'officier au service de la Nation dans le monde du XXI e siècle*, p. 56.

56. *Entretien avec un architecte réseau d'Orange.*

Quatre caractères spécifiques contribuant à la dangerosité de la cyberconflictualité contemporaine peuvent être dégagés. Le premier est celui de la multiplication des acteurs concernés tant en terme d'assaillants, de donneurs d'ordre que de victimes. Le deuxième est la course aux armements cyber du fait de l'accroissement des capacités offensives de certaines puissances et de la démocratisation des techniques d'attaque avec la constitution d'un marché parallèle. Le troisième est l'incertitude, elle provient à la fois des aspects techniques mais aussi du fait que les opérations dépassent le cadre militaire. Le doute demeure sur l'acteur effecteur, le commanditaire (du fait de l'utilisation de proxy ou de prestataires), sur les objectifs recherchés (économiques, politiques, culturels, réputationnels) et sur les cibles réelles. Le quatrième est la dimension multiforme, et l'ubiquité de la menace qui peut passer d'un stade local à une échelle mondiale en quelques heures en s'affranchissant de toute notion de frontière. Cependant, la majorité des crises reste localisée géographiquement ou ne frappe qu'un petit nombre d'acteurs. Il importe donc d'avoir « une compréhension fine du système international et de la nature des crises existantes » [57] afin de pouvoir plonger les opérations cyber dans leur contexte. Pour les États, la menace cyber est liée à deux autres facteurs [58] : 1) l'imbrication des enjeux de cybercriminalité et de sécurité nationale (les outils utilisés à des fins de fraudes ou d'extorsion peuvent causer des dommages aux systèmes d'information de l'État ou à ceux des systèmes critiques) et 2) l'exposition accrue de nos société à la menace. Les forces armées ne sont pas en reste, elles sont soumises à une exposition grandissante à cause d'un manque d'hygiène numérique, principalement à travers l'usage de leurs terminaux personnels [59] (smartphones, montres connectées), d'une modernisation des équipements et de l'utilisation d'armements intégrant des composantes numériques. L'art de la guerre en est profondément modifié. « Dès maintenant, perdre dans le cyber, c'est perdre tout court ! » [60]

57. « Cybersécurité : Extension du domaine de la lutte ». In : *Politique étrangère* 2 (2018), p. 9-230, p. 11.

58. Ibid., p.10.

59. *La Défense belge démontre qu'utiliser un téléphone portable personnel peut mettre en échec une opération militaire.* 26 février 2020. URL : `http://www.opex360.com/2020/02/26/la-defense-belge-demontre-quutiliser-un-telephone-portable-personnel-peut-mettre-en-echec-une-operation-militaire/` ; « Une application de jogging menace la sécurité des bases militaires ». In : *Le Monde* (28 janvier 2018).

60. p. 10 A. Bonnemaison et S. Dossé. *Attention : Cyber ! : vers le combat cyber-électronique.* Economica, 2014, p. .

Bibliographie

Bibliographie générale

Cattaruzza, A. « Chapitre 1. La construction politique de l'espace numérique. Penser l'espace numérique comme un espace stratégique ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 19-25.

L'officier au service de la Nation dans le monde du XXI e siècle. LesCahiersdelaRevueDéfenseNationale. 2018, p. 72.

Taillat, S. « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33.

Leese, M. et S. Wittendorp. *Security/mobility : Politics of movement*. Manchester University Press, 2017.

Bonnemaison, A. et S. Dossé. *Attention : Cyber ! : vers le combat cyber-électronique*. Economica, 2014.

Rapports

ANSSI. *Etat de la menace rançongiciel à l'encontre des entreprises et des institutions*. 5 février 2020.

CADIC, O. et R. MAZUIR. *Projet de loi de finances pour 2020. Direction de l'action du gouvernement :coordination du travail gouvernemental : SGDSN, ANSSI, cyberdefense, INHESJ, IHEDN*. Note de synthèse N° 46 (2019-2020). Sénat, novembre 2019.

James Andrew Lewis. *Economic Impact of Cybercrime—No Slowing Down Report*. CSIS - Center for strategic & International studies, février 2018, p. 28.

PALLE, A. *Vulnérabilité et protection des réseaux électriques : Approches comparées Union européenne - Etats-Unis*. Note de recherche 62. IRSEM, 28 septembre 2018, p. 18. (Visité le 16/04/2020).

SGDSN. *Revue stratégique de cyberdéfense*. 2018.

Sunak, R. et J. Stavridis. *Undersea cables : indispensable, insecure*. Policy Exchange, 2017. URL : `https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf`.

Articles de recherche

Bilge, L. « Invited Keynote : Is Proactive Security even Possible ? » In : *13th European workshop on Systems Security*. 2020.

Kempf, O. « Du cyber et de la guerre ». In : *Fondation pour la recherche stratégique* (Note n°17/2019 12 septembre 2019).

« Cybersécurité : Extension du domaine de la lutte ». In : *Politique étrangère* 2 (2018), p. 9-230.

Gautier, L. « Cyber : les enjeux pour la défense et la sécurité des Français ». In : *Politique étrangère* Été.2 (2018), p. 29-42.

Nocetti, J. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27.

marine, C. d'études stratégiques de la. « Les câbles et les GAFAM ». In : *Brèves Marines - Technologie* 205 (novembre 2017).

Morel, C. « Les câbles sous-marins : un bien commun mondial ? » In : *Études* Mars.3 (2017), p. 19-28.

Zyw Melo, A. « Un câble pour les BRICS : un défi stratégique insurmontable ». In : *Hermès, La Revue* 79.3 (2017), p. 145-149.

Articles de presse

« En Ile-de-France, l'accès au réseau téléphonique et Internet d'Orange perturbé par la destruction de câbles en fibre optique ». In : *Le Monde* (6 mai 2020).

« Après la cyberattaque au CHU de Rouen, l'enquête s'oriente vers la piste crapuleuse ». In : *Le Monde* (26 novembre 2019).

Untersinger, M. « Une attaque informatique perturbe le fonctionnement du groupe M6 ». In : (octobre 2019).

Yugo Neumorni. « La 'taupe' venue du réseau électrique ». In : *Observatoire FIC* (24 juillet 2019). (Visité le 13/04/2020).

« Une application de jogging menace la sécurité des bases militaires ». In : *Le Monde* (28 janvier 2018).

Bernard, T. S. « Ways to Protect Yourself After the JPMorgan Hacking ». In : *The New York Times* (3 octobre 2014). (Visité le 21/05/2020).

Ressources web

Cyber Operations Tracker. Council on Foreign Relations. URL : https://www.cfr.org/interactive/cyber-operations (visité le 09/12/2019).

La Défense belge démontre qu'utiliser un téléphone portable personnel peut mettre en échec une opération militaire. 26 février 2020. URL : http://www.opex360.com/2020/02/26/la-defense-belge-demontre-quutiliser-un-telephone-portable-personnel-peut-mettre-en-echec-une-operation-militaire/.

Qiu, W. *Complete List of Google's Subsea Cable Investments - Submarine Networks*. 9 juillet 2019. URL : https://www.submarinenetworks.com/en/insights/complete-list-of-google-s-subsea-cable-investments (visité le 21/05/2020).

Conférences

Forum International de la Cybersécurité (FIC). Lille, 2020.

Symposium sur la sécurité des technologies de l'information et des communications (SSTIC). Rennes, 2018.

Liste des entretiens

Entretien réalisé le 10/02/2020 avec un architecte réseau d'Orange.

Entretien réalisé le 16/06/2020 avec avec un reponsable du comité stratégique de filière industries de sécurité.

60. Le terme d'agent désigne un poste technique, le terme de conseiller désigne un poste s'intéressant à la stratégie et le terme de responsable désigne un poste d'encadrement et de décision.