LE PRÉSIDENT
COMITÉ CONSULTATIF DE TÉLÉCOMMUNICATIONS
POUR LA SÉCURITÉ NATIONALE

Rapport du NSTAC au Président sur la résilience de l'Internet et des communications

TABLE DES MATIÈRES

RÉSUMÉ EXÉCUTIF

Les attaques automatisées et distribuées facilitées par les botnets menacent la sécurité et la résilience de l'écosystème Internet et des infrastructures critiques de la nation. La taille et l'ampleur des attaques par déni de service distribué (DDoS) facilitées par les botnets ont augmenté de façon spectaculaire au cours des dernières années. Cette évolution accroît les craintes que ces attaques puissent submerger les infrastructures critiques des États-Unis. Pour aggraver le problème, le mélange croissant d'appareils de l'Internet des objets (IoT) offre un environnement propice aux acteurs malveillants pour lancer des attaques automatisées mondiales à l'aide d'appareils IoT compromis. Cette situation menace la sécurité de l'écosystème Internet.

En mai 2017, le Bureau exécutif du président (EOP) a demandé au Comité consultatif sur les télécommunications de sécurité nationale du président (NSTAC) d'examiner comment le secteur privé et le gouvernement pourraient améliorer la résilience de l'écosystème de l'Internet et des communications. [1] L'EOP, à l'appui de l'Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, a spécifiquement demandé au NSTAC d'identifier les moyens d'encourager la collaboration afin de réduire les menaces liées aux attaques automatisées et distribuées (par exemple, les botnets). Ce *rapport du NSTAC au président sur la résilience de l'Internet et des communications* (le "rapport") présente le travail du NSTAC et ses recommandations.

PRINCIPAUX ENSEIGNEMENTS TIRÉS

Un plus grand sentiment d'urgence est nécessaire. La menace ne fera que croître à mesure que le nombre et le type de dispositifs IoT augmentent et que ces dispositifs deviennent plus autonomes, plus performants et plus omniprésents.
Dans la mesure du possible, l'étude, le test et la mise en œuvre des solutions possibles doivent être menés en parallèle plutôt que de manière séquentielle. Des efforts doivent être faits pour devancer les menaces.

Les partenariats public-privé sont essentiels. Les partenariats public-privé, tels que le Financial Systemic Analysis & Resilience Center, ainsi que les efforts déployés par le Federal Bureau of Investigation, Microsoft et les fournisseurs d'accès à Internet (FAI), montrent que les botnets criminels et les structures de commande et de contrôle peuvent être efficacement perturbés. La collaboration entre les secteurs public et privé est essentielle pour atténuer les réseaux de zombies.

Les solutions dépendent de chaque partie de l'écosystème Internet. Les attaques distribuées constituent un défi complexe. Aucun segment de l'écosystème Internet ne peut résoudre ce problème seul.

Les solutions dépendent à la fois des normes et de l'innovation au niveau de l'infrastructure réseau et Internet. Bien qu'il existe une variété de normes et de meilleures pratiques, il y a un manque de cohérence mondiale dans l'adoption de ces pratiques. Les normes jouent un rôle essentiel dans la sécurisation de l'écosystème Internet. Cependant, avec un environnement de normes fragmenté et de nombreux appareils fabriqués en dehors des États-Unis, le déploiement des normes sera probablement inégal. Il existe un besoin pour des solutions émergentes au niveau de l'infrastructure. En outre, il pourrait être utile de développer des normes en amont du dispositif, par exemple au niveau du jeu de puces.

[1] Bureau du secrétaire de presse de la Maison Blanche. *Ordre exécutif 13800, Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques*. 16 mai 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

L'éducation et la sensibilisation sont en retard. La nation a besoin d'un citoyen numérique informé. Les particuliers et les entreprises doivent comprendre comment leurs décisions influencent les réseaux, les systèmes et les autres.

Des normes internationales floues compliquent les défis. Une grande partie de la menace provient de l'étranger, de sorte que les enquêtes et les poursuites internationales sont essentielles. Une coopération mondiale est nécessaire en matière de normes techniques, de sécurité des dispositifs, d'attribution, de flux de trafic, ainsi que de normes et de défenses communes.

Un nouveau modèle de confiance est nécessaire. Le protocole de contrôle de transmission/protocole Internet, le protocole de passerelle de frontière, le système de nom de domaine et de nombreux autres protocoles qui sous-tendent l'Internet n'ont pas été conçus avec la sécurité comme préoccupation principale. Les réseaux étant de plus en plus ouverts et interconnectés, ce modèle de confiance ne peut plus être le seul fondement de la sécurité de l'internet. [2] La définition de la manière dont une plus grande confiance peut être intégrée à l'internet devrait être un point central de l'effort du Moonshot de la cybersécurité décrit ci-dessous.

RECOMMANDATIONS CLÉS

Le secteur privé doit agir. La lutte contre les attaques automatisées et distribuées nécessite une vigilance de l'ensemble de l'écosystème Internet, y compris les fournisseurs de services réseau ou ISP, les fabricants d'appareils, les développeurs de logiciels, les fournisseurs de cloud, d'applications et d'hébergement et d'autres entités, qui constituent tous l'infrastructure Internet. Le NSTAC recommande les actions à court terme suivantes :

- **Accélérer l'adoption de lignes directrices en matière de sécurité**. Le secteur des communications devrait collaborer avec le Department of Homeland Security (DHS), en tant qu'agence sectorielle pour les communications, et la National Telecommunications and Information Administration (NTIA) pour identifier les pratiques de sécurité communes pertinentes pour les réseaux de communications afin de se protéger contre les botnets et les attaques DDoS dans les organismes de normalisation nationaux et mondiaux (par exemple, Best Common Practice (BCP) 38) et identifier les obstacles à l'adoption et/ou les incitations pour promouvoir l'adoption. Les réseaux ne sont pas forcément limités aux grands fournisseurs d'accès à Internet (FAI), car de nombreuses pratiques devraient être déployées par toute entité exploitant un réseau adressable par le public, y compris les entreprises.

- **Élaborer des directives sur la sécurité des dispositifs IoT.** Le ministère du Commerce (DOC), par l'intermédiaire de la NTIA et du National Institute of Standards and Technology (NIST), doit collaborer avec les fabricants de dispositifs pour faciliter le développement d'une base de référence de pratiques de sécurité de bon sens recommandées en fonction du risque associé à un dispositif. Le DOC devrait également examiner le rôle et la viabilité de la certification volontaire des dispositifs et des tests indépendants pour garantir la sécurité des dispositifs.

- **Continuer à innover autour de solutions basées sur l'infrastructure.** Les pouvoirs publics et l'industrie ne peuvent pas compter uniquement sur l'adoption systématique de normes pour sécuriser l'IdO. Les FAI, les fournisseurs de services sans fil, les fabricants de routeurs, les fournisseurs de solutions de sécurité et autres développent des services pour gérer la sécurité de l'IdO. Ces solutions peuvent être employées à différentes couches du réseau, depuis l'intérieur de la maison (par exemple, Ethernet, Wi-Fi) jusqu'à l'intégration de la sécurité à long terme.

[2] Conseil de la fiabilité et de l'interopérabilité de la sécurité des communications (CSRIC) V : Groupe de travail 10, Réductions des risques hérités (2017) (Rapport sur les réductions des risques hérités), https://www.fcc.gov/files/csric5-wg10- finalreport031517pdf.

Evolution ou de cinquième génération ; le cœur du réseau de commutation multiprotocole par étiquette ; et au niveau de la couche application ou dans le nuage. [3] Ces capacités sont émergentes et le secteur privé doit continuer à investir dans ces technologies. Le gouvernement américain devrait contribuer à stimuler ces capacités en les intégrant dans les exigences des marchés publics fédéraux et en sensibilisant à leur application pour la sécurité de l'IdO.

- **Promouvoir les contrôles de sécurité des entreprises pour améliorer la sécurité des dispositifs IoT.** Le NIST devrait développer des cas d'utilisation s'appuyant sur le cadre de cybersécurité du NIST pour permettre aux entreprises d'intégrer l'IdO dans la gestion des risques. De nombreux dispositifs IoT auront un double usage dans les réseaux des consommateurs et des entreprises. Les entreprises et le gouvernement peuvent promouvoir des normes de sécurité de l'IdO pour les dispositifs dans les accords d'achat.

- **Promouvoir l'assurance logicielle.** L'industrie du logiciel devrait travailler avec le DHS pour promouvoir des pratiques communes en matière d'assurance logicielle. La connaissance des meilleures pratiques permettrait aux acheteurs de savoir comment leurs fournisseurs intègrent la sécurité et les aiderait à prendre de meilleures décisions d'achat.

Le gouvernement doit agir. Le gouvernement doit répondre à la menace croissante des botnets dans trois domaines fondamentaux. Le NSTAC recommande au gouvernement (1) de prendre des mesures plus importantes pour soutenir l'application de la loi, (2) de promouvoir l'adoption de normes de sécurité et de meilleures pratiques et (3) d'élaborer une stratégie internationale efficace en matière de cybersécurité.

- **Application de la loi**

    - **Soutenir la collaboration public-privé et les démantèlements.** Le gouvernement, y compris le ministère de la Justice (DOJ), devrait accroître les efforts de démantèlement qui ont permis d'atténuer l'impact des botnets. Le gouvernement américain devrait inciter davantage, notamment au sein du DOJ, à faire de la prévention de la cybercriminalité et du démantèlement des botnets une priorité plus importante. Les répercussions des botnets sur la sécurité nationale justifient la prévention et les poursuites judiciaires. Le ministère de la Justice pourrait avoir besoin de ressources supplémentaires pour intensifier ces efforts, qui dépendent également de la collaboration avec le secteur privé et d'éventuels partenaires internationaux.

- **Promouvoir l'adoption de normes de sécurité et de meilleures pratiques**

    - **Promouvoir des normes flexibles à l'aide d'incitations et supprimer les obstacles à l'adoption.** La NTIA, le NIST et d'autres agences devraient réunir les parties prenantes et promouvoir la coordination entre les secteurs afin de développer des normes communes et de promouvoir des pratiques cohérentes au sein du gouvernement et dans les infrastructures critiques. Le gouvernement devrait identifier les lacunes et les incitations pour motiver l'industrie à adopter des normes et des pratiques. Certaines industries, si elles sont en retard, peuvent avoir besoin de plus d'incitations, en particulier lorsqu'il s'agit d'atténuer les risques des dispositifs actuellement en place. Les petites entreprises peuvent également ne pas disposer des mêmes ressources et du même accès à l'expertise cybernétique que les grandes entités. Enfin, le marché de l'assurance peut conduire

[3] Cisco propose un exemple de cadre pour la sécurité de l'IdO à chaque couche du réseau à l'adresse https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.

l'amélioration, car les souscripteurs sondent les entreprises sur la maturité de leurs pratiques de gestion des risques de sécurité et proposent des primes plus basses aux entreprises situées plus haut sur l'échelle de maturité.

- **Chercher à harmoniser les exigences de sécurité aux niveaux fédéral, étatique et international.** Les normes, pratiques et réglementations en matière de cybersécurité sont souvent abordées de manière fragmentée et quelque peu inefficace. Au niveau national, certains États établissent des exigences de sécurité spécifiques. Au niveau international, l'Union européenne, le Japon, la Chine et plusieurs autres pays envisagent de développer des programmes de certification et de test des dispositifs IoT. Le gouvernement américain doit se faire le champion de normes de sécurité IdO interopérables cohérentes à l'étranger et au niveau national parmi les États afin d'encourager une approche unifiée.

- **Améliorer la cybersécurité du gouvernement.** Le gouvernement américain doit donner l'exemple en améliorant la sécurité des réseaux fédéraux. La modernisation des technologies de l'information (TI) est un élément clé de l'amélioration de la cybersécurité fédérale. Le gouvernement devrait utiliser ses efforts actuels de modernisation des TI fédérales pour stimuler l'adoption de nouvelles technologies et de solutions de sécurité dans le secteur privé.

- **Cybersécurité internationale**

  - **Élaborer une stratégie globale d'engagement des États-Unis en matière de normes**. Les États-Unis ont traditionnellement compté sur la collaboration avec l'industrie privée pour renforcer les efforts du gouvernement dans les forums internationaux sur les normes. Cependant, ces dernières années, les entités étrangères ont rapidement accru leur présence dans l'élaboration des normes internationales. Le gouvernement américain devrait collaborer avec le secteur privé afin d'assurer une représentation dans les forums clés ayant un impact sur le développement de normes technologiques susceptibles d'entraîner des problèmes de sécurité nationale à l'avenir.

  - **Élaborer une stratégie internationale efficace en matière de cybersécurité axée sur l'augmentation du coût pour les attaquants.** Le gouvernement devrait donner la priorité à l'élaboration d'une stratégie internationale globale en matière de cybersécurité, en s'appuyant sur les outils diplomatiques traditionnels et en soutenant l'application de la loi au niveau mondial, dans le but d'augmenter les coûts pour les cyberattaquants. De nombreuses attaques DDoS sont internationales, et le gouvernement doit mettre en œuvre une stratégie mondiale pour faire face à ces menaces. La nature persistante des cyberattaques signifie que même les entités ayant les meilleures pratiques peuvent toujours être exploitées. La nation doit augmenter le coût pour les attaquants tout en adoptant des normes, des pratiques et de nouvelles solutions technologiques innovantes pour rendre les attaques plus difficiles.

- **La nation a besoin d'un "Moonshot" en matière de cybersécurité.** Un futur effort du NSTAC devrait analyser le concept de lancement d'un Moonshot sur la cybersécurité en deux phases. La première phase consisterait à examiner d'autres modèles de Moonshot réussis, y compris en dehors du domaine de la cybersécurité, afin d'identifier les principes cohérents qui peuvent être appliqués au défi de la cybersécurité. Pour commencer, il s'agirait d'étudier les modèles qui présentent au moins les caractéristiques suivantes :

  - Appel national à l'action ;
  - Se concentrer sur un objectif final, en fixant un objectif spécifique ou un état final à une certaine date ; et
  - Un processus multipartite dirigé par le gouvernement.

Dans la deuxième phase de l'étude, le NSTAC cherchera à clarifier les principales considérations en matière de cybersécurité liées aux principes du Moonshot (appel à l'action, objectif final et processus multipartite), en faisant appel à des experts en cybersécurité pour définir un objectif final et des sous-éléments, et en développant les documents que le NSTAC a examinés lors de la préparation du présent rapport. [4]

[4] Par exemple, le briefing sur les modèles de référence de mémoire unifiée fourni par Steve Wallach. Micron Technology, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 7 septembre 2017.

1.0 INTRODUCTION

On s'inquiète de plus en plus de la possibilité pour des acteurs malveillants d'utiliser des réseaux de zombies pour faciliter des attaques par déni de service distribué (DDoS) à grande échelle qui pourraient perturber les infrastructures critiques des États-Unis. Les attaquants exploitent les vulnérabilités fondamentales de l'Internet, telles que le système de noms de domaine (DNS), le protocole NTP (Network Time Protocol), le protocole Simple Service Discovery, le protocole CharGen (Character Generator Protocol) et d'autres protocoles, afin d'augmenter considérablement la taille et l'ampleur des attaques. De plus, si les réseaux de zombies ne sont pas nouveaux, les dispositifs de l'Internet des objets (IoT) aggravent le risque car ils connectent un nombre croissant de personnes, de dispositifs et de réseaux. L'attaque du botnet Mirai en 2016 a été le premier botnet basé sur l'IdO ayant un impact significatif, mais on s'attend à ce que de telles attaques augmentent. [6]Ces facteurs ont conduit à une augmentation rapide de la taille et de l'ampleur des attaques DDoS. Par exemple, selon une source, la taille des attaques se situait autour de 100 gigabits par seconde (Gbps) jusqu'à la mi-2012, après quoi la taille a commencé à augmenter de façon spectaculaire. La même source a estimé que la taille maximale des attaques en 2016 était d'environ 800 Gbps, soit une multiplication par huit au cours des quatre dernières années. [7]Ce rapport fournit des recommandations pour réduire l'impact potentiel des botnets et des attaques DDoS et la menace qu'ils représentent pour les infrastructures critiques de la Nation.

1.1 Champ d'application et charge

En mai 2017, le Bureau exécutif du président (EOP) a demandé au Comité consultatif sur les télécommunications de sécurité nationale du président (NSTAC) d'examiner comment le secteur privé et le gouvernement peuvent collaborer pour améliorer la résilience de l'écosystème de l'Internet et des communications. [8]L'EOP, à l'appui de l'Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (renforcement de la cybersécurité des réseaux fédéraux et des infrastructures critiques)*, a chargé le NSTAC d'identifier les moyens d'encourager la collaboration pour réduire les menaces liées aux attaques automatisées et distribuées (telles que les botnets). En outre, l'EOP a demandé au NSTAC d'examiner quelles règles d'engagement permettront des efforts de coopération pour protéger la posture de cybersécurité de la Nation. En juin 2017, le NSTAC a formé le comité sur la résilience de l'Internet et des communications (ICR) pour répondre aux demandes de l'EOP. [9] L'EOP a indiqué que les conclusions du NSTAC alimenteront un rapport préliminaire qui sera publié par le ministère du Commerce (DOC) et le ministère de la Sécurité intérieure (DHS) en janvier 2018.

Les attaques DDoS et botnet sont de plus en plus préoccupantes. En 2014, le NSTAC a observé que " [d]ans 2020, des dizaines de milliards de dispositifs seront utilisés. Il est temps d'influencer la conception de ces appareils et les protocoles qui régissent leur utilisation ; une fois qu'ils auront été déployés, de nouvelles politiques seront nécessaires.

[5] Arbor Networks Worldwide Infrastructure Security Report, Volume XII, disponible à l'adresse https://www.arbornetworks.com/insight-into-the-global-threat-landscape.

[6] Voir Computer Weekly, " Global Hacker Botnet Tops 6 Million Hijacked Devices ", 27 septembre 2017 http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6-million-hijacked-devices.

[7] Arbor Networks Worldwide Infrastructure Security Report Volume XII, disponible à l'adresse https://www.arbornetworks.com/insight-into-the-global-threat-landscape.

[8] Bureau du secrétaire de presse de la Maison Blanche. *Ordre exécutif 13800, Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques*. 11 mai 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[9] Un rapport du sous-comité du RIC est attendu en octobre 2017. Le DHS et le DOC publieront un rapport préliminaire d'ici janvier 2018 et un rapport final d'ici mai 2018.

Le but du NSTAC est d'aider l'administration à renforcer la coopération entre le gouvernement et le secteur privé.

Ce *rapport du NSTAC au président sur la résilience de l'Internet et des communications* ("rapport") présente le travail du NSTAC et ses recommandations. Il fournit à l'EOP une feuille de route exploitable pour faire face aux menaces posées par les botnets et autres attaques distribuées et automatisées contre notre infrastructure Internet, nos services en ligne et nos utilisateurs finaux. Ce rapport examine les menaces et les solutions, des remèdes à court terme au développement de l'architecture Internet à long terme. Le rapport est organisé comme suit :

- La section 1 explique le champ d'application et les objectifs.
- La section 2 décrit l'écosystème mondial de l'Internet et la manière dont les attaques distribuées menacent la sécurité d'un monde de plus en plus connecté.
- La section 3 identifie les défis et les efforts d'atténuation dans chaque segment de l'écosystème : réseaux, consommateurs/appareils de pointe, entreprises et logiciels/applications/systèmes d'exploitation (OS).
- La section 4 propose des recommandations à court et à long terme, ainsi qu'une étude Moonshot de suivi pour aborder de manière plus globale les défis de la cybersécurité, notamment les attaques automatisées et distribuées.
- La section 5 identifie les possibilités pour le gouvernement d'utiliser les outils uniques dont il dispose et de collaborer avec le secteur privé.

1.2 Approche

Le NSTAC a utilisé plusieurs méthodes pour recueillir des informations, y compris des briefings d'experts en la matière, des examens de politiques et l'examen de rapports sur les menaces de cybersécurité, d'articles et de meilleures pratiques pour combattre ces menaces. Entre autres choses, le NSTAC :

- Nous avons reçu plus de deux douzaines de séances d'information de la part d'experts de l'industrie, du milieu universitaire et du secteur public, comme en témoigne l'annexe A ;
- Examen des politiques, réglementations, rapports et meilleures pratiques du secteur privé et du gouvernement fédéral en matière de cybersécurité, comme le cadre de cybersécurité du National Institute of Standards and Technology (NIST) ;
- examiné les meilleures pratiques et recherches actuelles de l'industrie en matière de cybersécurité ; et

[10] Comité consultatif du président sur les télécommunications pour la sécurité nationale (NSTAC). *Rapport du NSTAC au président sur l'Internet des objets*. November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf. Annexe E, E-5.

- Examen des études et des commentaires sur la cybersécurité au NIST et à la National Telecommunications and Information Administration (NTIA).

Le NSTAC a examiné les faiblesses de la sécurité de l'écosystème et a identifié les domaines dans lesquels il est possible d'améliorer la sécurité au niveau du réseau, des dispositifs et des utilisateurs. Dans ce rapport, le NSTAC recommande des mesures pour créer un écosystème Internet plus sûr, en mettant l'accent sur les partenariats entre le gouvernement et l'industrie pour lutter contre les activités malveillantes.

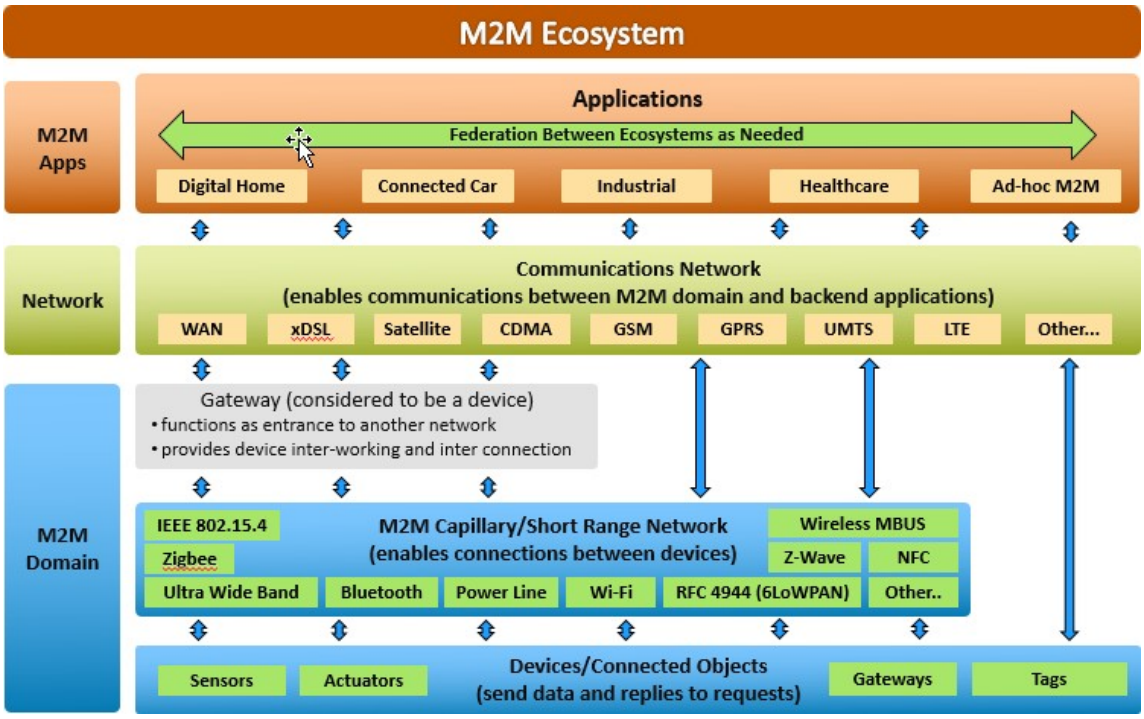
2.0 LA NATURE GLOBALE DE L'ÉCOSYSTÈME FACILITE LES ATTAQUES DISTRIBUÉES ET AUTOMATISÉES

L'écosystème Internet est divers et diffus, et chaque partie joue un rôle dans la sécurité. L'écosystème continue de se développer avec une prolifération d'appareils qui relient à l'Internet des objets du quotidien tels que les voitures et les thermostats, prennent en charge les systèmes de contrôle industriels et surveillent les infrastructures critiques. Un acteur malveillant contrôlant un appareil infecté crée de multiples risques. Premièrement, le dispositif peut être utilisé dans une attaque par déni de service contre un autre dispositif. Ensuite, un logiciel zombie installé sur un appareil peut être utilisé pour voler des informations ou suivre l'appareil. Par exemple, un logiciel zombie installé sur le logiciel de navigation de la voiture d'un membre du Congrès pourrait suivre les déplacements du véhicule. Troisièmement, le logiciel bot sur un appareil pourrait être utilisé pour générer un déni de service (DoS) sur l'appareil lui-même. Quatrièmement, le bot pourrait manipuler les données ou provoquer un comportement incorrect de l'appareil, mettant ainsi en danger la sécurité des utilisateurs ou corrompant les données de l'appareil influençant les résultats pour les consommateurs de données. À mesure que les dispositifs IoT prolifèrent et remplissent des fonctions de plus en plus sensibles, comme la conduite autonome et les contrôles industriels, la neutralisation des dispositifs IoT peut avoir des répercussions importantes et dangereuses dans le monde réel.

2.1 L'écosystème mondial de l'internet et des communications est diversifié et en pleine évolution

Les utilisateurs finaux, les fournisseurs d'accès à Internet (FAI), les opérateurs de réseau, les fabricants et les développeurs de logiciels constituent l'écosystème mondial de l'Internet. Les gouvernements et les systèmes internationaux jouent également un rôle. Les couches supportant l'IdO de machine à machine (M2M) qui composent l'écosystème sont illustrées dans la figure 1 de la page suivante.

Figure 1. L'écosystème M2M



Source : Présentation d'AT&T sur le rapport du NSTAC au président sur l'Internet des objets. 19 novembre 2014.

Bien que certains prétendent que les FAI sont les mieux placés pour atténuer les attaques de botnet, l'IdO se compose d'appareils, de réseaux de transport, d'applications, ainsi que des entreprises et des utilisateurs qui les déploient. Chaque segment est confronté à des menaces et nécessite une attention particulière.

Figure 2. Paysage des menaces

Source : Brian Rexroad. AT&T. Briefing au sous-comité ICR du NSTAC. Le 20 juillet 2017.

Les experts prévoient une migration vers les services IoT gérés, les entreprises proposant des solutions complètes. [11] La prolifération des appareils IoT offre une nouvelle échelle aux réseaux de zombies.

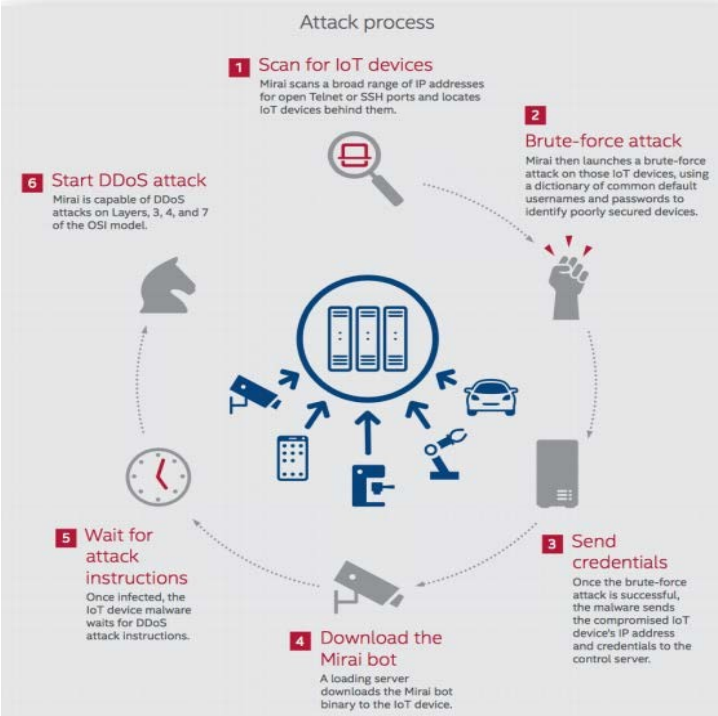
[11] Kevin Walsh. Palo Alto Networks, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 18 juillet 2017.

2.2 Les botnets et les attaques distribuées automatisées évoluent

Les botnets ont été conçus à l'origine pour un usage positif et ont ensuite été réaffectés à des actions hostiles. Un bot est "un programme installé sur un système pour permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous le commandement et le contrôle d'un administrateur distant (alias bot master ou bot herder)".[12] Ces programmes peuvent exécuter un code qui n'est pas fourni par le vendeur ou autorisé par son propriétaire. La plupart des bots peuvent soutenir des activités malveillantes telles que le spam, le phishing, la fraude au clic et le DDoS.

Un botnet est "un réseau d'appareils informatiques d'utilisateurs finaux connectés à Internet, infectés par des logiciels malveillants et contrôlés à distance par des tiers à des fins néfastes "[13] Une attaque par botnet se produit lorsqu'un réseau d'ordinateurs, d'appareils IoT ou d'autres appareils compatibles avec le protocole Internet (IP) est réquisitionné pour exécuter un code non autorisé à l'appui d'activités malveillantes telles que le spam, le phishing, la fraude au clic et le DDoS. La figure 3 fournit une représentation de la manière dont les attaques de botnet se produisent.

Figure 3. Comment se produisent les attaques de botnet



Source : McAfee, https://www.mcafee.com/us/resources/misc/infographic-threats-report-mar-2017.pdf

Les robots sont généralement diffusés par des sites web infectés ou des liens vers des sites web malveillants intégrés dans des courriels de phishing. Les utilisateurs peuvent installer des robots par inadvertance en se basant sur des courriels trompeurs, des instructions en ligne ou des vulnérabilités du navigateur ou du système d'exploitation. Les bots peuvent également être déployés sans aucune action de la part de l'utilisateur final. Par exemple, dans le botnet Mirai, plusieurs appareils ont été infectés sans qu'aucun utilisateur n'ait eu à intervenir.

[12] Commission fédérale des communications (FCC). CSRIC. III, *Code de conduite anti-bot (ABC) américain pour les fournisseurs de services Internet*. Mars 2012. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

[13] Ibid.

Les mots de passe par défaut pour la gestion des appareils ou les portes dérobées installées par le fournisseur peuvent être compromis, ce qui permet un accès non autorisé à un appareil et son contrôle. Les bots sont également distribués par le biais de programmes d'hameçonnage, de spam et d'autres menaces de sécurité. L'un des aspects clés des campagnes de botnet est la nature persistante des attaques, qui cherchent à exploiter toute faiblesse disponible pour obtenir un accès. Les bots peuvent mettre à jour les correctifs de sécurité et les logiciels antivirus d'une machine afin d'assurer un fonctionnement stable et d'exclure les autres bots. Lorsque l'on parle de botnets, on pense souvent à des attaques DDoS. Mais les réseaux de zombies peuvent faciliter le vol de données, la distribution de contenu illégal, le vol de traitement, le spam par courriel, la fraude au clic et d'autres attaques15. [15]

Les attaques de botnets augmentent en taille et en sophistication avec l'essor de l'IoT. Certains botnets utilisent l'intelligence artificielle (IA), la cryptographie quantique ou l'informatique neuromorphique, pour fabriquer des virus plus intelligents qui s'adaptent à la vitesse d'Internet. [16]La plus grande attaque signalée était de 800 Gbps, et environ un tiers des attaques culminent à plus de 100 Gbps. [17] Les FAI ont considérablement augmenté la protection contre les attaques DDoS à la suite des attaques DDoS contre les institutions financières en 2012-2013,[18]mais les attaques DoS ont augmenté en taille, et les attaquants ont changé de tactique. Par exemple, les attaquants ciblent les domaines ayant le plus grand enregistrement DNS pour amplifier l'efficacité de leur attaque.
En outre, à mesure que les appareils deviennent plus autonomes et intègrent une IA sophistiquée, les implications de la cybercriminalité par le biais de l'IdO donneront lieu à de nouveaux risques graves qui doivent être anticipés et planifiés à court terme.

Les **mesures d'atténuation renforcent la prévention**. Les cyberattaques se produiront. [19]Selon la Direction des sciences et des technologies du DHS, 70 % des piratages utilisent des informations d'identification perdues, volées ou faibles, et 60 % des logiciels malveillants utilisent l'escalade des privilèges ou des informations d'identification volées. [20]Plutôt que de prévenir les attaques de botnet, les experts se sont orientés vers la construction de réseaux plus résistants et l'atténuation des effets des attaques. Les meilleures pratiques pour atténuer les attaques se concentrent sur la formation des utilisateurs et des entreprises à l'hygiène des réseaux et à la gestion des vulnérabilités. Cela inclut l'authentification forte, la désactivation des fonctions indésirables et la mise à jour des services. Parmi les autres outils d'atténuation, citons l'analyse des réseaux et des données, les proxys inversés, les pare-feu d'application et de réseau, les équilibreurs de charge et la reconfiguration/sécurisation des routeurs Internet. L'atténuation des attaques DDoS à grande échelle fonctionne mieux lorsqu'elle est complétée par des services de centre de données/de périphérie. L'analyse des données, les signaux, les mesures systémiques, la détection des anomalies, la détection des données et les déclencheurs sont tous utiles pour atténuer les attaques de botnet. Il est important d'examiner les caractéristiques et les dépendances communes pour identifier les comportements similaires et les attribuer aux acteurs. [21]

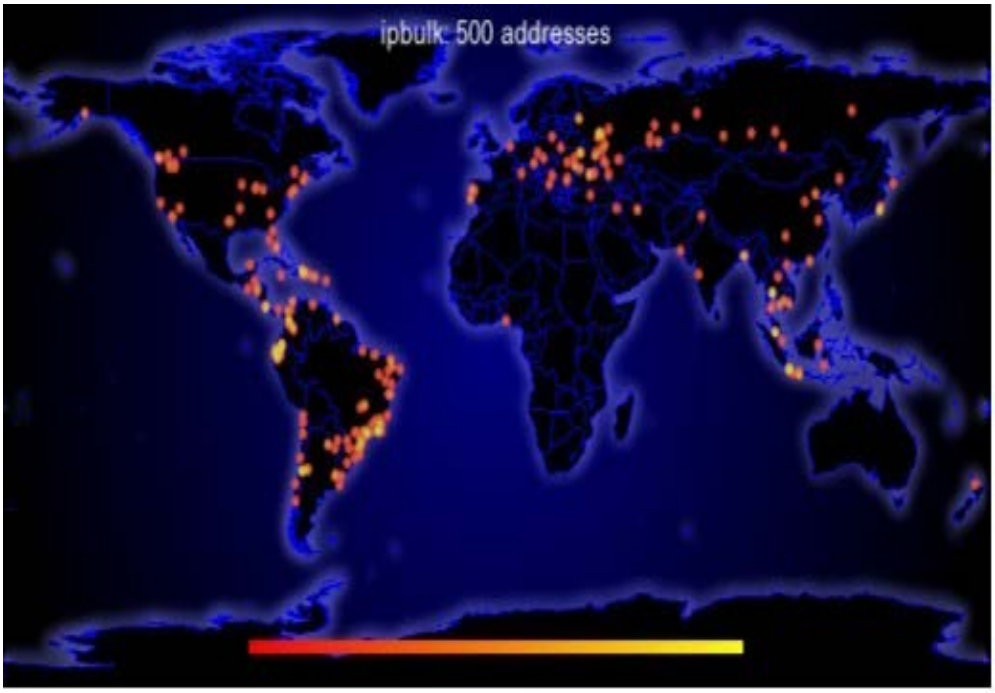
[14] Kim Zetter. "Hacker Lexicon : Que sont les attaques DoS et DDoS ?" *Wired.* 6 janvier 2016. https://www.wired.com/2016/01/hacker-lexicon-quoi-sont-des-dos-et-des-dos-attaques/.
[15] NTIA. Conseil de coordination du secteur des communications. *Livre blanc technique de l'industrie*. 17 juillet 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.
[16] Anthony Scriffignano. Dun & Bradstreet, Inc. *Briefing au sous-comité ICR du NSTAC*. 15 août 2017.
[17] Arrabelle Hallawell. Arbor Networks, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 3 août 2017.
[18] Bill O'Hern. AT&T, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 20 juillet 2017.
[19] Anthony Scriffignano. Dun & Bradstreet, Inc. *Briefing au sous-comité ICR du NSTAC*. 15 août 2017.
[20] Ann Cox. DHS. *Briefing au sous-comité ICR du NSTAC*. Le 1er août 2017.
[21] Anthony Scriffignano. Dun & Bradstreet, Inc. *Briefing au sous-comité ICR du NSTAC*. 15 août 2017.

2.3 Les réseaux de zombies et les attaques distribuées automatisées sont mondiaux, ce qui rend la réponse complexe

Les dispositifs infectés, les cibles, les mauvais acteurs et les victimes sont répartis dans le monde entier. Les mauvais acteurs sont des États-nations, des groupes criminels organisés, des hacktivistes et des particuliers. L'état de droit a peu d'impact, et la capacité des délinquants à couvrir leurs traces complique l'attribution. Les acteurs malveillants sont généralement motivés par le gain financier ou la possibilité de provoquer une perturbation des services. Il existe des cibles dans le secteur des soins de santé, le monde universitaire et le secteur public ; les victimes aux États-Unis sont plus susceptibles de payer une rançon23. [23]

Plus de 80 % du trafic des botnets provient de l'étranger et la plupart du trafic est conçu pour avoir l'air légitime. La Chine possède le plus grand nombre de botnets, avec près de 1,4 million. L'Inde est deuxième avec moins d'un million et la Russie est troisième avec moins de 600 000.[24] Au premier trimestre 2017, la Chine et la Corée du Sud "ont continué à être en tête de la liste des pays attaquants... La plupart des attaques (50,8 %) provenaient de Chine, suivie de la Corée du Sud (10,8 %)" et des États-Unis (7,2 %). "[25] La plupart des résolveurs DNS ouverts utilisés dans les attaques se trouvent en dehors des États-Unis. [26]

Figure 4. Emplacement des résolveurs DNS



Source : Bill O'Hern. AT&T. Briefing au sous-comité de la résilience de l'Internet et des communications (ICR) du NSTAC. 20 juillet 2017

[22] Ibid.
[23] Raj Samani. McAfee, Royaume-Uni. *Briefing au sous-comité ICR du NSTAC*. 15 août 2017.
[24] Projet Spamhaus. *Les pires pays du monde en matière de botnets*. 18 août 2017. https://www.spamhaus.org/statistics/botnet-cc/.
[25] Incapsula. *Global DDoS Threat Landscape (paysage mondial des menaces DDoS)*. 2017. https://www.incapsula.com/ddos-report/ddos-report-q1- 2017.html.
[26] Bill O'Hern. AT&T, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 20 juillet 2017.

En octobre 2016, le botnet Mirai a lancé une attaque DDoS contre le fournisseur de services DNS Dyn. L'attaque a perturbé certains des plus grands sites web du monde. Mirai exploite la faiblesse de la sécurité de nombreux appareils IoT, en recherchant en permanence les appareils IoT accessibles sur Internet qui ne sont protégés que par les paramètres d'usine par défaut et contiennent des noms d'utilisateur et des mots de passe codés en dur. Mirai infecte les appareils avec des logiciels malveillants et les oblige à se rapporter à un serveur de contrôle central, les transformant en bots pouvant être utilisés dans des attaques DDoS. [27] Un nombre relativement faible de fabricants et leurs fournisseurs en aval sont connus pour avoir développé des dispositifs IoT vulnérables.

L'industrie travaille en interne et avec les forces de l'ordre pour fermer les hôtes des botnets, mais la collaboration est difficile lorsqu'elle se déroule au-delà des frontières politiques. Le gouvernement américain dispose d'autorités et d'outils qui pourraient lui permettre de prendre des mesures affirmatives (offensives et défensives) contre les botnets, mais l'utilisation de ces outils soulève des problèmes de politique. Des questions complexes se posent autour de la "défense active" et des cyberopérations offensives, notamment ce qui devrait être mené, comment améliorer la prévisibilité des effets (car l'une des principales raisons de la retenue est le manque de prévisibilité/précision des impacts), et qui devrait être impliqué. Ces questions nécessitent une discussion et une planification conjointes entre le gouvernement américain, les partenaires étrangers et l'industrie. La "défense active" a des significations différentes selon les contextes, et une discussion plus approfondie est nécessaire.

3.0 CHAQUE PARTIE DE L'ÉCOSYSTÈME DOIT ABORDER LA SÉCURITÉ

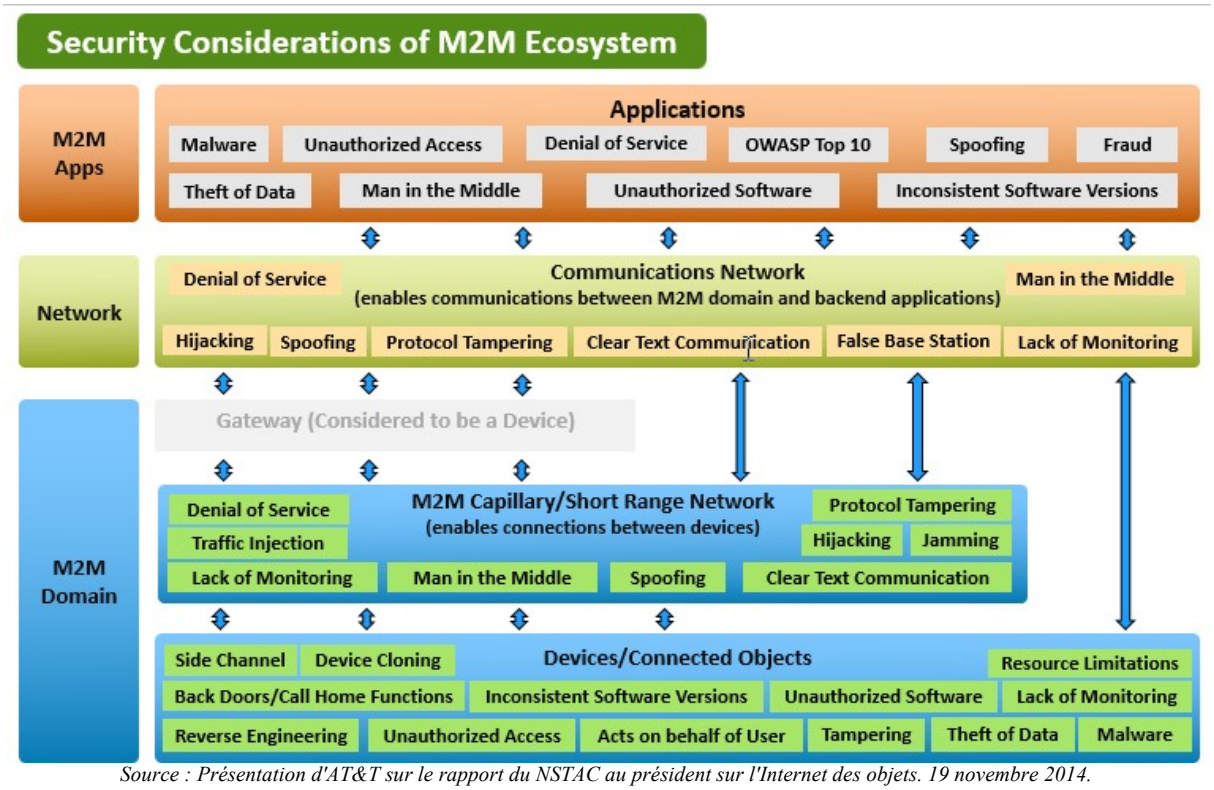
Aux fins du présent rapport, le NSTAC a divisé l'écosystème en couches :

- Réseau (3.1)
- Consommateurs/Bordures/Dispositifs (3.2)
- Entreprise (3.3)
- Applications/logiciels/OS (3.4)
- Gouvernement (3,5)
- International (3,6)

La cybersécurité exige des mesures énergiques dans chaque partie de l'écosystème.

[27] Symantec. *Mirai : Ce que vous devez savoir sur le botnet à l'origine des récentes attaques DDoS majeures*. 27 octobre 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent- major-ddos-attacks.

Figure 5. Considérations relatives à la sécurité de l'écosystème M2M



Source : Présentation d'AT&T sur le rapport du NSTAC au président sur l'Internet des objets. 19 novembre 2014.

LES PRINCIPALES CONCLUSIONS RELATIVES À CHAQUE COUCHE DE L'ÉCOSYSTÈME

Plusieurs mesures permettront de sécuriser l'écosystème Internet contre les attaques distribuées et automatisées. Différents acteurs doivent contribuer - individuellement et collectivement - à créer une meilleure sécurité. Ce rapport se concentre sur les acteurs clés et leur rôle dans le renforcement de la sécurité de l'internet.

Couche réseau. Les fournisseurs de services réseau ont mis en place une série de pratiques communes pour atténuer les attaques distribuées. Ces pratiques comprennent les pratiques communes DDoS des fournisseurs de services réseau, le code de conduite anti-botnet (ABC) pour les ISP, le BCP de l'Internet Engineering Technical Forum (IETF) et les méthodes du Communications Security, Reliability and Interoperability Council (CSRIC) de la Federal Communications Commission (FCC). Le secteur des communications a élaboré des pratiques au sein du CSRIC28 de la FCC sur de nombreuses questions, notamment les meilleures pratiques en matière de DDoS, l'atténuation des botnets et la mise en œuvre du *cadre du* NIST *pour l'amélioration de la cybersécurité des infrastructures critiques*. De nombreux fournisseurs ont mis en œuvre ces pratiques, mais d'autres FAI nationaux et internationaux, et ceux qui exploitent des réseaux

[28] Le CSRIC et l'organisation qui l'a précédé, le Conseil de fiabilité et d'interopérabilité des réseaux (NRIC) ont d'abord abordé les meilleures pratiques de cybersécurité dans NRIC VI de 2002 à 2004. Voir https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-4.

29 doivent également les adopter pour réduire l'impact des attaques distribuées. Le rapport du CSRIC recommande notamment de bloquer le trafic à destination et en provenance de certains ports Internet, d'améliorer les renseignements sur le réseau et la visibilité des flux de trafic, de filtrer le trafic en transit entre les fournisseurs d'accès Internet en cas d'attaque à grande échelle et d'appliquer l'apprentissage automatique à la détection des réseaux de zombies.

Les fournisseurs de services réseau peuvent également contribuer à sécuriser les dispositifs IoT connectés à leurs réseaux ; par exemple, les opérateurs de téléphonie mobile peuvent offrir des services pour aider à gérer la sécurité des dispositifs IoT connectés aux réseaux Long Term Evolution ou Fifth Generation (5G) en partenariat avec divers autres acteurs de l'écosystème. Par exemple, AT&T, IBM, Nokia, Palo Alto Networks, Symantec et Trustonic ont récemment formé une alliance pour la cybersécurité de l'IdO, dont l'objectif est de favoriser la collaboration entre les entreprises membres afin de développer des solutions à plusieurs niveaux pour relever les défis de la cybersécurité de l'IdO. Les fournisseurs de réseaux développent actuellement des capacités au niveau de la couche réseau en tirant parti de l'analyse des données massives et de l'apprentissage automatique pour détecter et atténuer les attaques basées sur l'IdO, et ils continueront probablement à introduire de nouvelles capacités et de nouveaux services pour aider à mieux gérer les dispositifs IdO.

Couche périphérique/de pointe. La sécurité des dispositifs doit être améliorée car l'arsenalisation des dispositifs et leur utilisation potentielle dans des attaques DDoS reste un problème majeur. Alors que de nombreuses activités privées sont en cours, le gouvernement devrait réunir les parties prenantes pour favoriser l'adoption de normes et de meilleures pratiques. Le secteur privé devrait diriger l'élaboration des normes, et le gouvernement peut réunir des experts pour démontrer comment ces normes peuvent être appliquées grâce à des cas d'utilisation. Au fur et à mesure de l'émergence des meilleures pratiques, l'écosystème pourrait envisager des certifications de dispositifs volontaires, dirigées par l'industrie, qui incluraient également le soutien du fabricant pour le cycle de vie du produit. Le NSTAC a précédemment recommandé "d'envisager la création d'un Underwriters Lab (UL) pour la certification de politiques spécifiques en matière de valeurs mobilières".[31] Le NSTAC soutient la conclusion selon laquelle une certaine forme de certification des dispositifs IoT par l'industrie, basée sur des normes internationales, serait utile.

Dans une certaine mesure, cet effort est déjà en cours. UL développe un programme de certification des appareils et d'autres organisations telles que le Cybersecurity Independent Testing Laboratory32 (CITL) testent des appareils. Consumer Reports a commencé à collaborer avec des entités, dont le CITL, pour prendre en compte la sécurité dans les évaluations des appareils, ce qui pourrait sensibiliser les consommateurs. En outre, le gouvernement a lancé des processus, tels que les travaux de la NTIA sur l'évolutivité des dispositifs IoT et les efforts du NIST en matière de systèmes cyber-physiques. Le gouvernement et l'industrie peuvent favoriser l'adoption en exigeant que les appareils répondent à des critères de déploiement dans des environnements propriétaires. Un cadre pour

[29] Alors que les pratiques communes telles que le BCP 38/84 sont largement discutées en relation avec les ISP, la technologie anti-spoofing doit être déployée par toute personne exploitant son propre espace d'adresses IP, y compris les entreprises et autres entités qui fournissent certaines de leurs propres fonctionnalités de réseau.

[30] Voir Matt Tooley, NCTA - The Internet & Television Association, Communications Sector Coordinating Council, *Livre blanc technique de l'industrie sur les botnets et les menaces automatisées*.

[31] NSTAC. *Rapport du NSTAC au président sur l'Internet des objets*. 9 novembre 2014. https://www.dhs.gov/sites/default/files/publications/2012-05-15-NSTAC-Cloud-Computing.pdf, annexe E, E-5. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[32] Cyber Independent Testing Lab (CITL). http://cyber-itl.org/.

Le cadre de déploiement des dispositifs, élaboré dans le cadre d'une collaboration public-privé, devrait recommander des processus de gestion des risques et confirmer que les besoins diffèrent en fonction de la fonctionnalité et du contexte. Le gouvernement devrait s'inspirer du *Framework for Improving Cybersecurity for Critical Infrastructure33* du NIST. De nouveaux services sont continuellement mis en place pour faciliter la gestion et la sécurisation des dispositifs IoT. Les FAI, les fournisseurs de services sans fil, les fabricants de routeurs, les fournisseurs de solutions de sécurité et autres développent des services pour gérer la sécurité des dispositifs IoT. Comme indiqué précédemment, les opérateurs sans fil collaborent également avec diverses entités pour mettre sur le marché des solutions permettant de gérer la sécurité de l'IdO. Des sociétés d'antivirus et de sécurité telles que McAfee et Symantec proposent également des services de sécurité à domicile. [34] Cisco promeut des normes au sein de l'IETF, telles que la norme MUD (Manufacturer Usage Description), qui permet aux appareils de s'identifier dans la maison et peut permettre aux routeurs et aux réseaux d'appliquer une politique de sécurité à l'encontre de l'appareil. Il s'agit de capacités encore émergentes qui pourraient compléter les normes de sécurité des appareils.

Entreprise. Les entreprises doivent planifier et gérer les appareils connectés pendant leur acquisition, leur utilisation et leur fin de vie. Ces organisations comptent de nombreux utilisateurs qui peuvent être vulnérables à des exploits non sophistiqués, mais qui peuvent aussi grandement bénéficier d'une éducation à la sécurité. Les entreprises doivent également adopter les meilleures pratiques pour assurer la redondance et la résilience des réseaux, des données (comme les sauvegardes pour se protéger contre les ransomwares), des offres de services en nuage et du DNS. Les entreprises jouent un rôle clé dans la gestion de leur environnement en adoptant et en exigeant des mesures de sécurité de la part de leurs fournisseurs, et cette approche peut conduire à de meilleures normes de sécurité IoT dans l'ensemble de l'écosystème Internet.

Applications/Software/OS (voir *section 3.4*). L'écosystème exige un recours accru aux pratiques de développement et de gestion de logiciels sécurisés. Comme l'explique le NIST, "[i]l existe de nombreuses approches, à différents niveaux de maturité, qui sont très prometteuses pour réduire le nombre de vulnérabilités dans les logiciels". [35] Toutefois, l'utilisation des pratiques de développement et de gestion de logiciels sécurisés est inégale, en particulier chez les fournisseurs de technologies plus petits ou non traditionnels, disposant de moins de ressources et de moins d'expertise. L'industrie et le gouvernement doivent promouvoir les meilleures pratiques, soutenir les développeurs dans les start-ups et mettre en avant une communication efficace entre les ingénieurs logiciels et les experts en sécurité.

3.1 Réseaux

CONSTATATIONS

Les réseaux jouent un rôle essentiel dans la défense contre les botnets et les attaques DDoS. Les fournisseurs de réseaux prennent diverses mesures, mais il est possible de faire davantage pour lutter contre les botnets et les attaques DDoS.
Un défi majeur consiste à encourager l'adoption des meilleures pratiques existantes. Le NSTAC a identifié les techniques suivantes employées et les défis rencontrés par l'industrie, et a élaboré des recommandations pour résoudre ces problèmes.

[33] Institut national des normes et de la technologie (NIST). *Cadre pour l'amélioration de la cybersécurité des infrastructures critiques*. 12 février 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cyb ersecurity-framework-021214.pdf.
[34] Par exemple, voir la Plateforme sécurisée pour la maison de McAfee https://securehomeplatform.mcafee.com.
[35] Publication du NIST ITL. Janvier 2017. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922589.

Activités actuelles

Les opérateurs de réseaux atténuent chaque jour des milliers de menaces, de botnets et d'attaques DDoS, en utilisant des outils en constante évolution et d'énormes ressources pour fournir à leurs clients et aux autres utilisateurs finaux une connectivité sécurisée. Par exemple, les fournisseurs mettent en œuvre des normes pour la lutte contre l'usurpation d'identité, bloquent les vecteurs d'attaque, et détectent et atténuent les attaques qui ciblent ou affectent le service réseau. Les fournisseurs de services aident à identifier les adresses IP sources, à filtrer/bloquer les courriels qui correspondent aux signatures des listes noires et à filtrer/bloquer le trafic destiné aux sites de phishing. Voici quelques-unes des techniques de sécurité réseau employées par les FAI :

- **Meilleure pratique commune (BCP)38.** Les principaux opérateurs mettent en œuvre la BCP38 dans au moins une partie de leurs réseaux. BCP38 est une pratique de l'IETF inventée pour empêcher l'usurpation d'adresse IP et empêcher les utilisateurs finaux d'initier du trafic avec une adresse source usurpée. La mise en œuvre de BCP38 augmente la probabilité que le trafic des botnets soit bloqué parce qu'il provient d'une adresse source falsifiée, ou qu'il soit traçable afin que l'opérateur puisse remédier à une faille de sécurité une fois celle-ci identifiée. La plupart des grands FAI intègrent BCP38, et un nombre croissant de petits FAI commencent à l'adopter également.

- **Blocage, filtrage et limitation du débit des ports.** De nombreux opérateurs mettent en œuvre le blocage, le filtrage et la limitation du débit des ports. Ces techniques sont largement utilisées dans les services de sécurité gérés pour les entreprises et les administrations. Les fournisseurs de services bloquent également certains ports sur leurs dorsales qui sont connus pour contribuer aux risques de sécurité. Si le blocage de ports est aujourd'hui pratiqué dans une certaine mesure, le calcul des risques est différent selon que l'on bloque ou que l'on bloque le trafic sur le réseau d'une entreprise ou sur l'Internet public. Les FAI sont préoccupés par les faux positifs en ce qui concerne le blocage à l'échelle de l'Internet, et les modèles de blocage ou de filtrage plus agressifs peuvent ne pas s'étendre. Le NSTAC reconnaît qu'il y a peut-être une possibilité d'améliorer ces efforts, mais cela nécessiterait un partenariat avec le gouvernement pour développer un cadre politique soutenant les ISP qui prennent des mesures plus agressives pour bloquer et filtrer le contenu. Les FAI sont nécessairement conservateurs sur ces questions, étant donné le potentiel de faux positifs et l'incertitude de l'environnement réglementaire, notamment en raison des réglementations de la FCC sur la neutralité des réseaux. En outre, de nombreux sites de commandement et de contrôle utilisent des moyens de communication légitimes qui peuvent entraîner des dommages collatéraux. Les FAI bloquent déjà des ports qui sont largement utilisés lors d'événements de sécurité. AT&T, par exemple, tente d'isoler la menace et de minimiser les dommages au réseau en bloquant certains ports qui transfèrent du trafic malveillant ou perturbateur, comme les ports 25, 135, 139, 445 et 1900.[36] D'autres fournisseurs prennent des mesures similaires. Les fournisseurs limitent également le débit du trafic pour certains protocoles dont l'utilisation est nominale ou limitée, ou qui consomment normalement de petites quantités de bande passante (par exemple, CharGen ou NTP), ce qui permet l'utilisation normale de ces protocoles, mais contribue à atténuer leur utilisation dans les attaques DDoS. Tout effort visant à étendre ces activités au-delà des exemples ci-dessus qui sont clairement exploités dans les cyberattaques nécessiterait une collaboration avec le gouvernement pour s'assurer qu'un cadre politique est établi pour soutenir ces activités.

[36] Voir AT&T. *Pratiques de réseau*. 24 avril 2017. https://www.att.com/gen/public-affairs?pid=20879 ; Xfinity. *Liste des ports bloqués de Comcast*. 2017. https://www.xfinity.com/support/internet/list-of-blocked-ports/. CenturyLink http://www.centurylink.com/aboutus/legal/internet-service-disclosure/full-version.html

- **Cadre de cybersécurité du NIST**. L'industrie encourage l'utilisation du *cadre du* NIST *pour l'amélioration de la cybersécurité des infrastructures critiques*, en mettant en œuvre le cadre dans chaque domaine fonctionnel essentiel identifié par le NIST :

  - *Identifier* : identification des actifs critiques, partage de l'information.

  - *Détection* : échantillonnage de paquets, analyse de signatures, analyse heuristique/comportementale.

  - *Protection* : listes de contrôle d'accès, contrôle de l'activité, trous noirs et trous d'évacuation, épurateurs DDoS, spécification des flux du protocole BGP (Border Gateway Protocol), réseaux de diffusion de contenu, anycast, logiciels antivirus pour l'utilisateur final, services de sécurité gérés pour les clients.

  - *Réagir et récupérer* : atténuer le trafic d'attaque, travailler avec les fournisseurs en amont pour filtrer, et informer les clients. Les FAI bloquent les ports qui sont utilisés dans les attaques en cours (par exemple, le port 445).
- **ABC pour les FAI.** L'industrie encourage l'adoption du code de conduite anti-bot américain pour les fournisseurs de services Internet, élaboré par le groupe de travail 7 du CSRIC III. L'ABC est un ensemble de pratiques volontaires qui "abordent la menace des bots et des botnets dans les réseaux résidentiels à large bande par une participation volontaire". Il met l'accent sur dix principes clés : participation volontaire, neutralité technologique, neutralité de l'approche, respect de la vie privée, conformité juridique, responsabilité partagée, durabilité, partage des informations, efficacité et communication efficace avec les consommateurs. La conformité à l'ABC exige l'éducation de l'utilisateur final, la détection des botnets, la notification à l'utilisateur final d'une infection potentielle par un botnet, l'élimination des botnets et la collaboration des FAI. Les obstacles potentiels à la mise en œuvre comprennent : les limites technologiques (les solutions actuelles peuvent être insuffisantes pour éliminer les menaces des botnets et/ou avoir des conséquences inattendues) ; les obstacles liés aux consommateurs et au marché (les solutions peuvent être considérées par les clients comme inefficaces ou indésirables, comme l'augmentation des coûts pour les consommateurs) ; les obstacles opérationnels (impact sur la mission principale et les ressources de l'organisation) ; les obstacles financiers (difficulté à quantifier les coûts/avantages associés à des recommandations spécifiques) ; et les obstacles juridiques, réglementaires ou politiques (lois ou politiques qui découragent la collaboration et le partage d'informations).

- **Gestion du trafic**. Les FAI et les opérateurs réseau investissent massivement dans des capacités de gestion du trafic. Parmi les exemples, citons le blocage des ports, l'apprentissage automatique et l'IA pour aider à détecter les bots, le filtrage des trous noirs de destination et le sinkholing des adresses IP malveillantes.

- **Notification des consommateurs**. Les FAI consacrent beaucoup de temps et de ressources à la notification des consommateurs en cas d'infection, ce qui est un élément clé des principes de l'ABC. D'après les données globales fournies volontairement et confidentiellement au Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), les FAI déclarants ont notifié entre 98,41 % et 99,13 % des clients infectés par des robots en 2012 et entre 94 % et 99,82 % des clients infectés par des robots en 2013. Mais, comme décrit ci-dessous, l'utilité de l'éducation des consommateurs a des limites, et l'impact de ces efforts sur la réduction de la prolifération des logiciels malveillants et des botnets est incertain.

- **Collaboration de l'industrie**. L'industrie s'engage dans la collaboration et le partage des meilleures pratiques. Par exemple, l'industrie, sous la direction de l'IETF, explore des solutions de collaboration.

Comme la signalisation des menaces ouvertes DDoS. Les participants collaborent pour identifier les attaques contre leurs serveurs et partagent des informations pour élaborer des réponses aux menaces avant qu'une attaque ne se produise contre d'autres réseaux. L'échange en temps réel de télémétrie entre les plateformes d'atténuation des DDoS facilite l'atténuation des DDoS et les mises à jour de l'état des réseaux entre eux. Le récent rapport du groupe de travail CSRIC V de la FCC sur le partage des informations donne un aperçu détaillé du partage des informations dans le secteur des communications. D'autres efforts sont en cours, notamment un projet pilote entre les principaux transporteurs pour coopérer et perturber le flux de trafic lors d'une attaque DDoS à grande échelle au niveau de leurs principaux points d'échange de trafic.

- **Partage d'informations.** L'industrie s'engage dans le partage d'informations comme le souligne un récent rapport du groupe de travail 5 du CSRIC V de la FCC. [37] L'industrie partage des informations avec des pairs de confiance et des partenaires commerciaux, des agences gouvernementales sous contrat, des forces de l'ordre, des pairs de l'industrie dans le cadre du processus de politique et de planification du secteur, et des agences gouvernementales telles que le centre de coordination national du DHS et le centre national d'intégration de la cybersécurité et des communications (NCCIC). [38] Le DHS gère également le réseau international de veille et d'alerte en partenariat avec le département d'État afin de partager les informations au niveau international.

- **Réseaux définis par logiciel/répartition en tranches du réseau/virtualisation.** Les développements architecturaux, tels que la 5G, la transition vers les réseaux tout-IP, et l'émergence des réseaux définis par logiciel (SDN) et de la virtualisation, favoriseront la sécurité. SDN est une architecture émergente qui découple les fonctions de contrôle du réseau et d'acheminement, permettant au contrôle du réseau de devenir directement programmable. Cette architecture, associée à des interfaces ouvertes et facilement programmables, permet de combiner plus facilement les solutions de différents fournisseurs et de développer de nouvelles capacités. Bien que toute nouvelle approche ait le potentiel d'être compromise, SDN aidera les opérateurs à répondre aux menaces en raison de la vue centrale qu'ils ont du réseau. Le découpage en tranches du réseau permettra aux opérateurs de réseaux 5G de fournir des réseaux sur la base d'un service. Avec le découpage du réseau, une seule couche physique peut être divisée en plusieurs réseaux virtuels, ce qui permet aux opérateurs de prendre en charge différents services pour différents clients. Ces services comprennent le filtrage, le routage, la limitation des protocoles et la limitation du débit. Les opérateurs peuvent personnaliser la sécurité des tranches de réseau afin de répondre de manière dynamique. La virtualisation de réseau comprend une sécurité intégrée, comme l'isolation et la multilocation, la segmentation, le pare-feu de distribution, l'insertion et le chaînage de services. [39]

- **Services de sécurité gérés/sécurité des consommateurs.** De nombreux FAI proposent des services de sécurité gérés, tels que des services de défense contre les attaques DDoS, aux entreprises clientes et aux consommateurs pour les aider à gérer les risques de sécurité. Du côté des consommateurs, les FAI proposent, entre autres, des notifications d'infections potentielles, un service antivirus gratuit fourni avec le service haut débit résidentiel et un support technique pour aider à y remédier. Au niveau des entreprises, les FAI offrent des services de sécurité, de surveillance et de gestion des réseaux aux secteurs privé et public.

[37] FCC CSRIC V, Working Group 5 Final Report, *Information Sharing,* 15 mars 2017. https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.
[38] Ibid, page 6.
[39] Bill O'Hern. AT&T, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 20 juillet 2017.

Défis

Ces solutions existantes posent plusieurs problèmes :

- **Cadre juridique de la gestion des réseaux.** De nombreuses techniques destinées à l'Internet public ou à l'espace grand public font appel à des solutions telles que le blocage, le black holing ou le sinkholing des adresses IP, le blocage des ports utilisés pour le trafic malveillant, la notification des infections potentielles aux utilisateurs finaux et le déploiement de pratiques courantes de lutte contre l'usurpation d'adresses IP telles que le BCP 38/84. L'un des défis de ces approches est le potentiel de faux positifs et de conséquences involontaires. Pour remédier efficacement à ces problèmes, les FAI devraient prendre des mesures plus agressives en matière de surveillance et d'inspection du trafic, ce qui soulève des problèmes de politique. Par exemple, bien qu'il y ait une exception de sécurité dans les règles antérieures de neutralité du Net de la FCC, l'attente générale que les FAI n'interfèrent pas dans le flux de trafic augmente les risques liés à certaines activités.

- Le **cryptage**. Les FAI perdent de la visibilité car le trafic est de plus en plus crypté. Aujourd'hui, la plupart du trafic sur Internet est crypté. Et c'est une affaire simple pour les opérateurs de botnet de crypter le trafic de ces derniers. Un expert a prédit que d'ici à la fin de 2016, plus des deux tiers du trafic sur Internet seraient cryptés. [40] Si les FAI peuvent avoir une certaine visibilité sur les données de flux net, telles que l'adresse IP source et destination, il est peu probable qu'ils aient une large visibilité sur la charge utile qui pourrait être nécessaire pour un blocage agressif.

- **Protocole Internet version 6 (IPv6).** Les opérateurs exploitant des réseaux IPv6 ont besoin d'outils de sécurité, de détection et de surveillance. En raison des défis uniques en matière de sécurité que pose l'IPv6, l'écosystème doit faire évoluer la prise en charge de la sécurité pour l'IPv6, améliorer les outils de détection et de découverte des actifs afin d'identifier les dispositifs IPv6 malveillants, et veiller à ce que la surveillance du réseau prenne en charge les actifs des réseaux IP version 4 et IPv6.

- **Évolutivité.** Des questions persistent quant à l'efficacité des solutions à grande échelle. Dans les entreprises, les FAI surveillent les plages d'adresses IP correspondant à leurs clients professionnels pour identifier, détecter et contrecarrer les cyberattaques. Il n'est pas certain que des solutions plus granulaires pour l'ensemble de l'Internet puissent être mises à l'échelle, car les grands réseaux acheminent d'énormes quantités de trafic chaque jour. [41]

- **Transporteurs de petite/moyenne taille**. Il faut faire une distinction entre les grandes et les petites entreprises et leurs capacités à mettre en œuvre le BCP38 ou d'autres mesures de sécurité. Les petites entreprises peuvent avoir besoin du financement du service universel pour une sécurité efficace. Les entreprises qui vendent des services Internet à faible marge et qui ne disposent pas de modèles de revenus pour couvrir les investissements en matière de sécurité sont confrontées à des défis importants. Le NSTAC recommande au gouvernement de réexaminer la question des incitations au déploiement, en particulier pour les petites et moyennes entreprises où même un investissement marginal peut nécessiter des incitations pour ces entités.

- **Notifications aux consommateurs**. De nombreux FAI ont des programmes de notification, mais l'efficacité globale de ces programmes est inconnue. Même lorsque les consommateurs reçoivent une notification d'un

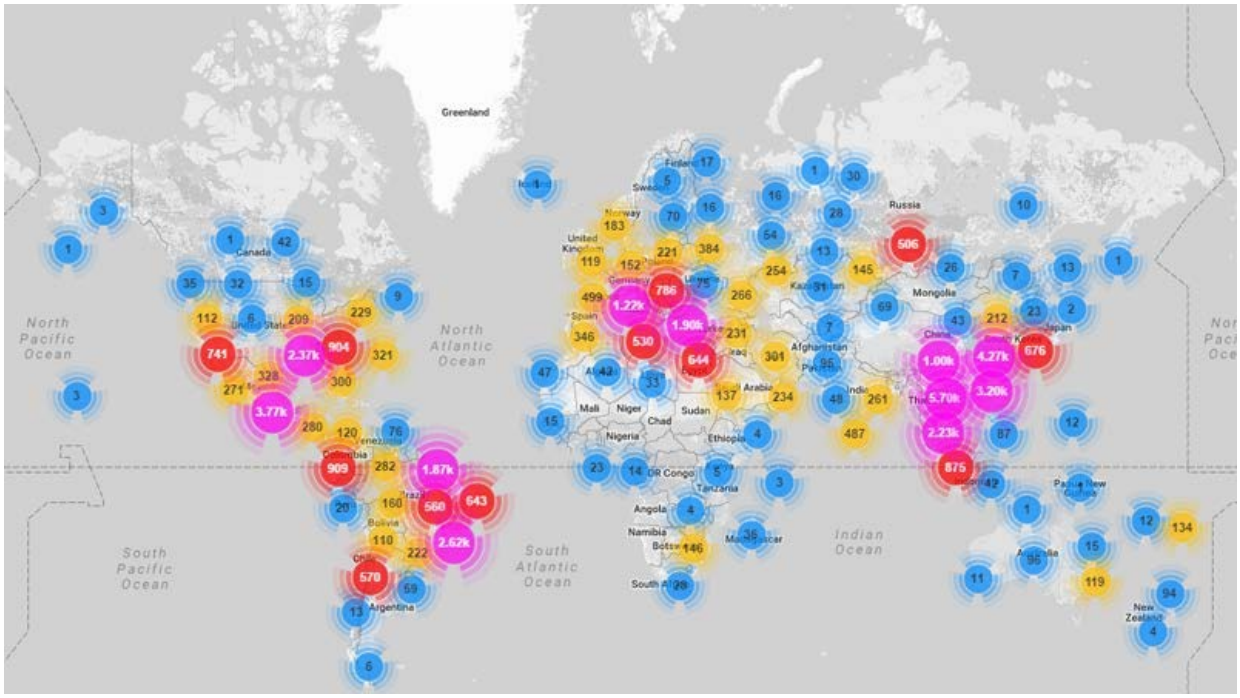
[40] Sandvine. *Phénomènes mondiaux de l'Internet : Le trafic Internet crypté*. 2016. https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

[41] Bill O'Hern. AT&T, Inc. *Briefing au sous-comité ICR du NSTAC*. 20 juillet 2017. Par exemple, plus de 168 pétaoctets transitent quotidiennement sur le réseau d'AT&T.

de sécurité, beaucoup n'ont pas les compétences nécessaires pour nettoyer leur système. Il existe également un taux élevé de réinfection, car les consommateurs répètent souvent le comportement qui a corrompu leur appareil en premier lieu.

- **International**. Les attaques de botnet contre les États-Unis proviennent en grande partie de l'étranger. Par exemple, la carte suivante montre les sources de trafic d'une attaque de botnet Mirai le 17 août 2016, qui se trouvaient principalement en dehors des États-Unis.

Figure 6. Sources de trafic pour une attaque du botnet Mirai 17 août 2016



Source : Brian Rexroad. AT&T. Briefing au sous-comité ICR du NSTAC. Le 20 juillet 2017.

Autres questions

Le NSTAC a abordé d'autres questions concernant la sécurité des FAI, notamment le déploiement des extensions de sécurité DNS (DNSSEC) et le routage interdomaines sécurisé. Le DNSSEC n'est peut-être pas une solution viable, car il était utile au départ, mais au fur et à mesure de l'évolution du réseau, le DNSSEC n'a pas été mis en œuvre de manière optimale, ce qui a diminué son efficacité. Les FAI sont confrontés à des attaques par amplification, notant que plusieurs cadres de sécurité reposent sur l'infrastructure et la validation des clés. Le contrôle d'admission au réseau et la protection de l'accès permettent de faire respecter la validation avant l'accès au réseau. Le problème majeur est la confiance et la réputation, car chaque paquet sur le réseau comporte un certain degré de risque.

Le NSTAC a également examiné les questions relatives au système de signalisation 7 (SS7). [42] Bien que le SS7 ait fait l'objet d'une attention considérable, il n'est pas en soi le problème. Ce sont plutôt l'interconnexion et l'accès inapproprié qui sont en cause. (Voir CSRIC V, WG10 (mars 2017) et le rapport du 3 mai 2017 sur SS7/2FA). L'industrie continue de lutter contre les opérateurs malhonnêtes qui sont complices de comportements criminels,

[42] Travis Russell. Oracle. *Briefing au sous-comité ICR du NSTAC.* Le 11 août 2017.

la vente d'identifiants de réseau et d'authentification à de mauvais acteurs. L'industrie s'efforce de renforcer la vérification des partenaires d'interconnexion (ou d'itinérance) et d'améliorer l'hygiène des réseaux.

Un autre problème est la sécurisation du routage BGP. Il s'agit notamment des préoccupations relatives aux entités publiant de fausses routes sur l'Internet qui peuvent être exploitées pour acheminer le trafic afin de permettre aux entités de surveiller le trafic ou de procéder à d'autres formes de surveillance. Jusqu'à présent, la solution à ce problème a été axée sur le développement d'une infrastructure à clé publique de ressources (RPKI) qui permettrait aux FAI et à d'autres entités de valider les routes. Le NIST National Cybersecurity Center of Excellence (NCCoE) a récemment lancé un projet pilote de routage interdomaine sécurisé afin d'explorer plusieurs questions relatives au développement de la RPKI et de nombreux ISP y participent.

- **Partager des informations exploitables sur les menaces. La** collaboration entre FAI devrait inclure le partage des méthodes de détection, de notification et d'atténuation prévues ou utilisées au sein du réseau.

- **Augmenter l'analyse du trafic.** De nombreux FAI effectuent des analyses, mais celles-ci devraient être intégrées à des services de sécurité gérés plus robustes afin d'aider les entreprises à gérer les attaques DDoS potentielles.

- **Adapter et appliquer l'apprentissage automatique pour la détection des anomalies.**

- **Veiller à ce que les opérateurs de réseau puissent filtrer le trafic malveillant.**

- **Encourager le développement de pratiques permettant d'atténuer le trafic DDoS aussi près de la source que possible pour éviter qu'il ne transite par les réseaux.**

- **Renforcer l'utilisation du BCP38/84 au-delà des FAI pour inclure les entreprises.**

- **Poursuivre la mise en œuvre du blocage des ports, de la limitation du débit et du filtrage, le cas échéant.**

- **Continuer à participer aux efforts de l'industrie pour accroître la sécurité de BGP.**

3.2 Consommateurs/Administration/Dispositifs

CONSTATATIONS

Les faiblesses à la périphérie des réseaux, dans les dispositifs qui se connectent aux réseaux et chez les utilisateurs qui achètent et utilisent des dispositifs sont à l'origine de l'insécurité. Le NSTAC a tenu compte à la fois des consommateurs et des périphériques dans ses recherches.

Les consommateurs jouent un rôle essentiel. L'erreur humaine peut saper les investissements du secteur dans les solutions techniques et logicielles. De nombreuses attaques utilisent encore des méthodes de faible technicité, comme le hameçonnage, et des acteurs malveillants exploitent une mauvaise hygiène informatique pour lancer des attaques par botnet. 70 % des piratages utilisent des informations d'identification perdues, volées ou faibles ; 60 % de tous les logiciels malveillants ont recours à l'escalade des privilèges ou à l'utilisation d'une carte de crédit.

Des informations d'identification volées. [43] Les recommandations du CSRIC de la FCC ont souligné l'importance d'éduquer les utilisateurs finaux sur les mesures de protection, telles que les mots de passe forts, les logiciels anti-virus, les pare-feu et l'acceptation des mises à jour. [44] Le gouvernement dispose de ressources pour éduquer les consommateurs, mais les messages peuvent se perdre dans le grand nombre de pages de conseils, d'avis du Federal Bureau of Investigation (FBI) et d'autres communications qui existent.

Les utilisateurs peuvent ignorer la sécurité lorsqu'ils prennent des décisions d'achat et ne pas installer ou configurer les dispositifs de manière appropriée. Les utilisateurs finaux peuvent ne pas changer les mots de passe, ne pas utiliser les outils de sécurité disponibles et ignorer les mises à jour disponibles. En outre, ils peuvent ne pas effacer les données ou les paramètres personnels des appareils lors de leur remplacement. Les utilisateurs peuvent ne pas disposer de suffisamment d'informations, mais ils peuvent aussi ignorer les informations disponibles. Une enquête menée par le Pew Research Center a révélé que 28 % des personnes interrogées étaient d'accord avec l'idée d'utiliser un dispositif de sécurité. Les propriétaires de smartphones américains n'ont pas sécurisé l'accès à leur appareil avec un simple numéro d'identification personnel à quatre chiffres ou un autre dispositif de sécurité. [45] Bien que la majorité des utilisateurs de smartphones déclarent mettre à jour les applications ou le système d'exploitation de leur appareil, environ 40 % d'entre eux ont dit qu'ils retardaient les mises à jour jusqu'à ce que cela soit pratique. [46] L'étude a révélé que 14 % des utilisateurs de smartphones n'ont jamais mis à jour le système d'exploitation de leur appareil et que 10 % n'ont jamais mis à jour leurs applications. [47] Le manque d'hygiène n'est pas l'apanage des utilisateurs commerciaux - les utilisateurs gouvernementaux doivent également améliorer leur cyber-hygiène. Les agences peuvent être limitées par des contraintes de ressources, et le gouvernement doit tenir compte des coûts de ses besoins futurs en matière de sécurité. L'EO 13800 souligne de manière appropriée l'obligation de rendre compte et la responsabilité des chefs d'agence. [48]

Les appareils sont critiques. De nombreux dispositifs sont développés avec peu de capacités de sécurité, car certains fournisseurs ne prêtent pas suffisamment attention aux questions de sécurité. L'attaque du botnet Mirai a exploité plus d'un million de caméras dont les mots de passe et les informations d'identification étaient faibles. [49] Les appareils peuvent avoir des mots de passe par défaut non modifiables, ce qui les rend facilement exploitables, ou être incapables de prendre en charge les mises à jour, ce qui rend plus difficile la gestion des correctifs en cas de vulnérabilité de sécurité. La Commission fédérale du commerce (FTC) a noté que la sécurité des appareils variera, mais qu'un certain consensus se dégage sur les caractéristiques sensibles50. [50] Avec des prévisions de 28 milliards de d'ici 2021, et 73 % du trafic Internet mondial étant mobile51, les réseaux ou les personnes ne pourront pas, à eux seuls, assurer la sécurité de tous ces dispositifs.

---

[43] Ann Cox. DHS. *Briefing au sous-comité ICR du NSTAC*. Le 2 août 2017.

[44] FCC. CSRIC II, Groupe de travail 2A : Rapport final. *Cyber Security Best Practices*. à 91. Mars 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

[45] Kenneth Olmstead et Aaron Smith. "Les Américains et la cybersécurité". *Rapport du Pew Research Center*, p. 19. 26 janvier 2017. http://assets.pewresearch.org/wpcontent/uploads/sites/14/2017/01/26102016/ Americans-and-Cyber-Security-final.pdf.

[46] Ibid., p. 20.

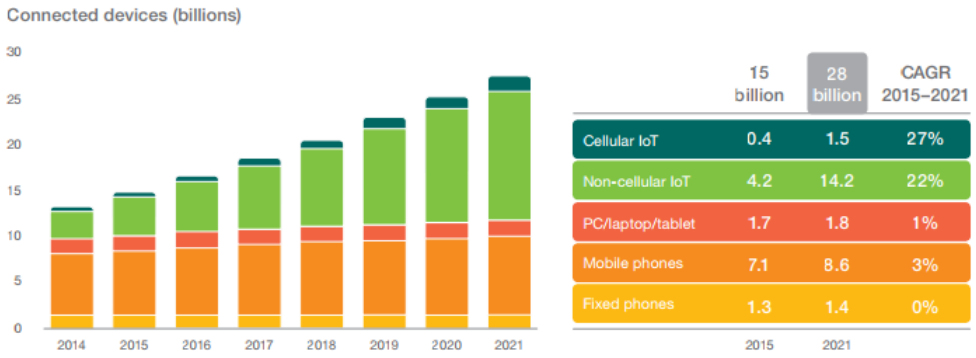
[47] Ibid.

[48] Bureau du secrétaire de presse de la Maison Blanche. *Ordre exécutif 13800, Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques*. 16 mai 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[49] Lorenzo Franceschi-Bicchierai, *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet.* 29 septembre 2016. https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected- cameras-ddos-botnet-brian-krebs.

[50] Thomas B. Pahl. FTC. *Commencer par la sécurité - et s'y tenir*. 28 juillet 2017. https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it ("En matière de sécurité des données, ce qui est raisonnable dépendra de la taille et de la nature de votre entreprise et du type de données que vous traitez.") ; Internet of Les choses : La vie privée et la sécurité dans un monde connecté. FTC. n.130. Janvier 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet- things-privacy/150127iotrpt.pdf (" Il peut y avoir d'autres mesures appropriées, comme les mesures de sécurité qu'une

Figure 7. Croissance des appareils connectés



Source : Rapport sur la mobilité d'Ericsson (juin 2016)[52]

La militarisation des appareils IoT représente un défi de taille. Des appareils mal sécurisés, toujours en service, compromis par des botnets pourraient avoir des conséquences catastrophiques. Les fournisseurs d'IoT et leurs utilisateurs finaux sont parfois apathiques face aux dommages que les appareils vulnérables peuvent causer, et peuvent être peu incités à investir dans la sécurité au-delà de ce qui est nécessaire pour assurer le fonctionnement de l'appareil.

L'IdO doit prendre en charge les mises à jour et un système d'authentification et de validation. [53] De nouveaux protocoles malveillants peuvent déjouer les modèles de sécurité dépassés, de sorte que les anciennes sécurités doivent être mises à niveau. Les fournisseurs de services réseau peuvent être en mesure d'aider à gérer les dispositifs non sécurisés du réseau, mais il existe des facteurs de complication. Par exemple, environ 70 % du trafic Internet dans le monde est crypté, et ce chiffre devrait augmenter. [54] Pour ajouter à la complexité, de nombreux appareils grand public ne sont pas adressables publiquement et fonctionnent derrière des routeurs domestiques et des systèmes de traduction d'adresses réseau qui ne sont pas gérés par les FAI. Les utilisateurs ont souvent plusieurs routeurs. Certaines entreprises, dont les FAI et les fournisseurs de solutions de sécurité, expérimentent des services de gestion de la sécurité, mais le potentiel du marché est incertain.

La sécurité ne se limite pas à la couche des dispositifs. Nous ne pouvons pas compter uniquement sur l'intégration de la sécurité dans les dispositifs pour résoudre le problème de la sécurité. Par exemple, les fournisseurs de réseaux peuvent effectuer des analyses du trafic traversant leurs réseaux et appliquer l'apprentissage automatique pour aider à identifier et à atténuer les menaces qui pèsent sur la sécurité des réseaux.

L'entreprise doit mettre en œuvre des mesures variables, en fonction des risques présentés par un accès non autorisé à l'appareil et de la sensibilité de toute information recueillie").

[51] Rapport Ericsson sur la mobilité. *Au pouls de la société en réseau*. Juin 2016. https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf; Cisco. *Cisco Visual Network Index : Prévisions et méthodologie, 2016-2021.* Livre blanc. Le 7 juin 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/ visual-networking-index-vni/complete-white-paper-c11-481360.html.

[52] Rapport Ericsson sur la mobilité. *Sur le pouls de la société en réseau*. Juin 2016. https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

[53] Raj Samani. McAfee, Royaume-Uni. *Briefing au sous-comité ICR du NSTAC.* Le 15 août 2017.

[54] Voir Sandvine. *Phénomènes Internet mondiaux : Le trafic Internet crypté*. 2016. https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-encryption.html.

Certains dispositifs IoT. Il y a également eu des propositions comme la norme MUD de Cisco, qui est en cours d'introduction à l'IETF. La norme MUD permettrait aux appareils de s'auto-identifier et d'être placés par les routeurs et autres équipements de réseau dans des classes de service distinctes appliquant des limites de débit et des listes blanches pour gérer la sécurité. En outre, des sociétés telles que McAfee commencent à proposer des services de gestion de la sécurité des appareils domestiques. Ces efforts n'en sont qu'à leurs débuts mais peuvent améliorer la sécurité à mesure que le marché évolue.

La chaîne d'approvisionnement est également importante. Les opérateurs améliorent leurs défenses, mais ils ne peuvent pas le faire seuls. Les fabricants de puces et les fournisseurs de plates-formes doivent redoubler d'efforts et l'écosystème doit promouvoir les nouvelles mises à niveau de sécurité "à boulonner" sur les réseaux domestiques. L'industrie et le gouvernement doivent se concentrer sur le marketing de la sécurité, reconnaître le partage des responsabilités et encourager le travail d'équipe.

Le NSTAC reconnaît que les avis divergent sur le rôle du gouvernement dans la sécurité de l'IdO. Il est clair, cependant, qu'il faut se concentrer sur l'atténuation de ces vulnérabilités.

Activités actuelles

De nombreuses innovations sont en cours de développement pour répondre aux besoins de l'utilisateur final et des appareils. Les fabricants de puces et les fournisseurs de plateformes intègrent une sécurité supplémentaire dans les appareils IoT non sophistiqués. [55] Comme l'explique la Consumer Technology Association (CTA) :

- Le Collaborative Research Institute for Secure Computing d'Intel a développé un cadre de sécurité TrustLite pour renforcer la sécurité des petits appareils IoT. [56]

- Les Field Programmable Gate Arrays ou Systems on a Chip d'Altera utilisent une accélération cryptographique matérielle et des mises à jour logicielles à distance sécurisées par AES.

- Les produits IoT d'Analog Devices utilisent l'accélération matérielle de la cryptographie, le démarrage sécurisé et la protection de la lecture de la mémoire en circuit.

- Apple, Qualcomm, Samsung Electronics et d'autres utilisent des puces dotées de la TrustZone d'ARMS.

- Les plateformes IoT d'IBM, de Microsoft, d'Intel, de NXP, de Panasonic et de Samsung disposent d'une sécurité intégrée ou de conseils en matière de sécurité à l'intention des utilisateurs.

Les dispositifs de surveillance du réseau (NMD) et les routeurs intelligents sont de plus en plus répandus. Les NMD grand public contiennent des spécifications qui incluent le mode réseau privé virtuel (VPN), la protection contre les attaques DoS, le blocage des accès non autorisés et l'analyse des virus et des logiciels malveillants. Les routeurs intelligents sont désormais dotés de caractéristiques similaires. L'industrie conçoit du matériel capable de fournir des mises à niveau de sécurité " boulonnées " aux réseaux domestiques des consommateurs.

L'industrie fournit plusieurs outils aux clients pour les aider à protéger leurs appareils. Il s'agit notamment de la fourniture d'outils antivirus aux consommateurs pour les aider à détecter les virus et à nettoyer les machines, de l'analyse des menaces à partir d'un site Web de l'industrie.

[55] Mike Bergman. Consumer Technology Association. *Briefing au sous-comité ICR du NSTAC*. 3 août 2017.
[56] Koeberl, Patrick, et, al. "TrustLite : A Security Architecture for Tiny Embedded Devices". http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

de la perspective du réseau ; la notification des utilisateurs finaux et la fourniture d'outils d'auto-réparation et d'options de prise en charge payante ; et la fourniture d'un service d'atténuation des DDoS pour les clients abonnés.

Il existe des directives volontaires et des bonnes pratiques pour atténuer les vulnérabilités des appareils et sensibiliser les consommateurs, et l'industrie s'appuie également sur ces efforts.

- Le Groupe Spécial Mobile Association (GSMA), par exemple, a élaboré des conseils pour le développement de produits et de services IoT sécurisés, y compris pour les fabricants de dispositifs d'extrémité IoT. [57]

- Le CTA élabore de solides meilleures pratiques pour renforcer la sécurité des appareils connectés à domicile. [58]

L'industrie collabore avec le gouvernement pour fournir des ressources pour la sécurité de l'IdO au stade de l'utilisateur final. Par exemple, les membres du secteur collaborent avec la NTIA dans le cadre d'un processus multipartite visant à développer un lexique commun pour la mise à niveau de l'IdO. Dans le cadre de ce processus, des groupes de travail ont identifié des conseils sur le sujet provenant de plus de 30 organisations américaines et internationales[59], des fonctionnalités pour sécuriser les mises à jour over-the-air et des conseils pour communiquer sur la mise à niveau de l'IdO aux consommateurs.

RECOMMANDATIONS POUR LES CONSOMMATEURS, LA POINTE ET LES APPAREILS

- **Établir et promouvoir des directives consensuelles sur la sécurité des dispositifs**. Les appareils doivent être renforcés par des pratiques de cyber-hygiène de base, notamment la possibilité de recevoir des mises à jour et des correctifs. Plusieurs initiatives gouvernementales visent à améliorer l'hygiène en matière de cybersécurité, mais il faut aller plus loin. [60] Les pouvoirs publics et l'industrie devraient déterminer s'il est nécessaire d'élaborer des attentes minimales en matière de sécurité. Les fabricants de dispositifs, en particulier les fabricants de kits de développement de dispositifs IoT, doivent s'assurer que de bons outils sont inclus et qu'ils utilisent une configuration par défaut sécurisée, des correctifs automatisés et la capacité de récupérer des infections par des logiciels malveillants. [61]

- **Promouvoir les services de gestion domestique**. Le gouvernement devrait soutenir les investissements de l'industrie dans les services de gestion domestique, qui superviseraient le fonctionnement des appareils connectés dans la maison. Cette capacité pourrait être offerte dans les routeurs ou comme un dispositif distinct dans la maison.

  Promouvoir la sensibilisation et l'éducation des consommateurs. L'industrie devrait continuer à éduquer les utilisateurs, notamment sur l'importance de compléter les mises à jour. Le gouvernement devrait amplifier et coordonner ses messages. Il existe des campagnes existantes, telles que STOP.THINK.CONNECT, qui peuvent être utilisées à cette fin.

[57] Voir GSMA IoT Security Guidelines. https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/.

[58] Consumer Technology Association. *Aperçu du projet : Securing Connected Devices for Consumers in the Home*. CTA-CEB33. 7 juillet 2017. https://standards.cta.tech/apps/group_public/project/details.php?project_id=429.

[59] Voir NTIA. *Catalogue des normes de sécurité IoT existantes (version préliminaire 0.01), processus multipartite de la NTIA sur la capacité de mise à niveau et de correction de la sécurité IoT, groupe de travail sur les normes, outils et initiatives existants*. Juillet 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

[60] Arabella Hallawell. Arbor Networks, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 3 août 2017.

[61] Voir le projet de NIST. Publication spéciale 800-193. *Lignes directrices sur la résilience des micrologiciels de plateforme.* Mai 2017. https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

- **Soutenir un meilleur partage de l'information**. Le gouvernement devrait encourager le partage d'informations entre les fabricants de dispositifs, y compris les règles d'exonération et la protection de la responsabilité.

3.3 Entreprise

CONSTATATIONS

Les utilisateurs et les systèmes des entreprises jouent un rôle essentiel. Les entreprises - qu'il s'agisse d'entreprises comptant des centaines de milliers d'appareils, d'organismes gouvernementaux dont les administrés dépendent de la connectivité ou de petites entreprises qui déploient des capteurs industriels et apportent leur propre appareil (BYOD) - sont touchées par les botnets de deux manières. Premièrement, les entreprises sont des cibles d'attaques de botnets. Deuxièmement, les entreprises ont des concentrations d'appareils IoT qui pourraient être exploités dans le cadre d'un botnet mondial s'ils sont laissés vulnérables.

Depuis des années, les adversaires utilisent des attaques DDoS basées sur des botnets pour perturber les opérations des entreprises. Les entreprises peuvent être la cible d'attaques DDoS à cause d'États-nations qui ciblent l'infrastructure américaine, de hacktivistes qui veulent faire une déclaration, de criminels qui veulent détourner l'attention d'attaques plus insidieuses ou d'autres entreprises qui tentent de perturber la concurrence. Au fur et à mesure que l'informatique, les infrastructures physiques et la continuité des activités des entreprises deviennent dépendantes des dispositifs IP, les entreprises deviennent plus sensibles à l'interruption à long terme ou permanente de leurs activités, ce que certains appellent la "destruction de service". Même si les entreprises ne sont pas elles-mêmes la cible de botnets, leurs appareils vulnérables peuvent servir de passerelle pour la pénétration de leurs réseaux, le vol de données de grande valeur, voire la destruction des infrastructures informatiques et opérationnelles de l'intérieur. Les propres appareils IoT d'une entreprise peuvent être utilisés pour lancer une attaque DoS contre l'entreprise elle-même en raison de la prolifération des appareils connectés sur le réseau de presque toutes les entreprises.

Le simple nombre d'appareils rend plus difficile le suivi des appareils par les entreprises, ce qui augmente le risque de vol et rend les appareils vulnérables aux attaques. Les entreprises de toutes tailles doivent gérer davantage de points d'interaction sur leurs réseaux, y compris les VPN, pour faciliter l'accès hors site. Cette augmentation de la connectivité expose les entreprises à des menaces supplémentaires, notamment des menaces provenant d'appareils dont la sécurité n'est pas forcément sophistiquée. Les besoins en matière d'approvisionnement, de surveillance, de mise à jour et de gestion de la fin de vie peuvent représenter un défi plus important que ce que les départements informatiques des entreprises existantes peuvent gérer.

La menace des botnets pour les entreprises va au-delà des attaques sur les appareils. Un défi majeur est la protection contre les attaques sur les ressources partagées que l'entreprise utilise pour mener ses activités. Comme les services des entreprises couvrent leur réseau informatique interne, les offres en nuage et les ressources partagées, elles doivent se protéger contre un incident ayant un impact sur l'activité de l'un de ces services. Par exemple, la présence sur Internet de nombreuses entreprises a été mise hors ligne lorsque leurs services DNS ont été arrêtés lors de l'attaque Mirai d'octobre 2016 contre Dyn.

Les entreprises peuvent jouer un rôle important dans l'atténuation des menaces liées aux botnets. Les déploiements IoT des entreprises au sein des réseaux internes devraient être plus faciles à gérer grâce à l'application de technologies de sécurité appropriées, proportionnelles aux risques identifiés. Pour réduire le risque pour l'entreprise, ces capacités de sécurité doivent être fournies de manière cohérente tout au long de la chaîne de valeur de l'IdO afin de permettre à l'entreprise d'atteindre les objectifs suivants

La visibilité et l'automatisation nécessaires aux entreprises pour empêcher les cybermenaces de cibler les éléments connectés, et protéger les réseaux et les environnements de contrôle des attaques lancées par les dispositifs. Ces capacités doivent être intégrées de manière native, avec des niveaux élevés d'automatisation entre les fonctions pour identifier rapidement les attaques avancées et garantir que les contrôles de sécurité préventifs peuvent être appliqués dans tous les environnements en temps quasi réel. Dans le contexte des déploiements IoT, la prévention des cybermenaces sur l'ensemble de la chaîne de valeur IoT de l'entreprise nécessite au minimum : (1) la sécurité des terminaux ; (2) la sécurité des réseaux locaux ; (3) la sécurité au sein des réseaux des fournisseurs de services associés ; et (4) la sécurité des environnements cloud et des contrôleurs hôtes IoT.

À titre d'exemple, le Corps des Marines adopte une approche agressive de la gestion des entreprises. [62] Le Corps des Marines suit chaque appareil qui tente de se connecter à son réseau, et s'assure que l'appareil est entièrement corrigé et conforme aux protocoles de sécurité avant de se connecter. Le Corps des Marines maintient une politique stricte pour les appareils personnels. Lorsque le BYOD est autorisé, les appareils sont placés dans des conteneurs virtuels afin de protéger les données sur l'appareil et le réseau gouvernemental. Les Marines veillent également à ce que les utilisateurs disposent des privilèges minimums pour assumer leurs responsabilités, utilisent l'authentification à deux facteurs et auditent les utilisateurs pour chaque création, modification et suppression de fichier.
Bien que cette approche soit plus agressive que ce que la plupart des entreprises peuvent faire, elle montre les mesures qui pourraient être prises dans le cadre d'un programme visant à protéger les entreprises contre les réseaux de zombies et autres menaces. [63]

L'une des conclusions du NSTAC est que les dispositifs IoT présentent un large éventail de caractéristiques et de capacités. Dans un environnement d'entreprise, certains biens IdO de grande valeur dotés de capacités de traitement avancées, comme les automobiles, peuvent présenter un degré de risque de cybersécurité qui rend viable le déploiement d'une solution de sécurité dédiée aux points d'extrémité. Cependant, de nombreux autres dispositifs IoT d'entreprise manquent de puissance informatique individuelle et s'appuient plutôt sur les fonctions de commande et de contrôle des hôtes contrôleurs pour l'application de la sécurité. En outre, un grand pourcentage de plateformes et de contrôleurs IoT d'entreprise dépendent de la connectivité du cloud qui peut être hébergée dans des centres de données internes, des clouds publics ou des environnements de fournisseurs de services. Une sécurité cohérente et bien intégrée sur l'ensemble de ces plateformes et contrôleurs, quel que soit leur emplacement, est essentielle pour empêcher la compromission et l'exécution d'une activité de commande et de contrôle non autorisée qui pourrait tirer parti de larges pans d'appareils IoT d'entreprise pour des attaques automatisées et distribuées.

Des innovations prometteuses sont prêtes à aider les entreprises : Le SDN et la virtualisation des fonctions réseau (NFV), ainsi que d'autres approches, affineront la manière dont les systèmes sont architecturés et organisés, et permettront des mesures de sécurité créatives. Le SDN offrira plusieurs avantages à la sécurité des entreprises :

- Contrôle centralisé : offre un point d'observation amélioré de la sécurité ;
- Gestion : la gestion de la sécurité s'améliore grâce à une visibilité totale du réseau ;
- Applications : Les applications SDN fournissent des fonctions de contrôle de sécurité natives ;
- Collecte de données : la collecte et l'analyse natives offrent une réponse améliorée ; et

[62] Ray Letteer. Corps des Marines des États-Unis. *Briefing au sous-comité ICR du NSTAC*. Le 29 août 2017.
[63] Ibid.

- Efficacité : Le SDN permet un réacheminement et des changements d'infrastructure plus immédiats (Dynamic Enforcement). [64]

La technologie NFV est également prometteuse. L'Institut européen des normes de télécommunications explique65 que la NFV dans la 5G prendra en charge le découpage en tranches du réseau, c'est-à-dire la création de plusieurs instances logiques de réseau (c'est-à-dire des tranches) sur le même réseau, qui peuvent être exploitées pour déployer et gérer les tranches de réseau de manière automatisée et flexible. Les principes de conception "cloud-native" maximisent l'utilisation efficace des ressources de l'entreprise grâce à un multiplexage à granularité plus fine sur l'infrastructure.
La gestion des services de bout en bout, c'est-à-dire la possibilité de proposer différentes offres de services à différents clients, permet à ces derniers de sélectionner les composants de base des services de réseau qui répondent le mieux à leurs besoins. L'informatique de périphérie, avec des systèmes hautement distribués, permet aux fonctions de réseau de s'exécuter sur les serveurs les plus proches du dispositif de l'utilisateur final, c'est-à-dire à la "périphérie" de l'architecture du réseau. La cloudification du réseau d'accès radio devrait offrir aux opérateurs des capacités sans précédent en termes de flexibilité, d'agilité, de gestion et d'orchestration des ressources et des services. Les services multisites/domaines, notamment la prise en charge de l'infrastructure en tant que service, de la NFV en tant que service et de la composition des services de réseau dans différents domaines administratifs, sont essentiels pour la transition vers la 5G. Gestion des licences NFV, la normalisation des mécanismes sous-jacents de gestion des licences éviterait d'aggraver la complexité de l'octroi des licences. Ces innovations favorisent la sécurité, la fiabilité et l'évolutivité de la sécurité des entreprises.

Les entreprises devraient établir des objectifs clairs pour faire face à ces risques, notamment les suivants :

Atténuer le risque d'attaques traditionnelles de botnet contre les réseaux d'entreprise. Les entreprises doivent explorer toutes les méthodes disponibles pour atténuer le risque d'attaques de botnets traditionnels dirigées contre leurs réseaux. Elles doivent notamment collaborer avec les fournisseurs d'accès Internet pour mettre en place des défenses au niveau du réseau, telles que le blocage des ports, le routage des flux de trafic, la lutte contre l'usurpation d'identité et d'autres méthodes d'attribution, avant les attaques de type DoS. De nombreuses entreprises se tournent vers leurs fournisseurs de réseaux pour qu'ils offrent des contrôles ou des fonctionnalités dans le cadre de services de sécurité gérés qui peuvent empêcher les dispositifs de communiquer avec des domaines extérieurs aux contrôleurs autorisés et activer des solutions de sécurité avancées telles que des pare-feu basés sur les applications, soutenus par de grandes quantités de renseignements dynamiques sur les menaces.

Veillez à ce que les appareils soient dotés d'une sécurité intégrée au moment de l'achat et tout au long du cycle de vie du produit. Les entreprises peuvent prendre plusieurs mesures pour s'assurer que les appareils connectés fonctionnent en toute sécurité sur leurs réseaux. Ces mesures comprennent la prise en compte de la sécurité des appareils au moment de l'achat, l'interrogation des fournisseurs potentiels sur la manière dont ils sécurisent les appareils, y compris la manière de s'authentifier auprès d'un appareil et la manière d'appliquer des correctifs ou de mettre à jour un appareil, et la possibilité de faire tester les appareils par un organisme indépendant. De nombreuses entreprises ont un pouvoir d'achat important et peuvent améliorer la sécurité globale pendant les phases de conception et de production du cycle de vie des appareils.

Après le déploiement, les entreprises doivent comprendre et utiliser toutes les méthodes disponibles pour empêcher que les dispositifs soient enrôlés (ou utilisés pour attaquer leurs propres réseaux). En sécurisant les dispositifs sur leurs réseaux, les considérations les plus importantes pour les entreprises sont : la détection (la capacité à

[64] Bill O'Hern. AT&T, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 20 juillet 2017.
[65] ETSI NFV Industry Specialization Group. *Perspectives des opérateurs de réseaux sur les priorités NFV pour la 5G.* 21 février 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

détecter tous les dispositifs de connexion en temps réel), la segmentation (la capacité de segmenter ou de "cloisonner" les points d'extrémité des autres parties de leurs réseaux, et l'automatisation (la capacité pour les solutions sélectionnées de fonctionner de manière automatisée), qui sont essentiels pour atteindre une certaine échelle alors que le nombre de dispositifs de connexion augmente de manière exponentielle. Il existe toute une série d'options offrant ces caractéristiques, notamment des outils permettant aux entreprises d'authentifier solidement les dispositifs, des outils permettant d'établir un profil comportemental des dispositifs (la capacité de détecter un comportement anormal des dispositifs qui pourrait indiquer une compromission) et des techniques d'analyse permettant aux entreprises de rechercher plus activement les vulnérabilités et les logiciels malveillants, afin de ne pas perturber le fonctionnement des dispositifs. Les entreprises doivent être attentives aux approches et outils émergents qui les aideront à sécuriser les dispositifs sur leurs réseaux, notamment les plateformes de gestion des informations et des événements de sécurité et d'orchestration qui permettent l'analyse et le partage en temps réel des informations contextuelles.

Il est difficile de motiver et de favoriser la sécurité des entreprises, notamment en raison de la diversité des contextes et des besoins des entreprises. Le NSTAC a identifié plusieurs mesures qui devraient être prises :

- **Considérez les recommandations applicables ci-dessus pour les appareils grand public comme des outils pour améliorer la posture de sécurité dans les environnements d'entreprise, en particulier pour le BYOD.**

- **Améliorer la sensibilisation aux meilleures pratiques.** Le DHS et d'autres agences devraient collaborer avec les secteurs verticaux de l'industrie, représentés par des groupes industriels (et, pour les entreprises considérées comme des "infrastructures critiques", par leurs conseils de coordination sectoriels) afin d'assurer la sensibilisation aux meilleures pratiques pour atténuer les effets des attaques de botnet et pour sécuriser les appareils connectés. Dans la mesure du possible, le DHS et l'industrie devraient fournir des guides de pratiques spécifiques au secteur. En outre, le DHS devrait s'appuyer sur le travail effectué par le NCCoE.

- **Envisager des incitations pour promouvoir l'adoption des normes.** Les agences fédérales et le Congrès devraient envisager d'utiliser des fonds fédéraux pour inciter à l'adoption des recommandations du présent rapport dans les projets financés par le gouvernement fédéral et pour les entreprises qui mettent en œuvre ces projets. Ces incitations ne seraient applicables que dans les cas où les exigences en matière de sécurisation des dispositifs qui sont dirigées ou supervisées par le gouvernement fédéral (comme pour les dispositifs médicaux) ne sont pas déjà en place.

- **Déployer des services de sécurité gérés.** Les entreprises de toutes tailles et de tous types doivent envisager de déployer des services de sécurité gérés. Chaque organisation doit évaluer son niveau de sécurité et réfléchir soigneusement à l'opportunité de déployer une approche de sécurité gérée. En outre, les capacités de surveillance doivent prendre en compte tous les types d'appareils connectés. Des services tels que l'atténuation des DDoS en cas d'attaques facilitées par des botnets sont utiles, car les entreprises seront de plus en plus tenues responsables de la sécurité.

- **Assurer la sécurité de l'entreprise.** Les entreprises doivent exploiter l'isolation du réseau, la micro segmentation et les techniques de filtrage pour sécuriser et limiter l'accès à Internet. D'autres options peuvent contribuer à la sécurité de l'entreprise :

    - *Connaissance des domaines :* Les entreprises doivent suivre et bloquer le trafic en provenance des domaines qui hébergent des menaces. Elles doivent également prendre des mesures pour protéger leurs domaines. Attaquants

ciblent souvent les domaines ayant la plus grande entrée DNS pour amplifier l'efficacité de leur attaque.

- *Déployer des contrôles compensatoires le cas échéant.* Toutes les organisations ne seront pas en mesure de déployer les protocoles prescrits. Comme l'explique le NIST, dans un environnement industriel, "il peut y avoir des situations où le [système de contrôle industriel ou ICS] ne peut pas supporter les contrôles de sécurité ou les améliorations de contrôle, ou lorsque l'organisation détermine qu'il n'est pas conseillé de les mettre en œuvre par le biais de l'ICS. Dans une telle situation, l'organisation fournit une justification décrivant comment les contrôles compensatoires offrent une capacité de sécurité ou un niveau de protection équivalent pour le SCI, et pourquoi les contrôles de sécurité de base correspondants ne pouvaient pas être employés. "[66] Des exemples de tels contrôles comprennent la détection en temps réel adaptée au réseau, l'authentification et l'autorisation, la gestion de la vulnérabilité, le profilage du comportement, la segmentation et l'atténuation. [67] Les contrôles compensatoires ne résoudront pas le problème des botnets mondiaux, mais ils constituent une étape importante dans la protection des entreprises.

- *Exploiter le cloud.* Les fournisseurs de services en nuage établis ont renforcé leur dispositif de sécurité et peuvent offrir aux entreprises des avantages considérables en matière de sécurité. Les entreprises - privées et publiques - devraient explorer les fournisseurs de services en nuage et la sécurité qu'ils peuvent offrir.

- *Utilisez le provisionnement dynamique.* Il s'agit d'un élément important de la virtualisation et de la segmentation du réseau, qui permet aux entreprises d'accélérer et de mieux contrôler la manière dont les appareils et les utilisateurs sont autorisés à se trouver sur un système. Le provisionnement dynamique automatise les processus informatiques et applique les exigences de sécurité, et permet de réagir plus rapidement aux problèmes de sécurité.

- La *redondance.* Toutes les entreprises devraient envisager la redondance pour le DNS et tous les services Internet essentiels à leur activité.

- **Prenons le marché de l'assurance. Le** marché de l'assurance peut favoriser l'amélioration, car les souscripteurs sondent les entreprises sur la maturité de leurs pratiques de gestion des risques de sécurité et proposent des primes plus basses aux entreprises qui se situent plus haut sur l'échelle de maturité.

3.4 Applications/Software/OS

CONSTATATIONS

Les logiciels des applications et des systèmes d'exploitation jouent un rôle essentiel dans la lutte contre les réseaux de zombies, qui s'intensifie à mesure que les logiciels sont intégrés dans un nombre croissant de systèmes et de dispositifs.
En outre, avec la prolifération des logiciels, de nombreuses entreprises technologiques non traditionnelles sont devenues des fournisseurs. Bien qu'il y ait eu une amélioration et un partage significatifs de logiciels sécurisés

[66] NIST ITL Bulletin. *Adaptation des contrôles de sécurité pour les systèmes de contrôle industriels*. Novembre 2015. http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf.
[67] Wallace Sann. ForeScout. *Briefing au sous-comité ICR du NSTAC*. Le 22 août 2017.

de développement et de gestion, les fournisseurs de logiciels non traditionnels, les start-ups et autres peuvent ne pas connaître ces processus ou ne pas avoir les ressources pour les mettre en œuvre. De plus, dans le contexte de l'IdO, le risque lié aux vulnérabilités logicielles peut être élevé ; les voitures connectées peuvent avoir un accident et les grille-pain intelligents peuvent provoquer un incendie. [68]

Pertinence du défi des botnets pour les applications/logiciels/systèmes d'exploitation

Les applications, les logiciels et les systèmes d'exploitation sont critiques car ils sont essentiels à la sécurité des terminaux et à la sécurité des services ou des ressources qui sont exploités par les terminaux. De nombreux développeurs fournissent des logiciels intégrés dans les dispositifs, les applications et les services ; cette diversité fait partie intégrante de l'innovation, mais représente un défi pour la sécurité. Les parties prenantes se situent à différents niveaux de maturité dans le développement et la gestion des logiciels. Alors que le développement de logiciels est essentiel pour limiter le nombre et la gravité des vulnérabilités dans les logiciels dès le départ, la gestion est essentielle pour garantir que les vulnérabilités découvertes puissent être traitées.

Il est impraticable ou impossible de développer un logiciel sans aucune vulnérabilité. Si des progrès sont réalisés dans les méthodes formelles de vérification pour les petites pièces hautement critiques des systèmes vitaux, l'utilisation de ces méthodes à grande échelle ou pour les systèmes cyber-physiques complexes reste un défi à moyen et long terme. [69] En revanche, la mise en œuvre de bonnes pratiques, de directives et d'outils de développement et de gestion de logiciels sécurisés peut améliorer la sécurité de base.

Cependant, malgré la disponibilité de pratiques, de lignes directrices et d'outils de la part des fournisseurs, la sensibilisation et la mise en œuvre par les fournisseurs et les clients accusent un retard considérable. Premièrement, tous les logiciels ne sont pas développés ou gérés par des fournisseurs à grande échelle, et les pratiques de développement sécurisé ne peuvent pas nécessairement être appliquées facilement ou de manière cohérente dans des environnements de développement plus petits. Deuxièmement, le code source ouvert est en augmentation ; il est souvent maintenu par des bénévoles qui peuvent ne pas avoir d'exigences ou de processus de développement sécurisé, de responsabilité claire ou de financement pour répondre aux problèmes de sécurité. Troisièmement, les utilisateurs peuvent interrompre la mise en œuvre, et beaucoup d'entre eux ont du mal à appliquer des correctifs de sécurité ou des mesures d'atténuation sur les produits, les services ou les appareils dans les contextes des consommateurs et des entreprises.

Des efforts sont en cours pour faire face à la menace

Les éditeurs de logiciels ont commencé à travailler à l'amélioration de la sécurité du code, c'est-à-dire du développement des logiciels, il y a plus de 15 ans. Ce domaine de pratique, souvent appelé assurance logicielle, encourage les développeurs à créer des logiciels plus sûrs et à répondre aux exigences de conformité en matière de sécurité. De nombreux grands fournisseurs ont développé des programmes, des formations et des outils pour le développement, la mise en œuvre et le perfectionnement du code. Par exemple, l'utilisation du cycle de vie du développement de la sécurité (SDL) garantit que le logiciel est conçu, développé et déployé en tenant compte de la sécurité tout au long de son cycle de vie. [70] Les fournisseurs ont collaboré par le biais d'organisations à but non lucratif telles que le Software Assurance Forum.

[68] Charlie Mitchell. Inside Cybersecurity. *Le fondateur de Black Hat voit la responsabilité logicielle comme un défi majeur de la politique de cybersécurité.* 26 juillet 2017. https://insidecybersecurity.com/daily-news/black-hat-founder-sees-software-liability- major-cybersecurity-policy-challenge.

[69] Kevin Hartnett. WIRED. *Les informaticiens se rapprochent d'un code parfait, à l'épreuve du piratage.* 23 septembre 2016. https://www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/.

[70] Microsoft. Qu'est-ce que le cycle de vie du développement de la sécurité ? https://www.microsoft.com/en-us/sdl/default.aspx.

pour l'excellence du code (SAFECode) afin de promulguer des pratiques d'assurance logicielle. [71] Les fournisseurs ont contribué au développement de la norme 27034 de l'Organisation internationale de normalisation (ISO)/Commission électrotechnique internationale (CEI), une norme internationale basée sur les processus pour spécifier, concevoir/sélectionner et mettre en œuvre des contrôles de sécurité de l'information.

Les éditeurs de logiciels s'efforcent d'améliorer la gestion des logiciels en développant, en mettant en œuvre et en promouvant des politiques, des processus et des programmes de divulgation coordonnée des vulnérabilités (CVD). La divulgation et le traitement des vulnérabilités impliquent de communiquer avec les tiers qui les trouvent, de valider et de trier les vulnérabilités, de développer une mise à jour pour atténuer la vulnérabilité (par exemple, un "patch") et d'appliquer les mises à jour ou les mesures d'atténuation aux systèmes en fonctionnement. Comme pour les outils visant à améliorer l'assurance du code, les fournisseurs de technologies ont investi dans les meilleures pratiques de divulgation et de traitement des vulnérabilités. Il existe deux normes ISO, ISO/IEC 29147 et ISO/IEC 30111, qui décrivent les processus pour recevoir des informations sur les vulnérabilités de la part de tiers, pour communiquer avec ces derniers au sujet des problèmes signalés, et pour enquêter, trier et résoudre les vulnérabilités.

Certains fournisseurs de technologies ont investi dans la promotion de la divulgation des vulnérabilités, et le gouvernement américain a également accru ses efforts dans ce domaine. [72] De nombreux fournisseurs de logiciels ont participé au processus multipartite de la NTIA sur la divulgation et le traitement des vulnérabilités afin d'accroître l'adoption des meilleures pratiques existantes, d'améliorer la réponse aux défis complexes de divulgation impliquant plusieurs parties et d'aider les industries critiques en matière de sécurité à mieux comprendre comment adopter la DVC. [73] S'appuyant sur les efforts de la NTIA, la Food and Drug Administration a publié des directives encourageant les fabricants de dispositifs médicaux à adopter le CVD, en se référant aux normes ISO/IEC 29147 et ISO/IEC 30111, [74] et la National Highway Transportation Safety Administration a publié des directives encourageant les constructeurs automobiles à disposer d'une méthode et d'une politique pour recevoir les rapports de vulnérabilité des chercheurs en sécurité. [75] En outre, le département de la défense (DoD) et l'administration des services généraux ont créé des programmes CVD et/ou des programmes de primes pour les bogues, permettant une coordination avec les chercheurs. [76] Plus récemment, le ministère de la Justice (DOJ) a publié un cadre pour aider les organisations à créer un programme volontaire de divulgation coordonnée des cyber-vulnérabilités. Le Congrès se penche également sur la question. Bien qu'il ne soit pas forcément adapté à toutes les organisations, le CVD pourrait aider à relever les défis de la gestion des logiciels.

---

[71] SafeCode. https://safecode.org/about-safecode/.

[72] Je suis la cavalerie. *Calendrier de divulgation coordonné par le DOT Gov.* https://www.iamthecavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.

[73] NTIA. Multi-stakeholder Process : Vulnérabilités en matière de cybersécurité. 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[74] Département de la santé et des services sociaux (HHS). "Gestion post-commercialisation de la cybersécurité des dispositifs médicaux-Guide pour l'industrie et le personnel de la Food and Drug Administration." 28 décembre 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022. pdf.

[75] National Highway Traffic Safety Administration (NHTSA). "Meilleures pratiques en matière de cybersécurité pour les véhicules modernes". Octobre 2016. https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[76] DOD. "Le DOD annonce une politique de divulgation des vulnérabilités numériques et le lancement de "Hack the Army"." *Communiqué de presse*. 21 novembre 2016. https://www.defense.gov/News/News-Releases/News-Release- View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/; https://hackerone.com/deptofdefense ; GSA. Vulnerability Disclosure Policy. https://18f.gsa.gov/vulnerability- disclosure-policy/.

Les efforts visant à améliorer l'assurance logicielle et à gérer et répondre aux vulnérabilités signalées ou découvertes d'une autre manière ont manifestement amélioré la cybersécurité, mais les travaux visant à créer un mélange d'incitations et de dissuasions pourraient être utiles. À cette fin, le NSTAC recommande les considérations suivantes :

Premièrement, les politiques axées sur l'assurance logicielle et la gestion des vulnérabilités - quel que soit le mécanisme de mise en œuvre - doivent s'appuyer sur des normes internationales, notamment les normes IEC/ISO 27034, ISO/IEC 29147 et ISO/IEC 30111. Elles doivent se concentrer sur les processus utilisés pour développer et corriger les logiciels (c'est-à-dire la manière dont les logiciels sont construits pour réduire le nombre de vulnérabilités et la manière dont les vulnérabilités sont corrigées ou atténuées) plutôt que sur la présence de vulnérabilités.

Deuxièmement, ni les gouvernements ni les entreprises n'ont efficacement tiré parti des forces du marché pour stimuler le développement de logiciels plus sûrs parce qu'on ne sait pas encore très bien à quelle norme les forces du marché devraient répondre. Le NSTAC recommande au gouvernement américain de favoriser la prise de conscience du rôle que l'assurance logicielle et les achats technologiques ont sur le risque opérationnel. Le gouvernement devrait également mettre l'accent sur les meilleures pratiques et normes existantes, permettant ainsi aux acheteurs de technologies de l'information et des communications (TIC) d'avoir des conversations avec leurs fournisseurs sur le développement de produits et services technologiques et sur les pratiques de gestion de la sécurité.

Le NSTAC recommande spécifiquement ce qui suit :

- **Le gouvernement et les établissements d'enseignement doivent s'efforcer d'intégrer la sécurité dans le programme d'enseignement de l'informatique dans le cadre de l'initiative Science, technologie, ingénierie et mathématiques.**

- **La communauté des développeurs de logiciels devrait fournir des directives sur les processus DevSecOps.**

- **L'industrie devrait envisager des programmes coordonnés raisonnables et prudents de divulgation des vulnérabilités. Il** pourrait s'agir de programmes de divulgation des vulnérabilités gérés par les organisations ou de programmes externalisés si les organisations n'ont pas la capacité de les gérer en interne.

- **L'industrie devrait donner aux développeurs les outils nécessaires pour coder en toute sécurité.** Améliorer les outils de développement du code pour renforcer la traçabilité et la sécurité.

- **Partager les meilleures pratiques pour traiter les vulnérabilités. La** NTIA a examiné cette question[77], et l'industrie peut soutenir les recommandations qui découlent de ce processus multipartite, ainsi que d'autres orientations. [78]

[77] NTIA. Multi-stakeholder Process : Vulnérabilités en matière de cybersécurité. 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[78] DOJ. " Cadre pour un programme de divulgation des vulnérabilités pour les systèmes en ligne. " Juillet 2017. https://www.justice.gov/criminal-ccips/page/file/983996/download.

- **Le gouvernement devrait envisager une protection de la responsabilité pour ceux qui abordent publiquement les vulnérabilités.** La nation a peut-être besoin d'un changement de paradigme dans sa façon d'aborder ces défis.

- **Les pouvoirs publics et l'industrie devraient collaborer à une campagne visant à promouvoir l'assurance logicielle, c'est-à-dire la validation des logiciels pour limiter les failles de sécurité.** Cela peut nécessiter la promotion de meilleures pratiques ou de lignes directrices afin de donner l'exemple aux développeurs de logiciels.

- **Examiner attentivement la manière de sécuriser le développement des sources ouvertes. L'**effort collectif de l'industrie pour fournir des fonds aux éléments critiques de l'infrastructure mondiale de l'information par le biais de l'initiative Core Infrastructure contribuera à résoudre certains problèmes, mais le NSTAC estime que des efforts supplémentaires sont nécessaires.

- **Les pouvoirs publics et l'industrie devraient faire en sorte que les utilisateurs de technologies comprennent mieux l'importance de l'application de correctifs en temps voulu.** Cela peut se faire en incorporant ces éléments dans les programmes de sensibilisation à la sécurité existants.

3.5 Gouvernement

CONSTATATIONS

Le gouvernement joue un rôle clé dans la résilience de l'Internet et des communications. Il est acheteur et gestionnaire d'appareils connectés ; il est régulateur ou rassembleur dans l'élaboration des politiques ; et il exerce un pouvoir souverain pour poursuivre les criminels, défendre la nation et négocier avec d'autres pays. Chaque rôle est différent, présentant différents défis et offrant différentes opportunités.

En tant que gestionnaire et acheteur, le gouvernement est confronté aux mêmes problèmes de botnet que les autres entreprises. Le nombre d'utilisateurs d'appareils connectés au sein du gouvernement rend la gestion des appareils difficile. Le gouvernement a la responsabilité supplémentaire de sécuriser les informations gouvernementales sensibles, ainsi que les données des citoyens - ce qui fait du gouvernement une cible de grande valeur. En outre, les entités du gouvernement américain gèrent plusieurs blocs IP vulnérables. [79]Il est confronté à d'autres défis dans l'environnement réglementaire et de politique d'approvisionnement, qui restreint la flexibilité et nécessite que les décisions d'approvisionnement soient prises longtemps à l'avance et soumises à une surveillance et à des contraintes externes.

Le gouvernement dispose d'opportunités uniques pour renforcer la sécurité. En tant que gestionnaire, le gouvernement peut prendre des mesures pour améliorer les pratiques de gestion de l'utilisation des mobiles - en utilisant un certain nombre de services de gestion des appareils existants et en sensibilisant davantage à l'importance d'employer des pratiques de cyber-hygiène de base. En tant qu'acheteur de technologies, le gouvernement peut exiger des appareils plus sécurisés. Les normes gouvernementales conduisent souvent à l'adoption de ces normes par le secteur privé, évitant ainsi le développement de pratiques différentes et potentiellement concurrentes. Le sénateur Mark Warner a présenté un projet de loi, le *Internet of Things (IoT) Cybersecurity Improvement Act of 2017*, qui propose d'améliorer la sécurité de l'IdO en établissant des exigences minimales pour les dispositifs IdO.

[79] Ann Cox. DHS. *Briefing au sous-comité ICR du NSTAC*. Le 1er août 2017.

achetés par le gouvernement fédéral. [80] Une législation comme la *loi sur la cybersécurité de l'IdO* pourrait toutefois avoir des conséquences inattendues si elle n'est pas abordée avec soin. Le projet actuel, s'il est adopté, pourrait exposer les entrepreneurs du gouvernement à la responsabilité en raison d'exigences de certification onéreuses, encourager le "piratage" des appareils gouvernementaux et limiter la capacité des entrepreneurs à gérer de manière appropriée les divulgations de vulnérabilité. La cybersécurité est mieux assurée par des solutions souples, axées sur le marché, qui reflètent le leadership et l'innovation du secteur privé et qui sont élaborées grâce à la collaboration entre l'industrie et le gouvernement. [81]

En tant que régulateur ou rassembleur, le gouvernement peut façonner la politique et les normes, tout en favorisant l'innovation. Aux États-Unis, la cyberpolitique met l'accent sur le rôle de rassembleur du gouvernement. Le gouvernement devrait continuer à réunir les parties prenantes pour développer les meilleures pratiques avec des acteurs issus de divers secteurs industriels et de l'ensemble de l'écosystème des communications et des TIC. Il est impératif que le gouvernement comble le fossé des connaissances entre les industries sophistiquées et non sophistiquées. Au niveau international, le gouvernement peut faciliter la collaboration à plus grande échelle, en encourageant d'autres pays à partager des informations et à adopter les meilleures pratiques appropriées pour atténuer les réseaux de zombies. Ces efforts pourraient réduire considérablement le nombre et l'ampleur de ces attaques, dont beaucoup proviennent de l'étranger.

Le gouvernement joue un rôle important en assurant le financement de la recherche sur la cybersécurité et l'atténuation des attaques, dont les avantages ne peuvent être surestimés. Outre les dépenses directes, le gouvernement doit continuer à chercher des occasions de s'engager auprès du public pour améliorer la sécurité. Cette année, la FTC a organisé un concours de prix visant à créer des solutions pour " se prémunir contre les vulnérabilités de sécurité des logiciels présents sur les appareils IoT de leurs maisons. "[82] Le gagnant - un développeur de logiciels du New Hampshire - a mis au point une application mobile qui peut aider les utilisateurs à déterminer si leurs appareils sont périmés ou si leurs réseaux ne sont pas sécurisés. [83]

Le gouvernement joue également un rôle unique dans la sécurité publique et devrait travailler avec le NIST et d'autres organismes pour renforcer la sécurité des systèmes de sécurité publique. Les mesures d'application prises par la FTC à l'encontre des fabricants qui emploient des mesures de sécurité lamentablement inadéquates ont fait prendre conscience à l'industrie de la nécessité de mettre en œuvre une sécurité de base et de donner une image fidèle de la sécurité de leurs appareils aux consommateurs. [84]

En tant que nation souveraine, le gouvernement a des pouvoirs et des devoirs uniques pour protéger les citoyens, faire respecter la loi et défendre le pays contre les menaces extérieures, y compris les botnets. Grâce à ces pouvoirs,

[80] Mark Warner. "Les sénateurs présentent une législation bipartisane visant à améliorer la cybersécurité des appareils de l'"Internet-of-Things" (IoT)". *Communiqué de presse*. 1er août 2017. https://www.warner.senate.gov/public/index.cfm/pressreleases?ID= 06A5E941-FBC3-4A63-B9B4-523E18DADB36.

[81] Mike Bergman. Consumer Technology Association. *Briefing au sous-comité ICR du NSTAC*. Le 3 août 2017.

[82] FTC. Défi de l'inspecteur de maison IoT. 2017. https://www.ftc.gov/iot-home-inspector-challenge.

[83] FTC. " La FTC annonce le gagnant de son concours sur la sécurité des appareils domestiques de l'Internet des objets. " *Communiqué de presse*. 26 juillet 2017. https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things- home-device-security.

[84] FTC. "La FTC approuve l'ordonnance finale réglant les accusations contre TRENDnet. Inc." *Communiqué de presse*. 7 février 2014. https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against- trendnet-inc; https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home- routeurs-cloud-services-put.

le gouvernement peut arrêter ou dissuader certaines activités malveillantes. Parmi les exemples d'outils efficaces, citons le blocage de l'enregistrement des domaines, le blocage des adresses IP, les enquêtes criminelles et le démantèlement des botnets.

Les partenariats public-privé avec les forces de l'ordre se sont avérés efficaces, et les États-Unis devraient rechercher les possibilités d'étendre ces efforts. Les forces de l'ordre, les équipes d'intervention en cas d'urgence informatique et autres s'appuient souvent sur le secteur privé pour obtenir des renseignements sur les menaces et des données provenant des fournisseurs de télécommunications, des vendeurs d'antivirus et du secteur financier. Les renseignements sont essentiels pour identifier les individus qui ont la motivation, l'intention et le soutien nécessaires pour mener des cyberattaques, et ces partenariats aident les gouvernements et les FAI du monde entier à identifier les menaces et à y remédier. Le NSTAC recommande au gouvernement d'accroître sa collaboration avec le secteur privé, notamment en ce qui concerne les enquêtes. De tels partenariats public-privé ont prospéré au Royaume-Uni, et les entreprises de sécurité américaines et autres sont prêtes à coopérer avec le gouvernement pour soutenir les enquêtes en cours et futures. [85]

Le DOJ, en coordination avec le FBI, d'autres organismes d'application de la loi et des entités privées, a réussi à poursuivre le démantèlement de botnets. Le premier démantèlement réussi a eu lieu en avril 2011, lorsque le gouvernement a arrêté "Coreflood", une attaque touchant plus de 378 000 appareils86. [86]Depuis lors, d'autres victoires ont été remportées, notamment le démantèlement récent de deux marchés noirs en ligne, AlphaBay et Hansa, avec la coopération de gouvernements étrangers. [87]

Exemples de démantèlements majeurs de botnets88

- 2011 : Changeur de DNS89
- 2011 : Coreflood (378 000 appareils)
- 2013 : Citadel (2 millions d'appareils)
- 2014 : GameOver Zeus (500 000 à 1 million d'appareils)
- 2016 : Avalance (500 000 appareils)
- 2017 : Kelihos/Waldec (100 000 appareils)

En réduisant les obstacles réglementaires qui limitent l'engagement de l'industrie, le gouvernement pourrait s'attaquer plus efficacement aux attaques de botnet les plus sophistiquées.

Le gouvernement peut améliorer le démantèlement des botnets en éliminant les obstacles qui limitent la participation de l'industrie. Le démantèlement d'un botnet demande du temps, de l'argent et des ressources, et peu d'entreprises sont incitées à engager les actions en justice nécessaires pour tenter de le démanteler. [90]Pour l'industrie, le démantèlement d'un botnet implique généralement de prendre le contrôle de l'infrastructure, de rediriger l'accès à l'infrastructure et d'assurer la sécurité.

[85] Raj Samani. McAfee, Royaume-Uni. *Briefing au sous-comité ICR du NSTAC*. Le 15 août 2017.
[86] DOJ. " Le ministère de la Justice prend des mesures pour désactiver un botnet international ". 13 avril 2011. https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.
[87] DOJ. " AlphaBay, le plus grand " marché noir " en ligne, fermé ". 20 juillet 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.
[88] Leonard Bailey. MINISTÈRE DE LA JUSTICE. *Briefing au sous-comité ICR du NSTAC*. Le 10 août 2017.
[89] http://www.dcwg.org/dns-changer/
[90] Ibid.

Communications, et l'atténuation des préjudices. Ces activités nécessitent souvent soit l'autorisation de l'utilisateur final, soit un mandat, une ordonnance d'interdiction temporaire ou une injonction civile. [91] C'est un défi lorsque les attaques malveillantes proviennent de l'extérieur du réseau d'un FAI. Ainsi, les gouvernements - avec le soutien de l'industrie - sont les mieux placés pour mener les activités de démantèlement des botnets.

La mesure du succès pour les procureurs est un autre problème susceptible de freiner les prises en charge. Dans le contexte de l'activité criminelle dans le monde physique, les objectifs et les structures d'incitation du gouvernement sont axés sur l'identification et la poursuite des défendeurs. Ces objectifs et structures d'incitation traditionnels ne sont peut-être pas totalement optimisés pour le monde virtuel, qui permet aux cybercriminels de bénéficier d'un plus grand anonymat et qui, par conséquent, contrarie considérablement les efforts visant à les identifier et à les poursuivre en tant que défendeurs. Cependant, il existe également d'autres moyens pour les procureurs de perturber et de dissuader la criminalité - y compris les attaques de botnets utilisant des logiciels malveillants - dans le monde virtuel. Tout en continuant à rechercher et à poursuivre les accusés criminels, ce qui reste essentiel, les procureurs peuvent également être incités à se concentrer plus largement sur la prévention du crime et la sécurité nationale.
Les procureurs peuvent contribuer à prévenir la prolifération et l'impact négatif des botnets. Ils peuvent perturber et démanteler les opérations des botnets, même lorsqu'aucun accusé potentiel n'est discernable.

La perturbation et le démantèlement des réseaux de zombies peuvent avoir des effets positifs importants. Par exemple, les efforts déployés par un partenariat public-privé pour couper les liens entre les ordinateurs infectés et l'infrastructure de Citadel, l'un des plus grands botnets répertoriés, ont permis de mettre fin à 90 % de l'activité du botnet. [92] De même, la prise de contrôle par le gouvernement de Coreflood, qui utilisait des logiciels malveillants pour siphonner les informations personnelles et financières d'utilisateurs peu méfiants, a permis aux victimes de supprimer les logiciels malveillants de leurs machines et d'éviter de nouvelles atteintes à la vie privée et à la sécurité financière des utilisateurs. En neuf jours, le nombre de balises provenant d'ordinateurs infectés et envoyées aux serveurs a considérablement diminué. [93]

Cependant, de nombreux botnets ne sont pas démantelés par le gouvernement - ou leur démantèlement est retardé - car, conformément à leur structure d'incitation, de nombreux procureurs se concentrent surtout sur l'identification et la poursuite d'un accusé criminel. [94] En vertu des directives actuelles, les procureurs fédéraux ne sont encouragés à engager des poursuites que lorsqu'ils estiment que le comportement de la personne constitue une infraction fédérale et que les preuves admissibles seront suffisantes pour obtenir et maintenir une condamnation. Cet accent mis sur les poursuites judiciaires limite la capacité du gouvernement à perturber et à démanteler les réseaux de zombies car, en grande partie, il n'y a pas de personne(s) facilement identifiable(s) à poursuivre, même lorsque les crimes sont en cours. Le gouvernement a effectivement mis l'accent sur la prévention dans d'autres contextes ; le DOJ a effectivement consacré davantage de ressources et d'énergie à la prévention dans le contexte de la lutte contre le terrorisme. Les leçons tirées de ces réussites peuvent s'appliquer au moment où le gouvernement étudie comment faire évoluer les structures d'incitation liées à la cybercriminalité d'une manière qui ne soit pas exclusivement liée à la lutte contre le terrorisme.

[91] Voir Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030) ; Wiretap Act (18 U.S.C. § 2511) ; Pen Register/Trap and Trace Statutes (18 U.S.C. §§ 3121 *et seq.*).

[92] Zach Lerner, *Microsoft the Botnet Hunter : The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 247 (2014).

[93] Mémorandum supplémentaire du gouvernement à l'appui de l'injonction préliminaire, p. 4, figure 1 dans *United States v. John Doe*, n° 3:11-cv-561 (VLB) (D. Conn. déposé le 11 avril 2011).

[94] Les budgets annuels et les mesures de performance du United States Attorney's Office (USAO) sont directement liés au nombre de condamnations.

Il s'agit plutôt d'encourager la coordination entre les agences fédérales et avec le secteur privé pour perturber et démanteler les botnets. Par exemple, si le FBI est investi de la fonction importante d'enquêter sur les cybercrimes, son pouvoir d'action n'est pas sans limite. Le FBI doit coopérer, coordonner et demander l'approbation des procureurs fédéraux pour utiliser certains outils d'enquête, et l'autorisation est généralement refusée à moins qu'il n'y ait une probabilité de condamnation, ce qui limite le potentiel du gouvernement à prévenir la cybercriminalité et à se protéger contre les risques pour la sécurité nationale. Le recentrage des ressources et des structures d'incitation permettrait également au gouvernement de s'appuyer sur le secteur privé et d'établir des partenariats avec lui en matière de prévention de la cybercriminalité de manière plus régulière et plus productive afin de mieux protéger les victimes des botnets et d'augmenter le coût des opérations des botnets pour les criminels. L'augmentation du coût des opérations criminelles a un effet positif en cascade ; la réduction du nombre de criminels qui peuvent se permettre de participer à la criminalité en ligne réduit également le "bruit" dans l'écosystème, ce qui permet aux entités des secteurs public et privé d'identifier plus efficacement les menaces persistantes avancées plus furtives.

Le NSTAC recommande les actions suivantes pour améliorer les efforts de démantèlement :

- **Les politiques du ministère de la Justice devraient être plus favorables à l'intervention du gouvernement. Le ministère de la Justice pourrait avoir besoin de ressources supplémentaires pour intensifier ces efforts, qui dépendent également de la collaboration avec le secteur privé et les partenaires internationaux potentiels.**

- **Les implications des botnets en matière de sécurité nationale justifient que le ministère de la Justice se concentre sur la prévention et l'interruption des attaques de botnets, et non sur les poursuites**.

- **Le budget consacré à la cybercriminalité au niveau fédéral devrait refléter l'importance de la prévention et ne devrait pas être lié aux poursuites et aux condamnations.** [95]

Le gouvernement doit également s'assurer que la législation existante ne limite pas le partage d'informations ou les activités de "défense active" appropriées de l'industrie. Des lois comme le *Computer Fraud and Abuse Act*, le *Wiretap Act* et le *Pen Register/Trap and Trace Act* peuvent involontairement décourager les FAI de prendre certaines "mesures de défense active" - comme la mise en œuvre du filtrage d'entrée/sortie (BCP 38 et 84), le blocage du mauvais trafic signalé et la neutralisation d'un système qui attaque le réseau du fournisseur - pour des raisons de responsabilité juridique. [96] Les protections juridiques en cas d'erreur sont limitées, et les entreprises sont potentiellement critiquées pour leurs erreurs. Le gouvernement devrait chercher des moyens de limiter les risques de responsabilité pour les fournisseurs qui emploient de bonne foi des mesures défensives actives.
La *loi sur le partage des informations relatives à la cybersécurité* (CISA) de 2015 autorise la surveillance des informations sur un système d'information à des fins de cybersécurité et prévoit des protections en matière de responsabilité pour ces activités et d'autres mesures défensives. [97] Des lois comme la CISA permettent à l'industrie de protéger ses réseaux et de soutenir les efforts de démantèlement du gouvernement. Si l'on attend davantage du secteur privé, des protections supplémentaires doivent être envisagées. L'amélioration de la cybersécurité nécessitera un partenariat mutuellement bénéfique entre l'industrie et le gouvernement.

[95] Richard Boscovich. Microsoft. *Briefing au sous-comité ICR du NSTAC*. Le 16 août 2017.
[96] Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030) ; Wiretap Act (18 U.S.C. § 2511) ; Pen Register/Trap and Trace Statutes (18 U.S.C. §§ 3121 *et seq.*) ; Leonard Bailey. MINISTÈRE DE LA JUSTICE. *Briefing au sous-comité ICR du NSTAC*. 10 août 2017.
[97] Cybersecurity Information Sharing Act of 2015, Pub. L. n° 114-113, 129 Stat. 2242 (2015).

RECOMMANDATIONS

Des efforts sont en cours pour renforcer la responsabilité des agences, comme le reflète le président dans le décret 13800.[98] Le gouvernement doit s'appuyer sur ces efforts, en montrant l'exemple. Le gouvernement doit s'appuyer sur ces efforts, en donnant l'exemple. En outre, le gouvernement doit utiliser de manière agressive ses outils d'application de la loi, tout en supprimant les obstacles à l'action privée.

- **Donner l'exemple en exploitant judicieusement les capacités dans les achats**. Le gouvernement devrait investir dans le renforcement de la sécurité des réseaux fédéraux. Les efforts actuels, tels que le déploiement du système de diagnostic et d'atténuation continus pour les agences civiles et du système Comply to Connect pour le DoD, tous deux ancrés dans les meilleures pratiques du NIST, permettent aux agences de détecter, d'inventorier et de remédier à tous les dispositifs IoT et de technologie opérationnelle, ainsi qu'aux points d'extrémité basés sur Windows, sur les réseaux fédéraux. Le leadership dans ce domaine pourrait servir d'exemple au secteur privé.

- **Employer les normes et les orientations du NIST pour la loi sur la gestion de la sécurité des informations fédérales et la gestion des TI**. Le NIST, en collaboration avec le secteur privé, améliore en permanence les meilleures pratiques en matière de cybersécurité. Il s'efforce notamment d'améliorer son cadre, de mettre à niveau les capacités cryptographiques (notamment la cryptographie résistante quantique) et d'explorer les capacités de sécurité de l'IA et de l'IdO. Le NIST s'efforce également d'améliorer l'architecture de l'internet, notamment la sécurité des domaines et du BGP. Le gouvernement devrait être parmi les premiers à mettre en œuvre ces normes.

- **Augmenter le nombre de démantèlements de botnets par les forces de l'ordre**. Le gouvernement devrait s'appuyer sur les récents succès en matière de démantèlement de botnets pour démontrer l'efficacité de la prévention. Entre autres choses, le gouvernement devrait envisager

  - Veiller à ce que les structures d'incitation reflètent l'importance de la prévention plutôt que d'être fortement liées aux poursuites et aux condamnations ;

  - Rationalisation des processus d'application de la loi pour le démantèlement des botnets, y compris l'utilisation de lignes directrices définitives en matière de condamnation ;

  - soutenir la collaboration entre le secteur public et le secteur privé en matière de démantèlement ; et

  - Moderniser ses méthodes de collecte de cyberespionnage en permettant à un analyste de se concentrer sur une cible pendant une période plus longue, devenant ainsi un expert et plus à même de combattre une attaque spécifique. Tout en réfléchissant aux moyens d'améliorer le démantèlement des botnets, il est impératif que le gouvernement agisse de manière transparente.

- **Éviter les doublons**. Le gouvernement devrait consolider et coordonner plus efficacement les efforts visant à renforcer la cybersécurité de la nation. Par exemple, plusieurs efforts se sont chevauchés pour améliorer la sécurité de la chaîne d'approvisionnement de la part de diverses agences, notamment le NIST, le DHS et la FCC. Des efforts se chevauchent également dans le domaine de la sécurité de l'IdO, notamment au sein du DHS, du NIST et de la NTIA, ainsi qu'au sein de plusieurs agences qui supervisent les différents secteurs verticaux de l'IdO (comme l'Agence nationale de la sécurité des télécommunications).

[98] Bureau du secrétaire de presse de la Maison Blanche. *Ordre exécutif 13800, Renforcer la cybersécurité des réseaux fédéraux*

et des infrastructures critiques. 16 mai 2017. https://www.federalregister.gov/documents/2017/05/16/ 2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

véhicules, villes intelligentes, etc.) Il s'agit de questions importantes qui bénéficieraient d'une approche coordonnée.

- **Maintenir un rôle de convocation et de promotion**. Le gouvernement est particulièrement bien équipé pour réunir l'industrie afin d'appliquer les cadres existants à de nouveaux domaines tels que l'IdO et de développer les meilleures pratiques pour les technologies en évolution. Les processus multipartites, tels que ceux du NIST et de la NTIA, doivent être encouragés et leurs conseils pratiques promus. Bien que le gouvernement ne doive pas émettre de mandats, il peut encourager les entités à adopter ces normes en fournissant des incitations. Dans le même temps, le gouvernement doit examiner les normes issues de ces processus afin d'identifier et de combler toute lacune susceptible d'affecter l'IdO.

- **Accroître les protections pour les ISP qui appliquent des mesures défensives**. Les lois existantes découragent souvent l'utilisation de mesures de défense active par l'industrie. Le gouvernement devrait donc chercher des moyens de limiter la responsabilité juridique des fournisseurs qui cherchent à protéger leurs systèmes contre les attaques de botnets.

- **Financer la recherche sur la cybersécurité et l'élaboration de normes.** Il est impératif de financer la recherche et le développement. Le gouvernement devrait soutenir financièrement ces efforts, notamment la recherche sur les mesures de base des chemins, la topologie au niveau des routeurs, la topologie au niveau des installations, les performances et les meilleures pratiques en matière d'hygiène de sécurité. La recherche sur les nouvelles technologies - en particulier la technologie quantique - est nécessaire car les menaces évoluent et le cryptage devient moins efficace.

- **Promouvoir des normes et des lignes directrices consensuelles et volontaires.** Les partenariats public-privé et les directives volontaires sont plus efficaces que les mandats, qui deviennent rapidement obsolètes dans cet environnement en constante évolution. [99] Toute réglementation devrait se concentrer sur l'atténuation des risques et la limitation de la responsabilité qui peut découler des efforts de l'industrie pour partager les informations et employer des mesures de défense.

3.6 International

CONSTATATIONS

Aucune discussion sur les attaques distribuées n'est complète sans une attention particulière aux acteurs internationaux, qui font partie de chaque couche de l'écosystème ci-dessus. Parmi les acteurs internationaux et les défis à relever, citons :

- **Entreprises technologiques internationales**. Les fabricants d'appareils et les fournisseurs de services sont présents dans le monde entier et vendent leurs produits à l'échelle internationale. Il s'agit notamment d'un large éventail de fabricants d'équipements (tels que les smartphones, les appareils électroménagers, les voitures, les capteurs industriels et les dispositifs médicaux) et de fournisseurs de services Internet et mobiles mondiaux (opérateurs de réseaux virtuels mobiles, propriétaires de réseaux, FAI, opérateurs de réseaux privés, grossistes et revendeurs).

- **Chaînes d'approvisionnement mondiales**. Les logiciels, les chipsets et les autres composants des appareils IoT et des réseaux de communication mondiaux proviennent du monde entier.

[99] Raj Samani. McAfee, Royaume-Uni. *Briefing au sous-comité ICR du NSTAC.* Le 15 août 2017.

- **Entités de gestion de l'internet**. Diverses entités sont impliquées dans la gestion et les fonctions essentielles de l'infrastructure mondiale de l'internet, des noms de domaine au routage du trafic. L'Internet Corporation for Assigned Names and Numbers et de nombreuses autres entités participent aux questions de gouvernance ainsi qu'aux activités quotidiennes.

- **Gouvernements individuels et blocs régionaux**. Chaque gouvernement a les mêmes actions et rôles que les États-Unis : utilisateur/acheteur, régulateur et souverain. Les pays ont des approches différentes en matière de réglementation et de politique technologique. Les régions ont également collaboré, les nations européennes et asiatiques travaillant collectivement sur des aspects de la politique technologique et de l'internet, y compris l'IdO. Les efforts nationaux et régionaux alimentent les systèmes et organismes mondiaux.

- **Organismes de normalisation mondiaux et coopératives industrielles**. Des dizaines d'organismes de normalisation, de l'Institute of Electrical and Electronics Engineers à l'Alliance for Telecommunications Industry Solutions et à l'ISO, définissent les normes et protocoles technologiques internationaux. Leur travail repose sur le consensus pour promouvoir de véritables innovations dans le domaine des réseaux de communication, notamment l'interopérabilité. Ils s'appuient sur l'expertise et la participation d'une communauté internationale. Les groupes industriels travaillent également ensemble, par exemple la GSMA, la Telecommunications Industry Association et d'autres. Et certains groupes régionaux, comme l'American Registry for Internet Numbers, sont essentiels à la mise en réseau des communications au niveau mondial.

Les botnets constituent une menace mondiale. Plus de 80 % du trafic des botnets provient de l'étranger.[100] Pour relever le défi des botnets, il faut une coopération internationale pour élaborer des normes, et tous les pays doivent s'efforcer de sécuriser leurs réseaux et leurs appareils.

L'effort du gouvernement britannique comme exemple

Les pays adoptent des approches variées, mais les efforts les plus prometteurs comprennent de véritables partenariats entre le secteur privé et le gouvernement, sans crainte de responsabilité ou de récrimination. Par exemple, le travail proactif en cours au Royaume-Uni, qui comprend des campagnes de sensibilisation du public, des pratiques gouvernementales internes et des partenariats privé-public, a permis de sécuriser davantage les réseaux. [101]

- **Campagnes de sensibilisation du public**. Le gouvernement britannique a lancé une série de campagnes de sensibilisation visant à éduquer le public sur des pratiques plus sûres. Il a collaboré avec les grands fabricants d'appareils pour promouvoir les comptes d'authentification à deux facteurs, qui réduisent les problèmes de sécurité liés aux mots de passe volés. Le gouvernement utilise également ses sites web pour rappeler aux utilisateurs de mettre à jour leurs logiciels. Par exemple, les déclarants qui utilisent un logiciel obsolète pour soumettre leurs déclarations sont avertis de mettre à jour leur logiciel et ne pourront pas déposer de déclaration s'ils ne le font pas avant la prochaine période de déclaration. Le gouvernement lance un partenariat avec le monde universitaire pour traduire les données et les statistiques relatives à la cybersécurité et à l'hygiène en informations et en graphiques.

[100] Mike Bergman. Consumer Technology Association. *Briefing au sous-comité ICR du NSTAC.* 3 août 2017 (indiquant qu'environ 89 % des lieux d'attaque de l'attaque Mirai/Dyn étaient situés dans un pays étranger).
[101] Ian Levy. Centre national de cybersécurité du Royaume-Uni. *Briefing au sous-comité ICR du NSTAC.* Le 9 août 2017.

que le public peut comprendre. Ces mesures importantes aideront le public à comprendre l'importance de la cybersécurité et à prendre les mesures appropriées pour modifier son comportement.

- **Pratiques internes du gouvernement**. Le Royaume-Uni protège son empreinte en ligne. Il a ajouté l'authentification, la notification et la conformité des messages basés sur le domaine à chaque domaine gouvernemental du pays afin d'empêcher l'usurpation d'adresses électroniques. Pour réduire les attaques de logiciels malveillants, le gouvernement effectue une analyse automatique de tout site utilisant un nom gov.uk. Le gouvernement protège également la marque gov.uk en traquant et en supprimant de manière agressive les sites Web usurpant le nom gov.uk. Le gouvernement prend également des mesures pour mieux gérer son entreprise. Il recueille des données sur les agences qui sont en retard sur les mises à jour et s'en sert pour obliger les intégrateurs de systèmes à s'améliorer, sous peine de voir le gouvernement publier ces informations à l'intention du public. Le gouvernement s'efforce également de ne pas acheter de logiciels peu sûrs ou qui n'ont pas été validés.

- **Partenariats public-privé**. Les partenariats entre le gouvernement britannique et le secteur privé permettent de prévenir les attaques et de rendre les réseaux plus sûrs. Par exemple, le gouvernement a demandé aux hébergeurs de supprimer ou de corriger le trafic nuisible, ce qui a entraîné une diminution spectaculaire de la disponibilité du phishing, du webinject et du phishing de marque gouvernementale. Selon les informations fournies par le Quartier général des communications du gouvernement britannique (GCHQ), le gouvernement a réussi à supprimer 153 magasins de justificatifs de kits d'hameçonnage, 2570 attaques de fraude par frais avancés et 23 000 relais de messagerie. Pour protéger ses réseaux, le gouvernement a construit une structure DNS récursive à l'échelle du secteur public qui comprend un service de filtrage. Il offre ce service gratuitement aux FAI. Selon le GCHQ, en juillet 2017, ce service a bloqué 23 046 domaines uniques hébergeant des contenus malveillants. L'utilisation du service d'atténuation du phishing et des logiciels malveillants du gouvernement a permis de faire tomber 79 567 attaques avec succès. Le gouvernement utilise également une tactique de "name and shame" pour encourager les industries comme les banques et les FAI à intégrer des processus sécurisés dans leurs défenses.

Autres partenariats internationaux

En Europe, le projet "No More Ransom" est une collaboration entre le Centre européen de lutte contre la cybercriminalité, la police néerlandaise et des sociétés commerciales, dont Amazon Web Services. [102] L'initiative a été créée pour servir de dépôt unique de clés de chiffrement dans le but d'améliorer la sécurité mondiale. La communauté informe les victimes du type de ransomware qui les a infectées et a éliminé collectivement plusieurs logiciels malveillants, dont Shade, Chimera et WildFire. Cette initiative fournit également 50 outils de cryptage accessibles au public pour les victimes de ransomware. Des initiatives comme "No More Ransom" sont des mesures importantes que la communauté internationale doit prendre pour lutter contre les réseaux de zombies.

RECOMMANDATIONS POUR LE GOUVERNEMENT

- **Le gouvernement américain devrait élaborer des normes internationales qui ralentiront la prolifération des botnets.** Le Royaume-Uni montre que les gouvernements peuvent jouer un rôle important en modélisant la sécurité et en travaillant avec le secteur privé pour faire en sorte que les réseaux - privés et publics
  - plus sûre. D'autres gouvernements peuvent apprendre de cet exemple ; cependant, les gouvernements

[102] Raj Samani. McAfee, Royaume-Uni. *Briefing au sous-comité ICR du NSTAC.* Le 15 août 2017.

ne peut agir seul. Le gouvernement américain doit collaborer avec le secteur privé pour travailler au sein d'organismes internationaux de normalisation afin de développer des normes inspirées des meilleures pratiques pour guider les gouvernements et les fournisseurs de services. L'adoption généralisée des normes constituera une défense importante.

- **Le gouvernement américain devrait s'orienter vers un cadre international pour la sécurité des dispositifs**. Le développement de dispositifs sécurisés nécessite une coopération internationale. Il s'agit notamment d'identifier un ou plusieurs organismes qui pourraient être chargés de développer un cadre ou une plate-forme pour le partage d'informations sur les caractéristiques de sécurité des dispositifs et les empreintes comportementales et/ou les exigences en matière de correctifs et de mise à niveau. Ces normes peuvent aider les fabricants à développer des dispositifs plus sûrs et aider les entreprises et les consommateurs à mieux gérer leurs dispositifs.

- **Développer une dissuasion internationale contre les attaques des États-nations.** Les États-nations sont aujourd'hui à l'origine d'un nombre important d'attaques de botnets. Pour décourager ce comportement, il faudra que les organismes internationaux et les nations individuelles adoptent une position ferme contre ces actions. Ces actions élimineront une source importante de ces attaques et, plus important encore, commenceront à augmenter le coût pour les attaquants.

MOONSHOT SUR LA 4.0 CYBERSÉCURITÉ

La section précédente du présent rapport (*section 3.0*) s'est concentrée sur les recommandations à court terme liées aux meilleures pratiques et technologies existantes et connues qui, si elles étaient mises en œuvre à plus grande échelle, pourraient avoir un impact tangible immédiat sur la réduction de la menace de cyberattaques automatisées et distribuées. Les conclusions du sous-comité ICR du NSTAC ont renforcé la recommandation précédente du NSTAC dans le *rapport du NSTAC au président sur la vision stratégique des technologies émergentes103* selon laquelle les défis actuels de la nation en matière de cybersécurité ne sont pas principalement limités par l'environnement technologique mais par des facteurs contrôlés par l'homme, tels que divers défis juridiques, comportementaux et éducatifs qui ont jusqu'à présent limité le déploiement des meilleures pratiques de cybersécurité largement acceptées.

Alors que la mise en œuvre complète des recommandations de la *section 3.0 aurait un* impact tangible sur la cybersécurité de la Nation, ces recommandations collectives représentent en fin de compte toujours des solutions incrémentielles qui sont insuffisantes pour relever la totalité des défis de cybersécurité plus fondamentaux et persistants de la Nation. En outre, le NSTAC a conclu que le paysage technologique actuel et émergent - y compris les avancées significatives dans l'apprentissage automatique, le cloud et l'informatique quantique - fournit la base nécessaire pour réaliser une transformation radicale de la cybersécurité. Le NSTAC a déterminé que les efforts manquent principalement d'une unité d'effort nationale concertée et d'une orientation stratégique. À ce titre, le NSTAC réitère sa recommandation, mentionnée pour la première fois dans le *rapport du NSTAC au président sur la vision stratégique des technologies émergentes*, selon laquelle le gouvernement devrait mettre en place un projet national de cybersécurité.

[103] NSTAC. *Rapport du NSTAC au Président sur les visions stratégiques des technologies émergentes*, https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20%287-10-17%29%20v3%20%281%29-%20508.pdf

Avec l'aval de la Maison Blanche, le NSTAC s'engage à lancer le concept de cybersecurity Moonshot afin de fournir des conseils au secteur privé sur la manière dont le gouvernement pourrait coordonner le plus efficacement possible un effort national. Sur la base du consensus du NSTAC et de l'EOP, cette étude serait limitée dans le temps pour refléter à la fois l'urgence à court terme du défi de la cybersécurité, tout en assurant une rigueur et une exhaustivité appropriées pour une initiative de cette ampleur. Pour mener à bien cette étude, le NSTAC propose un plan d'action initial en deux volets.

Définir le processus : Principes fondamentaux des modèles Moonshot

La première phase de l'étude du NSTAC examinera les modèles réussis, indépendamment de l'industrie ou du sujet, qui reflètent généralement les principes fondamentaux des efforts de Moonshot. Le NSTAC regardera bien au-delà du domaine de la cybersécurité pour identifier les leçons tirées des efforts de mobilisation nationale précédemment réussis. Cette première phase d'étude s'attachera à répondre à la question fondamentale : *Quels sont les principes fondamentaux et déterminants qui sont cohérents dans les modèles Moonshot réussis ?*

Comme base de départ, le NSTAC s'attachera à identifier d'autres initiatives caractérisées par les principes énumérés ci-dessous. Ces éléments proposés ne sont que des lignes directrices pour informer la portée initiale de l'étude et ne seraient pas considérés comme exhaustifs. Au moment de la rédaction de ce document, le NSTAC est arrivé à la conclusion que pour qu'un effort soit qualifié de Moonshot, il doit être caractérisé par au moins les éléments suivants :

- **Appel national à l'action :** Le gouvernement, aux plus hauts niveaux, doit publiquement considérer un problème comme ayant une conséquence nationale importante et déclarer que sa solution est une priorité stratégique nationale.

- **Axé sur l'objectif final** : Le gouvernement doit mettre l'accent sur une vision stratégique orientée vers un objectif final ambitieux, avec une échéance définie dans le temps, sans définir de manière prescriptive les étapes progressives nécessaires pour atteindre cet objectif final.

- **Processus multipartite :** Le gouvernement doit catalyser l'effort national en tirant parti de ses pouvoirs de rassemblement uniques et en créant les mécanismes de collaboration appropriés nécessaires pour mobiliser officiellement la communauté multipartite, y compris au moins l'industrie privée et le monde universitaire, afin d'atteindre l'objectif final stratégique défini.

Définir précisément le projet de cybersécurité (Cybersecurity Moonshot)

La deuxième phase de l'étude du NSTAC sera axée sur l'application au domaine de la cybersécurité des enseignements tirés de ces efforts nationaux de Moonshot. Cette deuxième phase visera à fournir davantage de clarté et de recommandations sur les considérations clés en matière de cybersécurité liées aux principes identifiés du Moonshot (appel à l'action, objectif final et processus multipartite) et d'autres encore à identifier. Ainsi, dans cette deuxième phase de l'étude, le NSTAC entendra une variété d'experts en cybersécurité et d'autres personnes pour définir de manière appropriée l'objectif final déclaré et les sous-éléments de l'objectif final. Cette phase cherchera à répondre à la question suivante : *Qu'est-ce qu'un moonshot correctement délimité, appliqué au domaine de la cybersécurité ?*

5.0 LE GOUVERNEMENT DOIT COLLABORER AVEC L'INDUSTRIE

Le gouvernement doit prendre l'initiative de s'attaquer aux menaces de cybersécurité qui pèsent sur notre avenir numérique et connecté. Ces menaces proviennent des États-nations, du crime organisé, des hacktivistes, des terroristes et d'autres acteurs. Le secteur privé ne peut y parvenir seul. Le gouvernement fédéral doit jouer un rôle de premier plan au niveau national et international, en encourageant la collaboration entre les secteurs économiques et les frontières politiques. Le NSTAC recommande les activités suivantes que le gouvernement doit mener pour assurer la sécurité de l'IdO.

Protéger et étendre les partenariats public-privé, qui ont été le fondement de la cyberpolitique fédérale. Depuis des décennies, l'industrie collabore avec le DHS dans des instances telles que le NCCIC et l'U.S. Computer Emergency Readiness Team. L'industrie travaille également avec le gouvernement au sein du CSRIC, du Conseil consultatif sur la technologie et d'autres instances, notamment le NIST et le NTIA.

L'industrie a collaboré avec le gouvernement pour protéger les infrastructures critiques. En réponse au décret présidentiel 13636, qui demandait l'identification et la protection des infrastructures critiques, huit directeurs généraux du secteur financier ont lancé une initiative visant à améliorer la cybersécurité des services financiers de base, connue sous le nom de Financial Systemic Analysis and Resilience Center (FSARC). Le FSARC, en collaboration avec le gouvernement, coordonne les campagnes contre les principaux adversaires, élabore et partage les meilleures pratiques et les leçons apprises, contribue aux affaires criminelles à l'appui de l'application de la loi fédérale, et exploite l'accès et les informations du gouvernement américain pour identifier les endroits où l'activité criminelle est alignée sur les acteurs du renseignement étranger ou utilisée par eux. [104] Le secteur privé a contribué à l'élaboration et à la mise en œuvre du cadre de cybersécurité du NIST et les secteurs l'ont adapté à leurs besoins spécifiques. Par exemple, le document final de mars 2015 du CSRIC IV, *Cybersecurity Risk Management and Best Practices*, [105] fournit des conseils pour aider les fournisseurs de communications à utiliser et à adopter le cadre de cybersécurité du NIST. Les initiatives de ce type sont particulièrement utiles pour les petits fournisseurs opérant avec des budgets limités.

Ces partenariats reposent sur la confiance et doivent rester à l'abri de la menace de la réglementation et de l'application des lois.

Envisager des moyens créatifs pour encourager le partage d'informations sur les vulnérabilités, y compris des protections en matière de responsabilité et des zones de sécurité. Si les opérateurs et les fabricants doivent discuter des vulnérabilités des produits et des services, il faut reconnaître les risques associés à cette démarche et protéger cette activité. Les programmes de divulgation des vulnérabilités sont intéressants, mais peuvent manquer de composants clés pour fonctionner. En 2016, le DHS a indiqué qu'il devrait réunir un groupe de partenaires pour examiner la responsabilité, entre autres questions. [106] L'Institut de la Chambre de commerce des États-Unis pour la réforme juridique et d'autres organismes se sont penchés sur ces questions ; par exemple, dans *Torts of the Future*, la Chambre note que " les fabricants de produits connectés sont confrontés à d'importants risques de responsabilité découlant de ce qui suit .

[104] Scott DePasquale. Centre d'analyse et de réponse des services financiers. *Briefing au sous-comité ICR du NSTAC.* 10 août 2017

[105] FCC, CSRIC IV, Groupe de travail 4 : Rapport final*, Groupe de travail sur la gestion des risques et les meilleures pratiques en matière de cybersécurité*. Mars 2015.https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[106] Voir DHS. "Principes stratégiques pour la sécurisation de l'Internet des objets (IoT)". Version 1.0. 15 novembre 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things- 2016-1115-FINAL.....pdf.

Le gouvernement fédéral doit examiner comment le risque de litige civil et notre système judiciaire litigieux peuvent entraver les activités bénéfiques.

Identifier et traiter les limites juridiques qui restreignent les mesures défensives du secteur privé. Les mesures DDoS et autres mesures d'atténuation peuvent exposer les entreprises à des risques en vertu du droit fédéral. Elles peuvent également avoir des conséquences inattendues, telles que des dommages à des tiers en cas d'erreurs d'attribution. Le gouvernement doit identifier ses objectifs en matière de défense active et le rôle du secteur privé.
En outre, le gouvernement doit se demander si les protections et les pouvoirs prévus par la CISA sont suffisants. La protection pour le partage des indicateurs de cybermenaces et des mesures défensives pourrait ne pas être suffisante. Une protection appropriée de la responsabilité des fournisseurs d'accès Internet et d'autres acteurs sera essentielle pour développer davantage les mesures défensives et le partage d'informations. Le langage législatif relatif à la protection de la responsabilité doit être mis à jour en même temps que l'élargissement du rôle des membres de l'écosystème.

Ajuster le mode de fonctionnement des services de renseignement américains face aux cybermenaces. Le National Infrastructure Advisory Council (NIAC) a récemment évalué les approches du Royaume-Uni et d'Israël en matière de collecte de renseignements. [109] Le NIAC suggère qu'une " coordination efficace et rapide passe par une autorité centrale capable de coordonner les cyberpriorités de la nation, d'aligner les ressources de l'industrie et du gouvernement et de fournir un leadership national pour la cyberdéfense ".[110] Le rapport examine en outre les efforts déployés au Royaume-Uni pour créer le U.K. National Cyber Security Centre et le National Cyber Bureau israélien. Le NSTAC recommande au gouvernement américain d'évaluer ces modèles et de déterminer si certains des concepts en cours de développement au Royaume-Uni et en Israël peuvent être utiles pour organiser les efforts du gouvernement américain en matière de cybersécurité. Le NSTAC recommande également que les États-Unis envisagent de modifier leurs méthodes de collecte de renseignements cybernétiques en permettant à un analyste de se concentrer uniquement sur une cible pendant une période plus longue, devenant ainsi un expert et peut-être plus capable de combattre une attaque spécifique de sa cible.

Améliorer le partage des informations avec le secteur privé. Le gouvernement a accès à des informations de renseignement ; cependant, le processus de partage de ces informations au niveau classifié peut être lourd. Le NSTAC recommande au président d'ordonner au gouvernement fédéral de procéder à un examen des programmes d'information existants afin de déterminer s'ils atteignent les objectifs et de recommander de nouvelles approches, même sur une base pilote, pour permettre un meilleur partage de l'information. Le gouvernement devrait également reconnaître que tous les destinataires de l'information n'ont pas les mêmes capacités. Il devrait y avoir une gamme de modèles de partage de l'information disponibles en fonction des capacités de chaque partie.

Éliminer l'excès de réglementation aux niveaux fédéral, étatique et local. Le secteur privé est préoccupé par les obligations réglementaires, les mandats techniques et les régimes d'établissement de rapports qui

[107] Institut de la Chambre américaine pour la réforme juridique. " Les délits civils du futur - Aborder les implications en matière de responsabilité et de réglementation des technologies émergentes. " Mars 2017. http://www.instituteforlegalreform.com/uploads/sites/1/_Torts_of_the_Future_Addressing_the_Liability_and_Regulaty_Implications_of_Emerging_Technologies_April_2017.pdf?pagename=uploads/sites/1/Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_.pdf.

[108] Section 104(c) du Cyber and Information Sharing Act of 2015, 6. U.S.C. 1504.

[109] NIAC. "Securing Cyber Assets-Addressing Urgent Cyber Threats to Critical Infrastructure". Août 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

[110] Rapport du NIAC au président " Securing Cyber Assets ", à la page 19 (août 2017), disponible à l'adresse https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

Les organismes de réglementation ne sont pas en mesure d'utiliser des ressources précieuses et encouragent un état d'esprit de conformité qui privilégie une mentalité de "vérification de la boîte" au lieu d'une innovation agile et agressive. Dans le domaine de la cybersécurité, les menaces, les vulnérabilités et les réponses évoluent de manière exponentielle, plus vite que n'importe quel régulateur. Si le gouvernement veut de véritables partenaires, il doit indiquer clairement que la collaboration et les meilleurs efforts ne rebondiront pas sur le secteur privé en matière de réglementation et d'application punitive. Le gouvernement fédéral doit décourager l'activité des États, qu'il s'agisse de mandats techniques, de charges liées à la protection de la vie privée en ligne ou d'autres mesures, car elles peuvent compliquer et entraver le développement de produits et de services.

Le gouvernement peut reconnaître qu'il y a, et qu'il continuera d'y avoir, une activité des États, qu'il s'agisse de mandats techniques, de charges liées à la confidentialité en ligne ou d'autres mesures, et que certains de ces efforts peuvent fragmenter et compliquer le développement de produits et de services. Compte tenu de cette réalité, le NSTAC recommande que le gouvernement fédéral encourage d'abord les États à adopter et à mettre en œuvre les meilleures pratiques et recommandations disponibles en matière de cybersécurité pour leurs propres organisations et systèmes administratifs, puis à promouvoir les mêmes pratiques pour les résidents et l'écosystème commercial des États. Les États devraient être encouragés à participer à des réunions nationales avec les principales parties prenantes afin de parvenir à des approches cohérentes en matière de cybersécurité. Il s'agit notamment de la National Governors Association, de la National Association of State Chief Information Officers, de la National Conference of State Legislatures et du DHS State, Local, Tribal, and Territorial Government Coordinating Council.

Représenter agressivement la politique et les intérêts économiques des États-Unis à l'étranger. Le secteur mondial des TIC a besoin que le gouvernement américain joue un rôle moteur à l'étranger. Les régions et les pays abordent la sécurité et la technologie de manière divergente. Il en va de la sécurité nationale et de l'intérêt économique que les États-Unis défendent vigoureusement des marchés ouverts, la neutralité technologique et des processus de normalisation transparents. Si les États-Unis ne prennent pas l'initiative, les normes juridiques et les réglementations prescriptives d'autres pays pourraient établir des références internationales et ralentir la croissance internationale des entreprises américaines.

Promouvoir le développement de la main-d'œuvre en matière de cybersécurité. De nombreux rapports recommandent au gouvernement de remédier aux insuffisances de la main-d'œuvre en matière de cybersécurité qui risquent de paralyser notre capacité à répondre aux menaces croissantes. Citons par exemple le rapport du NIAC (qui suggère un programme d'échange d'experts public-privé, par exemple),[111] le rapport final du CSRIC, *Cybersecurity Workforce Development Best Practices Recommendations*,[112] divers efforts du DHS, notamment la création de l'initiative nationale pour les carrières et les études en matière de cybersécurité,[113] le National Cybersecurity Workforce Framework,[114] le Cybersecurity Workforce Development Toolkit,[115]

[111] NIAC. "Securing Cyber Assets-Addressing Urgent Cyber Threats to Critical Infrastructure". Recommandation 4. Août 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17- 508.pdf.

[112] CSRIC. Rapport final du WG7. "Recommandations sur les meilleures pratiques en matière de développement de la main-d'œuvre en cybersécurité." Mars 2017. https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

[113] NICCS, https://niccs.us-cert.gov/.

[114] NICCS. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber- security-workforce-framework.

[115] NICCS. "Boîte à outils pour le développement de la main-d'œuvre en cybersécurité - Comment créer une main-d'œuvre solide en cybersécurité." Mars 2017. https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf.

et le rapport sur l'amélioration de la cybersécurité dans le secteur des soins de santé116 (juin 2016). En outre, le personnel chargé de la cybersécurité pourrait devoir comprendre à la fois le codage et les langues étrangères, car la plupart des botnets sont codés à l'aide de langues autres que l'anglais. Il y a beaucoup de travail à faire, mais un consensus s'est dégagé sur le fait qu'il s'agit d'un domaine essentiel pour l'attention du gouvernement.

Faire preuve de prudence dans l'utilisation du système de passation de marchés pour aborder la cybersécurité de l'IdO. Le gouvernement devrait réfléchir à la manière de garantir que ses produits et services sont sécurisés de manière appropriée. Cependant, le gouvernement doit éviter de se concentrer de manière disproportionnée sur les dispositifs ou de s'appuyer sur des mandats unilatéraux pour obtenir cette sécurité renforcée. Le NSTAC recommande au gouvernement d'explorer les services gérés qui peuvent être offerts par des experts du secteur privé. Cela permettrait au gouvernement d'exploiter l'expertise et l'envergure du secteur privé (FAI, fournisseurs de nuages, autres fournisseurs de services à des tiers) plutôt que d'utiliser des mandats de sécurité des appareils plus rudimentaires.

Développer des groupes de réflexion pour explorer les opportunités du Moonshot. Au lieu de répéter des idées déjà tentées, comme l'extension d'un nouveau protocole IP, le gouvernement devrait identifier de nouvelles approches. Le NSTAC recommande au gouvernement d'explorer la création de partenariats collaboratifs et innovants et de groupes de réflexion semblables au Centre d'excellence national de cybersécurité du NIST, qui s'associe au secteur privé, aux universités et à d'autres agences pour trouver des solutions aux problèmes technologiques. Une autre approche à envisager est une structure similaire à celle de la Defense Advanced Research Projects Agency, axée sur la cybernétique, qui bénéficie de pouvoirs d'embauche statutaires spéciaux et d'instruments contractuels alternatifs qui lui permettent de tirer parti des possibilités de faire progresser sa mission.

6.0 CONCLUSION

Les botnets et les attaques qu'ils facilitent ne devraient que croître. L'atténuation de ce problème complexe nécessitera diverses actions de la part de l'écosystème Internet. Si le présent rapport fournit des recommandations aux fabricants de dispositifs, aux fournisseurs de services réseau, aux développeurs de logiciels, aux entreprises et aux pouvoirs publics, ces entités ne sont pas les seules à devoir participer à l'atténuation de la menace. La cybersécurité est une responsabilité partagée et dépend du rôle de chaque partie de l'écosystème. Le NSTAC s'attend également à ce que l'éventail des solutions évolue avec le temps. Ainsi, le NSTAC ne prévoit pas que le présent rapport ou les processus qui lui succéderont seront statiques. Pour relever ce défi, il faudra une collaboration et un engagement permanents entre le secteur privé et le gouvernement. Enfin, bon nombre des recommandations sont itératives et ne changeront pas fondamentalement la nature sous-jacente du problème. Pour cette raison, le NSTAC recommande qu'une étude future du NSTAC examine la possibilité d'un Moonshot sur la cybersécurité visant à cibler l'infrastructure Internet sous-jacente et à recommander des améliorations à long terme.

[116] Groupe de travail sur la cybersécurité dans l'industrie des soins de santé (groupe de travail HCIC). "Rapport sur l'amélioration de la cybersécurité dans l'industrie des soins de santé". Recommandation 6.4. Juin 2017. https://www.phe.gov/Preparedness/planning/ CyberTF/Documents/report2017.pdf.

ANNEXE A : L'APPEND APPEND DE L'APPEND APPEND APPEND DE L'APPEND APPEND DE MEMBRE

MEMBRES DU SOUS-COMITÉ

M. Raymond Dolan, Sonus Networks Inc. et coprésident du sous-comité M. John Donovan, AT&T Inc. et coprésident du sous-comité

M. Chris Boyer, AT&T Inc. et coprésident du groupe de travail ICR M. Kevin Riley, Sonus Networks Inc. et coprésident du groupe de travail ICR

AT&T, M. Inc.	Jonathan Gannon M. Bill O'Hern
Avaya, Inc.	M. Vico Loquerico
CenturyLink, Inc.	Mme Kathryn Condello M. Paul Diamond M. John Schiel M. Donald Smith
Technologies de la communication, Inc.	M. Milan Vlajnic
Département de Homeland Security	M. Gregory Shannon
Diogène Group, LLC	M. William Gravell
Dun & Bradstreet M. Corporation	Gregory Mortensen M. Jon Rose
Equinix, Inc.	Mme Cindy Liu
ForeScout Technologies, Inc.	M. Tamer Baker Mme Katherine Gronberg
Lockheed Martin Corporation	M. Darrell Durst
Microsoft Corporation	M. Richard Boscovich Mme Amanda Craig Deckard
McAfee, LLCM. Patrick Flynn	M. Kent Landfield
Sécurité nationale Agency	Mme Cheri Caddy
National Telecommunications and Information Administration	M. Shawn Cochran Mme Megan Doscher

	Mme Evelyn Remaley
National Institute of Standards and Technology	M. Tim Polk M.
NCTA - The Internet & Television Association	Matt Tooley Mme
Neustar, Inc.	Terri Claffey
Oracle Corporation	Dr Prescott Winter M.
Palo Alto Networks, Inc.	Sean Morgan M.
Raytheon Company Unisys	Michael Daly
Corporation	M. Mark Cohn M. Tom Patterson
USTelecomm	M. Robert Mayer
Verizon Communications, Inc.	M. Kevin Kirsche M. Timothy Vogel

BRIEFERS - EXPERTS EN LA MATIÈRE

Arbor Networks, Inc.	Mme Arrabelle Hallawell
AT&T, Inc.	M. Brian Rexroad M. Bill O'Hern
CA Technologies, Inc.	M. Jaime Brown
Center for Democracy and Technology	Mme Michelle Richardson
Consumer Technology Association Cyber	M. Mike Bergman
Threat Alliance	M. Michael Daniel M.
Département de la défense	Mitchell Komaroff Dr.
Département de la sécurité intérieure	Ann Cox
Département de la justice	M. Leonard Bailey
Dun & Bradstreet Corporation	Dr Anthony Scriffignano
Ambassade du Japon	M. Daisuke Hayashi

Federal Bureau of Investigation	M. Tom Grasso
ForeScout Technologies, Inc.	M. Wallace Sann
Financial Services Analysis & Response M. Center	Scott DePasquale
Financial Systematic Analysis & Resilience Center M.	Bill Nelsen
Ministère japonais des affaires intérieures et de la communication	M. Atsushi Goto M. Yasu Taniwaki
Centre national japonais de préparation et de stratégie industrielle pour la cybersécurité	Mme Kasumi Sugomoto
Intelligence Advanced Research Project Agency	M. Kerry Long M.
McAfee Royaume-Uni	Raj Samani M.
Micron Technology, Inc.	Steve Wallach
Microsoft	M. Richard Boscovich M. Rob Spiger
NCTA - The Internet & Television Association	M. Matt Tooley
Agence de sécurité nationale	Mme Cheri Caddy
Institut national des normes et de la technologie	M. Andrew Regenscheid Dr. Charles Romine
Neustar, Inc.	M. Barrett Lyon M.
Oracle	Travis Russell M.
Palo Alto Networks, Inc.	Kevin Walsh M. J.F.
Raytheon Company sn3rd	Mergen M. Sean
LLC	Turner
Unisys Corporation	M. Brent Houlahan M. Jack Koons
United Kingdom Nation Cyber Security Centre US	Dr Ian Levy Dr
Marine Corps	Ray Letteer

USTelecom	M. Robert Mayer
Venable LLP	M. Ari Schwartz
VeriSign, Inc.	M. Danny McPherson Dr. Eric Osterweil

GESTION DES SOUS-COMITÉS

Fédéral désigné par le NSTAC Officer	Mme Helen Jackson
Alternate NSTAC DFO	Mme Sandy Benevides Mme DeShelle Cleghorn
Booz Allen Hamilton, Inc.	Mme Ursula Arno M. William Hyde
Total Systems Technology Corporation	M. Robert Carter

L'ANNEXE B : L'AC AC AC AC AC S

5G Cinquième génération
ABC Code de conduite ABC anti-botnet
Intelligence AI artificielle
BCP Meilleures pratiquesBCP communes
Protocole de BGP passerelle frontalière
Protocole du BYOD Bring Your Own Device
CharGen générateur de caractères
Loi sur le CISA partage des informations relatives à la cybersécurité
CITL Cybersecurity Independent Testing Laboratory CNSSI
Comité d'instruction des CITL Cybersecurity
Independent Testing Laboratory CNSSI systèmes de sécurité
nationale
CSRIC Sécurité, fiabilité et interopérabilité des communications Council CTA
Consumer Technology Association
CVD Coordinated Vulnerability Disclosure
DDoS Déni de service CVD Coordinated
Vulnerability Disclosure DDoS distribué
DHS Département de la sécurité DHS intérieure
Système de DNS nom de domaine
DNSSEC Domain Name System Security Extensions
DOC Département du commerce
DoD Département de la défense
DOJ Ministère de la Justice
DoS Déni de service
Ordre EO exécutif
EOP Executive Office of the President ETSV
Technologie émergente stratégique Vision
FBI Federal Bureau of Investigation
Commission FCC fédérale des FCC communications
FSARC Analyse systémique financière et résilience Center
FTC Federal Trade Commission
Gbps Gigabits par seconde
GCHQ Government Communications Headquarters
GSMA Groupe Spécial Mobile Association
Système de ICR Internet and Communications Resilience
ICS contrôle industriel
Forum Technologies IEC International Electrotechnical
Commission IETF technique sur l'ingénierie de l'ICT
information et des communications sur
Technologies IEC International Electrotechnical Commission
IETF Internet
IoT Internet des objets
Protocole IP Internet
IPv6 Protocole Internet version 6
Fournisseurs de ISO International Organization for
Standardization ISP services Internet
Technologies de l'IT information
M2M De machine à machine
Groupe de M3AAWG travail sur la messagerie, les logiciels malveillants et la lutte contre les abus
mobiles

MUD Fabricant Utilisation Description
Centre NCCIC national d'NCCIC intégration de la cybersécurité et des communications
NCCoE National Institute of Standards and Technology National Cybersecurity Center of Excellence (NCCoE Institut national des normes et de la technologie)
Virtualisation des NFV fonctions réseau
Conseil NIAC consultatif national sur l'infrastructure
Dispositifs de NIST National Institute of Standards and Technology NISTIR NIST Glossary of Information Security Terms NMD surveillance du réseau
NS/EP Sécurité nationale/Préparation aux situations NS/EP d'urgence
Protocole de NSTAC National Security Telecommunications Advisory Committee
NTIA National Telecommunications and Information Administration NTP temps réseau
Système d'OS exploitation
Infrastructure à RPKI clé publique des RPKI ressources
SAFECode Forum d'assurance logicielle pour l'excellence dans le cycle de vie du Code SDL développement de la sécurité
Réseau SDN défini par logiciel
SS7 Système de signalisation 7
Royaume-Uni
UL Underwriters Lab
États-Unis
Réseau VPN privé virtuel

5G - Un futur réseau mobile de cinquième génération, dont les spécifications n'ont pas été entièrement définies par l'Union internationale des télécommunications. Il devrait prendre en charge des débits de données de 10 gigabits par seconde et plus. Les déploiements commerciaux de la 5G ne sont pas prévus avant 2020 environ. (Dictionnaire des télécommunications de Newton)

Intelligence artificielle - L'intelligence dont font preuve les machines ou les logiciels. Terme popularisé par Alan Turing, il décrit historiquement une machine capable de faire croire aux gens qu'elle est un être humain grâce au test de Turing. Récemment, les scientifiques de ce domaine ont largement abandonné cet objectif pour se concentrer sur le caractère unique de l'intelligence des machines et apprendre à travailler avec elles de manière intelligente et utile. (Dictionnaire Newton's Telecom)

Authentification - Le processus par lequel un utilisateur, une source d'information ou simplement une information prouve qu'il est bien celui qu'il prétend être ; le processus de détermination de l'identité d'un utilisateur qui tente d'accéder à un réseau et/ou à un système informatique. (Newton's Telecom Dictionary)

Botnet - Réseau d'ordinateurs connectés à Internet qui ont été infectés par le logiciel de commande et de contrôle d'un tiers malveillant et qui peuvent être commandés à distance par ce tiers pour effectuer des actions nuisibles telles que des attaques sur Internet. (Newton's Telecom Dictionary)

Cloud Computing - Modèle permettant un accès réseau à la demande à un pool partagé de capacités/ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services), qui peut être rapidement approvisionné et libéré avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services. Il permet aux utilisateurs d'accéder à des services technologiques à partir du nuage de réseaux sans avoir de connaissances, d'expertise ou de contrôle sur l'infrastructure technologique qui les prend en charge. Les données de l'utilisateur et les services de sécurité essentiels peuvent résider et être gérés dans le nuage de réseau. (Committee on National Security Systems Instruction (CNSSI) 4009, Adapté) (Rapport NSTAC 2016)

Infrastructure critique - Système et actifs, physiques ou virtuels, si vitaux pour les États-Unis que l'incapacité ou la destruction de ces systèmes et actifs aurait un impact débilitant sur la sécurité, la sécurité économique nationale, la santé ou la sécurité publique nationale, ou toute combinaison de ces éléments. Les infrastructures critiques peuvent être détenues et exploitées tant par le secteur public que par le secteur privé. *Critical Infrastructures Protection Act of 2001*, 42 U.S.C. 5195c(e)] (CNSSI 4009, Adapté)

Cyberattaque - Attaque, via le cyberespace, visant l'utilisation du cyberespace par une entreprise pour perturber, mettre hors service, détruire ou contrôler de manière malveillante un environnement/infrastructure informatique, ou détruire l'intégrité des données ou voler des informations contrôlées. (CNSSI 4009)

Cybersécurité - La capacité de protéger ou de défendre l'utilisation du cyberespace contre les cyberattaques. (CNSSI 4009)

Attaques par déni de service - Empêcher l'accès autorisé aux ressources ou retarder les opérations dont le temps est critique. Le temps critique peut être de quelques millisecondes ou de plusieurs heures, selon le service fourni. (CNSSI 4009)

Attaques par déni de service distribué - Technique de déni de service qui utilise de nombreux hôtes pour réaliser l'attaque et empêche l'accès autorisé aux ressources ou retarde les opérations à délai critique. (Glossaire NIST des termes de sécurité de l'information - (NISTIR) 7298 - Révision 2)

Pare-feu - Pièce de matériel ou de logiciel, ou matériel et logiciel, qui empêche les personnes non autorisées d'accéder à un ordinateur ou à un réseau informatique. (Newton's Telecom Dictionary)

Internet des objets - Ensemble des réseaux de dispositifs interconnectés. (Newton's Telecom Dictionary)

Protocole Internet (IP) - Partie de la famille de protocoles Transmission Control Protocol/IP décrivant un logiciel qui suit l'adresse Internet des nœuds, achemine les messages sortants et reconnaît les messages entrants. Il est également utilisé dans les passerelles pour connecter les réseaux de niveau 3 et plus de l'Open Systems Interconnection Network. (Newton's Telecom Dictionary)

Malware - Logiciel créé et distribué à des fins malveillantes, comme l'invasion de systèmes informatiques sous la forme de virus, de vers ou d'autres plug-ins et extensions qui masquent d'autres capacités destructrices. (Dictionnaire Newton Telecom)

Communications de sécurité nationale/préparation aux situations d'urgence (NS/EP) - Services de télécommunications utilisés pour maintenir un état de préparation ou pour réagir et gérer tout événement ou crise (local, national ou international) qui cause ou pourrait causer des blessures ou des dommages à la population, des dommages ou des pertes de biens, ou qui dégrade ou menace la position NS/EP des États-Unis (47 Code of Federal Regulations Chapitre II, § 201.2(g)). Les communications NS/EP comprennent principalement les capacités techniques soutenues par des politiques et des programmes qui permettent à l'exécutif de communiquer à tout moment et en toutes circonstances afin de remplir les fonctions essentielles de sa mission et de répondre à tout événement ou crise (locale, nationale ou internationale), y compris la communication avec lui-même, les pouvoirs législatif et judiciaire, les gouvernements des États, des territoires, des tribus et des localités, les entités du secteur privé, ainsi que le public, les alliés et les autres nations. Les communications NS/EP comprennent également les systèmes et les capacités à tous les niveaux du gouvernement et du secteur privé qui sont nécessaires pour assurer la sécurité nationale et pour gérer efficacement les incidents et les urgences. (Définition du comité exécutif des communications NS/EP basée sur l'Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions* [2012]).

Réseaux - Système(s) d'information mis en œuvre avec un ensemble de composants interconnectés, qui peuvent comprendre des routeurs, des concentrateurs, des câblages, des contrôleurs de télécommunications, des centres de distribution de clés et des dispositifs de contrôle technique. (Glossaire des termes de sécurité de l'information du NIST (NISTIR) 7298 - Révision 2)

Virtualisation du réseau - Un moyen d'améliorer l'efficacité d'un réseau et de réduire les coûts. Elle consiste à créer plusieurs partitions virtuelles sur un seul matériel. Elle réduit le nombre de

quantité de matériel réseau nécessaire et permet de gérer plusieurs fonctions à partir d'une seule console. (Newton's Telecom Dictionary)

Protocole - Ensemble de règles et de formats, sémantiques et syntaxiques, permettant aux systèmes d'information d'échanger des informations. (Glossaire NIST des termes de sécurité de l'information - NISTIR 7298 - Révision 2)

Software Defined Network - Un réseau privé virtuel. Plus précisément, il fait référence au service de réseau défini par logiciel d'AT&T, qui a été introduit en 1985 pour les plus gros clients d'AT&T et qui ne fournissait que des services d'accès dédiés. (Newton's Telecom Dictionary)

Menace - Toute circonstance ou tout événement susceptible d'avoir un impact négatif sur les opérations de l'agence (y compris la mission, les fonctions, l'image ou la réputation), sur les actifs de l'agence ou sur les individus par le biais d'un système d'information via un accès non autorisé, la destruction, la divulgation, la modification des informations et/ou un déni de service. (NIST SP 800-53, CNSSI 4009, Adapté)

APPENDICE D : BIBLIOGRAPHIE Y

AT&T. *Pratiques de réseau*. 24 avril 2017. https://www.att.com/gen/public-affairs?pid=20879.

Arbor Networks. *Worldwide Infrastructure Security Report,* Volume XII, disponible à l'adresse https://www.arbornetworks.com/insight-into-the-global-threat-landscape.

Bailey, Leonard. DOJ. *Briefing au sous-comité ICR du NSTAC*. Le 10 août 2017. Bergman, Mike.

CTA. Briefing au sous-comité *ICR du NSTAC*. 3 août 2017. Boscovich, Richard. Microsoft. *Briefing*

au sous-comité NSTAC ICR. 16 août 2017. Boyer, Chris. Coprésident de la politique publique du

M3AAWG (AT&T), nouveau *rapport sur les métriques du bot du M3AAWG. Partage du point de vue des opérateurs de réseaux*. 20 octobre 2014. https://www.m3aawg.org/blog/nouveau-m3aawg-bot-metrics-report-shares-network-operators%E2%80%99-perspective.

Burke, Samuel. CNN. *Une entreprise chinoise reconnaît son rôle involontaire dans une cyberattaque.* 24 octobre 2016. http://money.cnn.com/2016/10/23/technology/ddos-cyber-attack-chinese-firm/index.html.

Cisco. *Cisco Visual Network Index : Prévisions et méthodologie, 2016-2021, livre blanc*. 7 juin 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual- networking-index-vni/complete-white-paper-c11-481360.html.

Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030) ; Wiretap Act (18 U.S.C. § 2511) ; Pen Register/Trap and Trace Statutes (18 U.S.C. §§ 3121 *et seq.*) ; Leonard Bailey. *Briefing au sous-comité ICR du NSTAC*. 10 août 2017.

Computer Weekly, "Global Hacker Botnet Tops 6 Million Hijacked Devices", 27 septembre 2017 http://www.computerweekly.com/news/450427023/Global-hacker-botnet-tops-6- million-hijacked-devices.

Consumer Technology Association, *Aperçu du projet : Securing Connected Devices for Consumers in the Home, CTA-CEB33,* 7 juillet 2017. https://standards.cta.tech/apps/group_public/project/details.php?project_id=429.

Cox, Ann. DHS. *Briefing au sous-comité ICR du NSTAC.* Le 1er août 2017. Cyber

Independent Testing Lab (CITL). http://cyber-itl.org/.

Loi de 2015 sur le partage des informations relatives à la cybersécurité, Pub. L. n° 114-113, 129 Stat. 2242 (2015).

CSRIC. Rapport final du WG7. "Recommandations sur les meilleures pratiques de développement de la main-d'œuvre en cybersécurité". Mars 2017. https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.

Département de la Défense (DoD). "Le DOD annonce une politique de divulgation des vulnérabilités numériques et le lancement de "Hack the Army"." *Communiqué de presse*. 21 novembre 2016. https://www.defense.gov/ News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital- vulnerability-disclosure-policy-and-hack-the-army-kick-off/.

Département de la santé et des services sociaux (HHS). "Gestion post-commercialisation de la cybersécurité des dispositifs médicaux-Guide pour l'industrie et le personnel de la Food and Drug Administration." 28 décembre 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Département de la sécurité intérieure (DHS). "Principes stratégiques pour la sécurisation de l'Internet des objets (IoT)". Version 1.0. 15 novembre 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115- FINAL .....pdf.

DHS. Équipe de préparation aux urgences informatiques des États-Unis. *Build Security In.* https://www.us-cert.gov/bsi.

Département de la justice (DOJ), *Cadre pour un programme de divulgation des vulnérabilités pour les systèmes en ligne* juillet 2017. https://www.justice.gov/criminal-ccips/page/file/983996/download.

DOJ. " AlphaBay, le plus grand " marché noir " en ligne, fermé ". 20 juillet 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

DOJ. " Le ministère de la Justice prend des mesures pour désactiver un botnet international ". 13 avril 2011. https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

Groupe de spécialisation industrielle NFV de l'ETSI. *Perspectives des opérateurs de réseaux sur les priorités NFV pour la 5G.* 21 février 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf

Rapport Ericsson sur la mobilité. *Sur le pouls de la société en réseau.* Juin 2016. https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

Federal Communications Commission (FCC), Communications Security Reliability and Interoperability Council (CSRIC) III*, U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers*, mars 2012. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/ CSRIC-III-WG7-Final-ReportFinal.pdf.

FCC, CSRIC II, Groupe de travail 2A : Rapport final*, Meilleures pratiques de cybersécurité*. Mars 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

FCC, CSRIC IV, Groupe de travail 4 : Rapport final*, Groupe de travail sur la gestion des risques et les meilleures pratiques en matière de cybersécurité*. Mars

2015.https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815. pdf.

FCC CSRIC V, Rapport final du groupe de travail 5, *Partage de l'information,* 15 mars 2017. https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

FCC CSRIC. Rapport final du groupe de travail 7, *recommandations sur les meilleures pratiques en matière de développement de la main-d'œuvre en cybersécurité.* Mars 2017. https://www.fcc.gov/files/csric5-wg7- finalreport031517pdf.

FCC CSRIC V, Groupe de travail 10, Réductions des risques hérités (2017) (Rapport sur les réductions des risques hérités), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

Fitzgerald, Brian et Chris Wysopal. Veracode. *Briefing au sous-comité ICR du NSTAC.* Le 1er août 2017.

Commission fédérale du commerce (FTC). " Annonce du gagnant de son concours sur la sécurité des appareils domestiques de l'Internet des objets ". *Communiqué de presse*. 26 juillet 2017. https://www.ftc.gov/news-events/press- releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

FTC. "La FTC approuve l'ordonnance finale réglant les accusations contre TRENDnet. Inc." *Communiqué de presse*. 7 février 2014. https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves- final-order-settling-charges-against-trendnet-inc ; https://www.ftc.gov/news-events/press- releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

FTC. L'Internet des objets : Vie privée et sécurité dans un monde connecté. n.130. Janvier 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

FTC. Défi de l'inspecteur de maison IoT. 2017. https://www.ftc.gov/iot-home-inspector-challenge. FTC.

Staff Report. *Internet des objets : Privacy & Security in a Connected World, FTC.* Janvier 2015. https://www.ftc.gov/system/files/documents/ reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet- things-privacy/150127iotrpt.pdf.

Franceschi-Bicchierai, Lorenzo, *Comment 1,5 million de caméras connectées ont été détournées pour constituer un botnet sans précédent.* 29 septembre 2016. https://motherboard.vice.com/en_us/article/ 8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs.

Université George Washington, Center for Cyber and Homeland Security. *Into the Gray Zone : le secteur privé et la défense active contre les cybermenaces.* Octobre 2016. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL .pdf.

GSA. Vulnerability Disclosure Policy. https://18f.gsa.gov/vulnerability-disclosure-policy/.

GSMA. Lignes directrices en matière de sécurité de l'IdO. Février 2016. https://www.gsma.com/iot/future-iot- networks/iot-security-guidelines/.

Hallawell, Arrabelle. Arbor Networks, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 3 août 2017.

Hartnett, Kevin. WIRED. *Les informaticiens se rapprochent d'un code parfait, à l'épreuve du piratage.* 23 septembre 2016. https://www.wired.com/2016/09/computer-scientists-close-perfect- hack-proof-code/.

Groupe de travail sur la cybersécurité dans le secteur des soins de santé. *Rapport sur l'amélioration de la cybersécurité dans l'industrie des soins de santé.* Juin 2017. https://www.phe.gov/Preparedness/planning/ CyberTF/Documents/report2017.pdf.

Je suis la Cavalerie. *DOT Gov Coordinated Disclosure Timeline.* https://www.iamthe cavalry.org/wp-content/uploads/2016/12/IATC_Gov-Coordinated-Disclosure-Timeline_v1.0.jpg.

Incapsula. *Global DDoS Threat Landscape.* https://www.incapsula.com/ddos-report/ddos-report- q1-2017.html.

Koeberl, Patrick, et, al. "TrustLite : A Security Architecture for Tiny Embedded Devices". http://www.icri-sc.org/fileadmin/user_upload/Group_TRUST/PubsPDF/trustlite.pdf

Lerner, Zach, "Microsoft the Botnet Hunter : The Role of Public-Private Partnerships in Mitigating Botnets", 28 HARV. J.L. & TECH. 237, 247 (2014).

Letteer, Ray. U.S. Marine Corps. *Briefing au sous-comité ICR du NSTAC*. 30 août 2017. Levy, Ian. UK

National Cyber Security Centre. *Briefing au sous-comité NSTAC ICR.* Le 9 août 2017.

McAfee. *Attaque du botnet Mirai IoT : Une illustration de pot de miel.* 5 avril 2017. https://www.youtube.com/watch?v=vnitAXYGmI0.

McAfee. Secure Home Platform Service. https://securehomeplatform.mcafee.com/. Microsoft.

Qu'est-ce que le cycle de vie du développement de la sécurité ? https://www.microsoft.com/en-. us/sdl/default.aspx.

Mitchell, Charlie. "Le fondateur de Black Hat voit la responsabilité logicielle comme un défi majeur de la politique de cybersécurité". *Inside Cybersecurity*. 26 juillet 2017. https://insidecybersecurity.com/daily- news/black-hat-founder-sees-software-liability-major-cybersecurity-policy-challenge.

National Highway Traffic Safety Administration (NHTSA). "Meilleures pratiques de cybersécurité pour les véhicules modernes". Octobre 2016. https://www.nhtsa.gov/staticfiles/nvs/pdf/812333 _CybersecurityForModernVehicles.pdf.

NIAC. "Securing Cyber Assets-Addressing Urgent Cyber Threats to Critical Infrastructure". Août 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft- report-08-15-17-508.pdf.

Virtualisation des fonctions réseau - Livre blanc sur les priorités NFV pour la 5G. 21 février 2017. https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf.

NICCS. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

NICCS. "Boîte à outils pour le développement de la main-d'œuvre en cybersécurité - Comment créer une main-d'œuvre solide en cybersécurité." Mars 2017. https://niccs.us-cert.gov/sites/default/files/documents /pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf.

Institut national des normes et de la technologie (NIST). *Cadre pour l'amélioration de la cybersécurité des infrastructures critiques*. 12 février 2014. http://www.nist.gov/cyberframework/ upload/cybersecurity-framework-021214.pdf.

NIST. Publication spéciale 800-193. *Lignes directrices sur la résilience des micrologiciels de plateforme.* Mai 2017. https://csrc.nist.gov/csrc/media/publications/sp/800-193/draft/documents/sp800-193-draft.pdf

Bulletin du NIST Information Technology Laboratory (ITL). *Réduire considérablement les vulnérabilités des logiciels.* Janvier 2017. http://ws680.nist.gov/publication/get_pdf.cfm?pub_ id=922589.

Bulletin du NIST ITL. *Adaptation des contrôles de sécurité pour les systèmes de contrôle industriels.* Novembre 2015. http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf.

Administration nationale des télécommunications et de l'information (NTIA). *Catalogue des normes de sécurité IoT existantes (version préliminaire 0.01),* processus multipartite de la NTIA sur l'évolutivité et les correctifs de sécurité IoT, groupe de travail sur les normes, outils et initiatives existants. Juillet 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA. Conseil de coordination du secteur des communications. *Livre blanc technique de l'industrie*. 17 juillet 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_ letter.pdf.

NTIA. *Multistakeholder Process : Vulnérabilités en matière de cybersécurité*. 15 décembre 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnérabilités.

NSTAC. *Rapport du NSTAC au président sur l'Internet des objets*. November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

O'Hern, Bill. AT&T, Inc. *Briefing au sous-comité ICR du NSTAC*. 20 juillet 2017. Olmstead,

Kenneth et Aaron Smith. " Les Américains et la cybersécurité ". *Pew Research Center Rapport.* à 19. 26 janvier 2017. http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

Pahl, Thomas B. FTC. *Commencer par la sécurité - et s'y tenir*. 28 juillet 2017. https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it.

SafeCode. https://safecode.org/about-safecode/.

Samani, Raj. McAfee, UK. *Briefing au sous-comité ICR du NSTAC*. 15 août 2017. Sann, Wallace.

ForeScout. *Briefing au sous-comité ICR du NSTAC*. 22 août 2017. Sandvine, *Global Internet*

Phenomena : Le trafic Internet crypté. 2016. https://www.sandvine.com/resources/global-internet-phenomena/spotlight/internet-traffic-cryptage.html.

Schneier, Bruce. *Nous devons sauver l'Internet de l'Internet des objets*. 6 octobre 2016. https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html.

Scriffignano, Anthony. Dun & Bradstreet, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 15 août 2017.

Projet Spamhaus. *Les pires pays du monde en matière de botnet.* 18 août 2017. https://www.spamhaus.org/statistics/botnet-cc/.

Symantec. *Mirai : Ce que vous devez savoir sur le botnet à l'origine des récentes attaques DDoS majeures.* 27 octobre 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks.

Tooley, Matt. National Cable and Television Association (NCTA), Communications Sector Coordinating Council, *Industry Technical White Paper on Botnets and Automated Threats*.

Institut de la Chambre américaine pour la réforme juridique. " Les délits civils du futur - Aborder les implications en matière de responsabilité et de réglementation des technologies émergentes. " Mars 2017. http://www.institutefor legalreform.com/uploads/sites/1/Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies_April_2017.pdf?pagename=uploads/sites/1/Torts_of_the_Future_Addressing_the_Liability_and_Regulatory_Implications_of_Emerging_Technologies._Technologies_.pdf.

Wallach, Steve. Micron Technology, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 7 septembre 2017.

Walsh, Kevin. Palo Alto Networks, Inc. *Briefing au sous-comité ICR du NSTAC*. Le 18 juillet 2017.

Warner, Mark. "Les sénateurs présentent une législation bipartisane visant à améliorer la cybersécurité des appareils de l'Internet des objets". *Communiqué de presse*. 1er août 2017. https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63- B9B4-523E18DADB36.

Bureau du secrétaire de presse de la Maison Blanche. *Executive Order 13800, Renforcement de la cybersécurité des réseaux fédéraux et des infrastructures critiques*. 11 mai 2017. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Xfinity. *Comcast Liste des ports bloqués.* https://www.xfinity.com/support/internet/list-of-blocked- ports/.

Zetter, Kim. "Lexique du hacker : Que sont les attaques DoS et DDoS ?" *Wired.* 16 janvier 2016. https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.