Un rapport au Président sur

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées et distribuées

---

Transmis par
Le secrétaire au commerce et
Le Secrétaire à la sécurité intérieure

22 mai 2018

Table des matières

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Résumé exécutif

Ce rapport répond au décret du 11 mai 2017 intitulé " Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques. " Ce décret appelait à la "résilience contre les botnets et autres menaces automatisées et distribuées", chargeant le secrétaire au commerce, conjointement avec le secrétaire à la sécurité intérieure, de "mener un processus ouvert et transparent pour identifier et promouvoir les actions des parties prenantes appropriées" dans le but de "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par *exemple,* les botnets)."

Les départements du commerce et de la sécurité intérieure ont collaboré à cet effort par le biais de trois approches - l'organisation de deux ateliers, la publication de deux demandes de commentaires et l'ouverture d'une enquête par le biais du comité consultatif présidentiel sur les télécommunications de sécurité nationale (NSTAC) - visant à recueillir un large éventail de contributions d'experts et de parties prenantes, y compris l'industrie privée, le monde universitaire et la société civile. Ces activités ont toutes contribué au processus de collecte d'informations pour les agences qui élaborent les recommandations de ce rapport.

Les ministères ont travaillé en consultation avec les ministères de la Défense, de la Justice et de l'État, le Federal Bureau of Investigation, les agences sectorielles, la Federal Communications Commission et la Federal Trade Commission, ainsi que d'autres organismes intéressés.

Les ministères ont déterminé que les opportunités et les défis à relever pour réduire considérablement les menaces liées aux attaques automatisées et distribuées peuvent être résumés en six thèmes principaux.

1. **Les attaques automatisées et distribuées sont un problème mondial.** La majorité des dispositifs compromis dans les récents réseaux de zombies notables étaient géographiquement situés en dehors des États-Unis. Pour accroître la résilience de l'Internet et de l'écosystème des communications face à ces menaces, dont beaucoup proviennent de l'extérieur des États-Unis, nous devons continuer à travailler en étroite collaboration avec des partenaires internationaux.
2. **Des outils efficaces existent, mais ne sont pas largement utilisés.** Bien que des améliorations soient encore possibles, les outils, les processus et les pratiques nécessaires pour améliorer de manière significative la résilience de l'écosystème de l'internet et des communications sont largement disponibles et sont couramment appliqués dans certains secteurs du marché. Cependant, ils ne font pas partie des pratiques courantes de développement et de déploiement de produits dans de nombreux autres secteurs pour diverses raisons, notamment (mais pas exclusivement) le manque de sensibilisation, l'évitement des coûts, l'insuffisance de l'expertise technique et l'absence d'incitations commerciales.
3. **Les produits doivent être sécurisés à toutes les étapes de leur cycle de vie.** Les appareils qui sont vulnérables au moment de leur déploiement, qui ne disposent pas des moyens de corriger les vulnérabilités après leur découverte ou qui restent en service après la fin de l'assistance technique du fournisseur, facilitent beaucoup trop l'assemblage de menaces automatisées et distribuées.
4. **La sensibilisation et l'éducation sont nécessaires.** Les utilisateurs privés et certaines entreprises n'ont souvent pas conscience du rôle que leurs appareils pourraient jouer dans une attaque de botnet et ne comprennent pas toujours les avantages des contrôles techniques disponibles. Les développeurs de produits, les fabricants et les opérateurs d'infrastructures manquent souvent des connaissances et des compétences nécessaires pour déployer des outils, des processus et des pratiques qui rendraient l'écosystème plus résilient.
5. **Les incitations du marché devraient être mieux alignées.** À l'heure actuelle, les incitations du marché ne semblent pas s'aligner sur l'objectif consistant à "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées". Les développeurs, fabricants et vendeurs de produits sont motivés par la volonté de minimiser les coûts et les délais de mise sur le marché, plutôt que d'intégrer la sécurité ou de proposer des mises à jour de sécurité efficaces. Les incitations du marché doivent être réalignées pour promouvoir un meilleur équilibre entre sécurité et commodité lors du développement de produits.

6. **Les attaques automatisées et distribuées constituent un défi à l'échelle de l'écosystème.** Aucune communauté de parties prenantes ne peut résoudre le problème de manière isolée.

Les ministères ont identifié cinq objectifs complémentaires et se renforçant mutuellement qui, s'ils étaient atteints, réduiraient considérablement la menace d'attaques automatisées et distribuées et amélioreraient la résilience et la redondance de l'écosystème. Une liste d'actions suggérées pour les principales parties prenantes renforce chaque objectif. Les objectifs sont les suivants :

- Objectif 1 : définir une voie claire vers un marché technologique adaptable, durable et sûr.
- Objectif 2 : promouvoir l'innovation dans l'infrastructure pour une adaptation dynamique à l'évolution des menaces.
- Objectif 3 : promouvoir l'innovation à la périphérie du réseau pour prévenir, détecter et atténuer les attaques automatisées et distribuées.
- Objectif 4 : Promouvoir et soutenir les coalitions entre les communautés de la sécurité, des infrastructures et des technologies opérationnelles au niveau national et international.
- Objectif 5 : accroître la sensibilisation et l'éducation dans l'ensemble de l'écosystème.

Les actions et options recommandées comprennent des activités en cours qui devraient être poursuivies ou étendues, ainsi que de nouvelles initiatives. Aucun investissement ou activité ne peut à lui seul atténuer toutes les menaces, mais les discussions organisées et les commentaires des parties prenantes nous permettront d'évaluer plus avant et de hiérarchiser ces activités en fonction du retour sur investissement attendu et de leur capacité à avoir un impact mesurable sur la résilience des écosystèmes.
Ce rapport demande une mise à jour de la situation qui évaluera le niveau des progrès réalisés par les parties prenantes dans la lutte contre les menaces automatisées et distribuées.

Cet effort ne se terminera pas avec la publication de ce rapport. Il y a encore beaucoup de travail à faire. Cependant, nous ne nous attendons pas à ce que toutes les actions se déroulent simultanément, en raison de considérations telles que les contraintes de ressources dans les communautés de parties prenantes concernées. En outre, certaines actions sont déjà en cours, tandis que d'autres dépendent de facteurs extérieurs. Nous proposons un modèle pour soutenir la coordination et la collaboration pour la mise en œuvre des actions décrites dans la section III, avec un accent particulier sur les exigences fédérales. Bien que certaines actions directement liées au gouvernement fédéral soient clairement appropriées pour que le gouvernement les dirige, ce modèle fournit un moyen pour les parties prenantes de collaborer avec le gouvernement alors qu'ils avancent sur les actions qui sont mieux accomplies grâce au leadership du secteur privé.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

I. Contexte

Le 11 mai 2017, le président a émis le décret (EO) 13800, "Renforcer la cybersécurité des réseaux fédéraux et des infrastructures critiques", appelant à la "résilience contre les botnets et autres menaces automatisées et distribuées".[1] Le président a demandé au secrétaire au commerce et au secrétaire à la sécurité intérieure de "mener un processus ouvert et transparent pour identifier et promouvoir l'action des parties prenantes appropriées" dans le but de "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par *exemple,* les botnets)".

Ces types d'attaques sont un sujet de préoccupation depuis les premiers jours d'Internet[2] et sont devenus un phénomène régulier au début des années 20003. [3] Les attaques automatisées et distribuées constituent une menace qui dépasse le cadre d'une seule entreprise ou d'un seul secteur. Ces menaces sont utilisées pour diverses activités malveillantes, notamment les attaques par déni de service distribué (DDoS) qui submergent les ressources en réseau, envoient des quantités massives de spam, diffusent des enregistreurs de frappe et d'autres logiciels malveillants ; les attaques par ransomware distribuées par des botnets qui prennent en otage les systèmes et les données ; et les campagnes de propagande informatique4 qui manipulent et intimident les communautés par le biais des médias sociaux. Les techniques traditionnelles d'atténuation des attaques DDoS, telles que la mise en place par les fournisseurs de réseaux d'une capacité excédentaire pour absorber les effets des botnets, sont conçues pour se protéger contre les botnets d'une taille anticipée. Avec les nouveaux botnets qui tirent parti du nombre considérable d'appareils de l'"Internet des objets" (IoT)[5], les attaques DDoS ont atteint une taille de plus d'un térabit par seconde, dépassant de loin la taille prévue et la capacité excédentaire. Par conséquent, le temps de récupération de ces types d'attaques peut être trop lent, en particulier lorsque des services essentiels à la mission sont concernés. En outre, ces techniques d'atténuation n'ont pas été conçues pour remédier à d'autres catégories d'activités malveillantes facilitées par les réseaux de zombies, comme les rançongiciels ou la propagande informatique.

À mesure que de nouveaux scénarios émergent, il est urgent de coordonner et de collaborer avec un ensemble diversifié de parties prenantes. Le gouvernement fédéral a travaillé avec les parties prenantes dans le passé pour faire face aux nouvelles menaces à mesure qu'elles apparaissent. Parmi les efforts antérieurs, citons le Industry Botnet Group, qui a débouché sur les Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace (2012) ; [6] les efforts de partage d'informations et de coordination du secteur des services financiers à la suite des attaques DDoS contre des banques en 2012 et

[1] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (11 mai 2017), *disponible à l'adresse suivante* . https://www.federalregister.gov/d/2017-10004.
[2] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
[3] *Voir, par exemple,* Stuart Staniford, Vern Paxson & Nicholas Weaver, How *to 0wn the Internet in Your Spare Time,* Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, Aug. 5-9, 2002, *disponible sur* https://www.usenix.org/legacy/event/sec02/full_papers/staniford/staniford.pdf.
[4] La propagande informatique est "l'assemblage de plateformes de médias sociaux, d'agents autonomes et de big data chargés de manipuler l'opinion publique." Samuel C. Woolley & Philip N. Howard, *Political Communication, Computational Propaganda, and Autonomous Agents-Introduction, 10* Int'l Journal of Commc'n 4882, 4886 (2016), *disponible sur* http://ijoc.org/index.php/ijoc/article/viewFile/6298/1809.
[5] Les exemples d'appareils IoT comprennent (sans s'y limiter) les ampoules connectées, les serrures de porte, les parcmètres, les moniteurs de santé personnels, l'automatisation et les capteurs industriels, et les automobiles.
[6] Industry Botnet Group, *Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace*, https://archive.is/20131015084520/www.industrybotnetgroup.org/principles/ (dernière visite le 4 avril 2018).

[20137] ; le code de conduite anti-bot du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications (CSRIC)[8] (2013)[9], les rapports sur les pratiques de protection des réseaux des fournisseurs de services Internet (ISP) (2010)[10] et sur la remédiation des attaques DDoS basées sur les serveurs (2014)[11] ; et les travaux actifs et continus du ministère de la Justice et de ses nombreux partenaires sur le traitement et l'élimination de l'infrastructure soutenant ces menaces12. [12] Bien que ces initiatives aient permis de réaliser des progrès, leur impact a été progressif et des défis importants restent à relever. En s'attaquant de manière proactive à ces défis, l'administration et les principales parties prenantes ont la possibilité d'améliorer la résilience du futur écosystème de l'Internet et des communications.

Les attaques DDoS lancées à partir du botnet Mirai à l'automne 2016, par exemple, ont atteint un niveau de trafic soutenu qui a submergé de nombreux outils et services d'atténuation DDoS courants, et ont même perturbé un service de système de nom de domaine (DNS) qui était un composant couramment utilisé dans de nombreuses stratégies d'atténuation DDoS. [13] Cette attaque a également mis en évidence l'insécurité croissante des dispositifs IoT grand public et les menaces qu'ils représentent. En tant que nouvelle technologie, les dispositifs IdO sont souvent construits et déployés sans que d'importantes fonctions et pratiques de sécurité soient en place14. [14] Alors que la variante originale de Mirai était relativement simple, exploitant les mots de passe faibles des appareils, des réseaux de zombies plus sophistiqués ont suivi ; par exemple, le réseau de zombies Reaper utilise des vulnérabilités de code connues pour exploiter une longue liste d'appareils,[15] et l'une des plus grandes attaques DDoS observées à ce jour a récemment exploité une vulnérabilité récemment découverte dans l'appareil relativement obscur

[7] *Evaluating the Security of the U.S. Financial Sector : Hearing Before the Task Force to Investigate Terrorism Financing*, House Committee on Financial Services, 114th Cong. 40-59 (2015) (déclaration de John W. Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center (FS-ISAC)), *disponible sur* https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96997/pdf/CHRG-114hhrg96997.pdf.

[8] Le CSRIC est un comité consultatif de la Federal Communications Commission, dont la mission est de faire des recommandations à la Commission pour promouvoir la sécurité, la fiabilité et la résilience des systèmes de communication de la nation. Pour plus d'informations, y compris les efforts passés en matière de sécurité, voir CSRIC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability- council-0 (dernière visite le 4 avril 2018).

[9] Groupe de travail 7 du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications III, *Final Report on U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)*, (Mar. 2013), *disponible sur* https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[10] Groupe de travail 8 du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications, *Rapport final sur les pratiques de protection des réseaux des fournisseurs de services Internet (FSI)*, (déc. 2010), *disponible à l'adresse* http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101 213.pdf.

[11] Groupe de travail 5 du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications IV, *Rapport final sur la remédiation des attaques DDoS basées sur le serveur*, (sept. 2014), *disponible à l'adresse* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

[12] *Voir, par exemple, le* ministère de la Justice des États-Unis, *Avalanche Network Dismantled in International Cyber Operation*, (5 déc. 2016), https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

[13] Équipe de préparation aux situations d'urgence informatique des États-Unis, *Alerte (TA16-288A) : Heightened DDoS Threat Posed by Mirai and Other Botnets*, https://www.us-cert.gov/ncas/alerts/TA16-288A (dernière révision le 17 octobre 2017).

[14] The National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things*, (19 nov. 2014), *disponible à l'adresse* 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.

[15] Brian Krebs, *Fear the Reaper, or Reaper Madness ?* Krebs on Security (27 oct. 2017, 4:39 PM), https://krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/.

le logiciel MemCacheD. [16] Ces exemples montrent clairement les risques posés par des réseaux de zombies de cette taille et de cette envergure, ainsi que l'innovation attendue et l'augmentation de l'échelle et de la complexité des attaques futures.

Approche

Les ministères du Commerce et de la Sécurité intérieure ont travaillé conjointement sur cet effort en adoptant trois approches visant à recueillir un large éventail de contributions de la part d'experts et de parties prenantes, notamment du secteur privé, du monde universitaire et de la société civile. Les ministères ont travaillé en consultation avec les ministères de la Défense, de la Justice et de l'État, le Federal Bureau of Investigation, les agences sectorielles, la Federal Communications Commission et la Federal Trade Commission, ainsi que d'autres organismes intéressés.

En juin 2017, l'Administration nationale des télécommunications et de l'information (NTIA) du Département a publié une demande de commentaires (RFC) sur la "promotion de l'action des parties prenantes contre les botnets et autres menaces automatisées".[17] La RFC demandait des commentaires sur "les approches actuelles, émergentes et potentielles pour faire face aux botnets et autres attaques distribuées et automatisées". La NTIA a reçu 47 commentaires, les répondants allant de grandes associations commerciales (représentant des milliers d'entreprises) à des experts techniques individuels. Les commentateurs représentaient également une gamme variée d'industries et de secteurs, y compris des fournisseurs de services Internet, des entreprises de sécurité, des fournisseurs d'infrastructure, des fabricants de logiciels, la société civile et le monde universitaire d'organisations américaines et non américaines.

En juillet 2017, le National Institute of Standards and Technology (NIST) du Département a organisé un atelier sur le thème "Renforcer la résilience de l'écosystème de l'Internet et des communications".[18] Cet atelier a encouragé les parties prenantes à explorer les solutions actuelles et émergentes pour faire face aux menaces automatisées et distribuées de manière ouverte et transparente. Il a attiré 150 participants de diverses communautés de parties prenantes, qui ont identifié un large éventail d'actions coordonnées par toutes les parties prenantes pour faire face à ces menaces.

Conformément à l'Executive Order 13800, un projet de rapport a été publié en janvier 2018, suivi d'un deuxième RFC et d'un atelier, au cours duquel les parties prenantes ont discuté des commentaires publics de fond et des prochaines étapes. Ces activités ont contribué au processus de collecte d'informations pour les agences élaborant les recommandations de ce rapport final. Les commentaires et les discussions de l'atelier éclaireront également de nombreuses actions qui auront lieu après la publication de ce rapport.

La participation du Department of Homeland Security (DHS) à cet effort s'est concentrée sur le sous-comité du President's National Security Telecommunications Advisory Committee (NSTAC) sur la résilience de l'Internet et des communications, qui a finalisé et approuvé le *rapport du NSTAC à l'intention de l*

[16] Lili Hay Newman, *GitHub a survécu à la plus grande attaque DDoS jamais enregistrée*, Wired (1er mars 2018, 11 h 01), https://www.wired.com/story/github-ddos-memcached/.

[17] Des informations supplémentaires, notamment les commentaires publics, sont disponibles à l'adresse suivante : National Telecommunications and Information Administration, *Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats*, (8 juin 2017), https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting- stakeholder-action-against-botnets-and-other-automated-threats.

[18] National Institute of Standards and Technology, *Enhancing Resilience of the Internet and Communications Ecosystem*, https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications- ecosystem (dernière mise à jour le 10 juillet 2017). Pour un résumé des travaux, voir Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem : A NIST Workshop Proceedings*, (sept. 2017), NIST Interagency/Internal Report No. 8192, *disponible sur* http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

President on Internet and Communications Resilience le 16 novembre 2017.[19] Lors de l'élaboration de son rapport, le NSTAC a étudié les botnets, ainsi que les formes d'attaques qui peuvent être facilitées par les botnets, telles que les attaques DDoS et les vecteurs qui pourraient être utilisés pour créer des botnets (c'*est-à-dire,* les appareils des utilisateurs finaux et l'IoT). Grâce à son étude, le NSTAC a conclu que les attaques automatisées et distribuées facilitées par les botnets menacent la sécurité et la résilience de l'Internet et de l'écosystème des communications, et à leur tour, les infrastructures critiques de la nation. En outre, le NSTAC a déterminé que les dispositifs IoT compromis seront de plus en plus utilisés par des acteurs malveillants pour lancer des attaques automatisées mondiales.

Thèmes principaux

Les opportunités et les défis auxquels nous sommes confrontés dans le cadre de nos efforts pour réduire considérablement les menaces liées aux attaques automatisées et distribuées peuvent être résumés en six thèmes principaux.

1. **Les attaques automatisées et distribuées sont un problème mondial.** La majorité des dispositifs compromis dans les récents réseaux de zombies notables étaient géographiquement situés en dehors des États-Unis. Pour accroître la résilience de l'Internet et de l'écosystème des communications face à ces menaces, dont beaucoup proviennent de l'extérieur des États-Unis, nous devons continuer à travailler en étroite collaboration avec des partenaires internationaux.
2. **Des outils efficaces existent, mais ne sont pas largement utilisés.** Bien que des améliorations soient encore possibles, les outils, les processus et les pratiques nécessaires pour améliorer de manière significative la résilience de l'écosystème de l'internet et des communications sont largement disponibles et sont couramment appliqués dans certains secteurs du marché. Cependant, ils ne font pas partie des pratiques courantes de développement et de déploiement de produits dans de nombreux autres secteurs pour diverses raisons, notamment (mais pas exclusivement) le manque de sensibilisation, l'évitement des coûts, l'insuffisance de l'expertise technique et l'absence d'incitations commerciales.
3. **Les produits doivent être sécurisés à toutes les étapes de leur cycle de vie.** Les appareils qui sont vulnérables au moment de leur déploiement, qui ne disposent pas des moyens de corriger les vulnérabilités après leur découverte ou qui restent en service après la fin de l'assistance technique du fournisseur, facilitent beaucoup trop l'assemblage de menaces automatisées et distribuées.
4. **La sensibilisation et l'éducation sont nécessaires.** Les utilisateurs privés et certaines entreprises n'ont souvent pas conscience du rôle que leurs appareils pourraient jouer dans une attaque de botnet et ne comprennent pas toujours les avantages des contrôles techniques disponibles. Les développeurs de produits, les fabricants et les opérateurs d'infrastructures manquent souvent des connaissances et des compétences nécessaires pour déployer des outils, des processus et des pratiques qui rendraient l'écosystème plus résilient. Des mécanismes conviviaux permettant d'identifier des choix plus sûrs, analogues à des programmes tels que le programme Energy Star20 ou le classement de sécurité 5 étoiles de la National Highway Traffic Safety Administration (NHTSA)21 sont nécessaires pour sensibiliser les consommateurs et éclairer leurs décisions d'achat.
5. **Les incitations du marché devraient être mieux alignées.** À l'heure actuelle, les incitations du marché ne semblent pas s'aligner sur l'objectif consistant à "réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées". Les développeurs, fabricants et vendeurs de produits sont motivés par la volonté de minimiser les coûts et les délais de mise sur le marché, plutôt que d'intégrer la sécurité ou d'offrir une sécurité efficace.

[19] Le Comité consultatif sur les télécommunications pour la sécurité nationale, *Rapport du NSTAC au président sur la résilience de l'Internet et des communications*, (16 novembre 2017), *disponible sur* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR.%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

[20] Energy Star, *About Energy Star*, https://www.energystar.gov/about (dernière visite le 4 avril 2018). [21] National Highway Traffic Safety Administration, *Search NHTSA's 5-Star Safety Ratings*, https://www.safercar.gov/Vehicle-Shoppers (dernière visite le 4 avril 2018).

mises à jour. Les incitations du marché doivent être réalignées pour promouvoir un meilleur équilibre entre sécurité et commodité lors du développement des produits.

6. **Les attaques automatisées et distribuées constituent un défi à l'échelle de l'écosystème.** Aucune communauté de parties prenantes ne peut résoudre le problème de manière isolée.

Une note sur les menaces

Le présent document ne fait pas de distinction entre les États-nations, les cybercriminels et les autres acteurs de la menace. Si certaines attaques peuvent être difficiles à attribuer au départ, l'écosystème doit néanmoins s'unir pour atténuer une attaque. Ce processus ouvert et transparent s'est concentré sur les domaines qui susciteraient la plus large participation des parties prenantes de l'ensemble de l'écosystème de l'Internet et des communications concernant les améliorations de la sécurité, ainsi que la coopération avant, pendant et après les attaques, en comprenant que l'identité d'un acteur de la menace donné peut être initialement inconnue. L'évaluation de la menace mondiale 2018 de la communauté du renseignement des États-Unis publiée par le bureau du directeur du renseignement national donne un aperçu du paysage de la cybermenace. [22] Bien que cela dépasse le cadre du présent rapport, il sera important de faire la distinction entre les acteurs de la menace de type État-nation, cybercriminel et autres pour déterminer la meilleure façon d'appliquer un large éventail d'autorités gouvernementales américaines spécifiques à la menace. Certains participants à l'atelier ont également reconnu leurs limites dans le traitement de catégories spécifiques d'acteurs de la menace. Il conviendrait d'accorder une attention particulière à ces questions à l'avenir, en impliquant les parties prenantes de l'écosystème au

II. État actuel de l'écosystème et vision pour l'avenir

Cette section décrit l'état actuel des domaines techniques et politiques de l'écosystème de l'internet et des communications mondiales, et envisage un avenir meilleur. Les domaines techniques de l'écosystème comprennent :

- L'***infrastructure*** qui relie les autres domaines techniques en un seul système ;
- ***Réseaux d'entreprise*** composés de dispositifs connectés localement et dotés d'adresses Internet IP version 4 (IPv4) et IPv6 attribuées par le registre Internet régional (RIR)[23], ainsi que de réseaux sous-locaux (LAN) connectés localement et utilisant un espace d'adressage IP privé ou des protocoles alternatifs (par *exemple,* Bluetooth Low Energy) ;
- les ***dispositifs de périphérie*** tels que les ordinateurs personnels, les dispositifs mobiles, les serveurs de périphérie et les dispositifs IoT et autres dispositifs connectés ; et
- ***Réseaux domestiques et de petites entreprises*** composés de dispositifs utilisant un espace d'adressage IP privé adressable à l'extérieur par le biais de la traduction d'adresses réseau (NAT).

Le domaine de la politique est lié aux domaines techniques, et comprend :

- Les **partenariats public-privé**, y compris les accords de partage d'informations ;

[22] *Voir* Daniel R. Coats, directeur du renseignement national, *Worldwide Threat Assessment of the US Intelligence Community*, déclaration pour le compte rendu à la commission spéciale du Sénat sur le renseignement, (13 février 2018), *disponible sur* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[23] "Les registres Internet régionaux (RIR) sont des sociétés à but non lucratif qui administrent et enregistrent l'espace d'adressage du protocole Internet (IP) et les numéros de systèmes autonomes (AS) dans une région définie." American Registry for Internet Numbers, *Regional Internet Registries*, https://www.arin.net/knowledge/rirs.html (dernière visite le 4 avril 2018).

- Les **processus d'attestation ou de certification volontaires**, dans lesquels les fournisseurs et les clients acceptent de partager des objectifs et des attentes en matière de sécurité ;
- **Normes et lignes directrices** élaborées dans des forums multipartites ;
- Des **politiques d'approvisionnement**, notamment au sein du gouvernement fédéral, pour créer des incitations au marché ;
- **Les actions réglementaires et législatives** au niveau fédéral et/ou étatique ; et
- Un **engagement international** pour s'appuyer sur des objectifs communs et des meilleures pratiques.

L'amélioration de la résilience face aux attaques automatisées et distribuées nécessitera une collaboration sur des ensembles de solutions techniques, politiques et autres entre les nations, les secteurs et les couches techniques. Des politiques efficaces fourniront des attentes claires pour l'utilisation de normes et de directives qui resteront flexibles et adaptables à mesure que le risque de sécurité évolue. Il n'existe pas de solution ou de cadre unique permettant de faire face à tous les risques, mais une meilleure collaboration entre les domaines améliorera la capacité des membres de l'écosystème à atténuer la menace des botnets.

Domaines techniques

Infrastructure : État actuel

Face aux attaques automatisées et distribuées, l'infrastructure actuelle qui sous-tend l'écosystème numérique a fait preuve d'une résilience remarquable, mais la taille et la portée croissantes des attaques semblent tester les limites de cette résilience. Ces deux perspectives sont apparues après les attaques du botnet Mirai de 2016, qui ont temporairement interrompu les services d'un fournisseur d'infrastructure Internet, perturbant ainsi de nombreux services en ligne et sites Web importants en Amérique du Nord et en Europe. Cependant, les perturbations étaient temporaires et les acteurs clés ont réagi rapidement. Cette réaction souligne à la fois l'interdépendance de l'infrastructure et la capacité des individus et des organisations à apprendre et à s'adapter rapidement.

Dans le présent rapport, le terme "infrastructure" englobe la technologie et les organisations qui permettent la connectivité, l'interopérabilité et la stabilité, allant au-delà des câbles physiques, des émetteurs et récepteurs sans fil et des liaisons par satellite pour inclure le matériel, les logiciels, les outils, les normes et les pratiques dont dépend l'écosystème - par exemple, les routeurs, les commutateurs, les fournisseurs de services Internet, les fournisseurs de DNS, les réseaux de diffusion de contenu, les fournisseurs d'hébergement et de services en nuage. [24] En raison de la complexité de l'infrastructure moderne, avec des outils et des acteurs clés disséminés dans l'écosystème, aucun outil unique ne peut sécuriser l'infrastructure. Traditionnellement, lorsque de nouvelles menaces apparaissent, des sous-ensembles particuliers d'acteurs de l'infrastructure collaborent pour comprendre le risque et les moyens de l'atténuer.

Le filtrage du trafic à l'entrée et à la sortie d'un réseau - technique connue sous le nom de filtrage à l'entrée et à la sortie - est l'un de ces outils. L'usurpation d'adresse IP est une technique couramment employée dans les attaques DDoS, où l'attaquant fabrique l'adresse IP source pour empêcher la victime de filtrer le mauvais trafic en fonction de son origine.
Les fournisseurs de réseaux peuvent limiter l'usurpation d'identité en restreignant le trafic entrant à celui qui provient réellement de son réseau déclaré, en filtrant le trafic qui prétend provenir de l'extérieur de son espace réseau prévu. [25] Le filtrage à l'entrée est reconnu comme une meilleure pratique de longue date par l'Internet Engineering

[24] Alors que la Presidential Policy Directive (PPD) 21 reconnaît les systèmes et les actifs des secteurs des communications et des technologies de l'information comme des infrastructures critiques, le présent document utilise le terme "infrastructure Internet" pour englober les organisations et les pratiques dont dépend l'écosystème Internet.
[25] Le DHS développe et soutient des outils logiciels à code source ouvert pour évaluer et rendre compte du déploiement des meilleures pratiques anti-spoofing de la validation de l'adresse source (SAV). Pour plus d'informations, voir Center for Applied Internet Data Analysis, *Spoofer*, https://www.caida.org/projects/spoofer/.

Task Force (IETF) et d'autres organisations axées sur l'infrastructure. [26] Il peut être complété par le filtrage de sortie, dans lequel une organisation ou un opérateur de réseau déploie des filtres à la périphérie de son réseau pour empêcher le trafic qui ne semble pas provenir de l'intérieur du réseau de sortir sur l'Internet mondial.

Les principaux opérateurs nationaux mettent en œuvre les normes de filtrage à l'entrée dans au moins une partie de leurs réseaux. Cependant, ces normes ne sont pas universellement soutenues dans le monde entier, ni par les petits fournisseurs d'infrastructure nationaux. De nombreux experts techniques et commerciaux se sont opposés aux propositions visant à appliquer le filtrage à l'entrée plus haut dans l'Internet, au niveau des dorsales internationales, parce qu'il serait plus susceptible de bloquer le trafic légitime. [27] Le filtrage à la sortie est préconisé comme une pratique de sécurité courante pour les entreprises,[28] mais il est encore peu répandu dans les petites et moyennes entreprises. Bien qu'il ne soit pas universellement mis en œuvre, le filtrage entrée/sortie du réseau, lorsqu'il est mis en œuvre, est efficace pour atténuer la catégorie d'attaques DDoS qui exploitent l'usurpation d'adresse IP source.

Les fournisseurs d'infrastructures et d'autres entreprises proposent des services anti-DDoS commerciaux, qui peuvent jouer un rôle clé dans la limitation de l'impact des attaques contre des cibles particulières. Cependant, toutes les entreprises clientes n'achètent pas la gamme complète de services anti-DDoS, en raison du coût et de la complexité de l'intégration de ces services dans les autres composants du réseau de l'entreprise. Parallèlement, les attaquants apprennent rapidement à exploiter les failles des services existants. Face à des attaques qui reposent sur le simple volume du trafic, les solutions d'atténuation des attaques DDoS hors site fournissent davantage de capacité réseau ou utilisent la forme du réseau lui-même pour limiter le volume du trafic qui atteint la cible. D'autres attaques visent le serveur web ou l'application elle-même. Les dispositifs et outils sur site d'une entreprise détectent et filtrent ces attaques sur le réseau cible.

Les meilleures pratiques actuelles impliquent l'emploi d'une approche hybride qui utilise à la fois le filtrage local et des outils de défense contre les DDoS qui augmentent la capacité hors site. Cependant, la mise en œuvre des meilleures pratiques peut être coûteuse, difficile à gérer et nécessiter un personnel qualifié. Ces meilleures pratiques sont aussi généralement construites autour de crises passées, ce qui rend difficile, par exemple, de plaider en faveur d'une grande quantité de capacité excédentaire jusqu'à ce que l'on subisse une attaque. Un programme de détection active des menaces qui détecte les vulnérabilités et les tendances des attaques peut compléter ces efforts, en aidant l'organisation victime à réagir en fonction des besoins. Les réseaux de diffusion de contenu (CDN) sont un autre outil qui peut tirer parti de grandes infrastructures privées dédiées pour protéger les clients. À mesure que des attaques différentes apparaissent ou que les adversaires choisissent de nouvelles cibles, les organisations investissent souvent dans des défenses spécifiques aux menaces.

Réagir en temps voulu nécessite une préparation et des connaissances. Compte tenu du grand nombre de contrôles de sécurité nécessaires dans l'Internet moderne, le personnel des petits fournisseurs d'infrastructure ou des entreprises clés n'est pas toujours conscient des avantages du filtrage et des autres outils. De nombreux fournisseurs d'infrastructure émettent des avertissements sur les compromissions et les attaques en cours, mais si les entreprises ignorent ces avertissements, le fournisseur d'infrastructure est moins susceptible de donner suite avec diligence à d'autres avertissements. Les victimes ont souvent du mal à

[26] *Voir, par exemple,* P. Ferguson & D. Senie, *Network Ingress Filtering : Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, (mai 2000), Internet Engineering Task Force - Network Working Group, *disponible sur* https://tools.ietf.org/html/bcp38 ("BCP 38") ; et F. Baker & P. Savola, Ingress *Filtering for Multihomed Networks, (*mars 2004), Internet Engineering Task Force - Network Working Group, *disponible sur* https://tools.ietf.org/html/bcp84 ("BCP 84").

[27] Les paquets peuvent être acheminés entre les points d'extrémité de l'Internet par des chemins sensiblement différents à différents moments dans le temps pour des raisons légitimes.

[28] *Voir, par exemple*, Chris Brenton, *Egress Filtering FAQ*, SANS Institute, https://www.sans.org/reading-room/whitepapers/firewalls/egress-filtering-faq-1059 (dernière révision le 19 avril 2006).

lorsqu'ils sont confrontés à leur première attaque importante sans plan d'intervention en place, car ils dépendent du réseau même attaqué pour le comprendre et contacter les fournisseurs de services pour obtenir de l'aide.

Vision pour l'avenir des infrastructures

Les fournisseurs d'infrastructure de tous types doivent développer une large compréhension des avantages des approches de défense partagées, et les communautés devraient travailler ensemble pour favoriser l'adoption des meilleures pratiques. Ce travail inclut l'adoption omniprésente du filtrage à l'interface avec les réseaux des clients, y compris les infrastructures multi-tenant telles que les fournisseurs de cloud. Idéalement, les fournisseurs d'infrastructures devraient comprendre les niveaux actuels d'attaques, maintenir une capacité suffisante pour absorber les niveaux de trafic malveillant attendus de manière réaliste, et communiquer ces capacités à leurs clients. Les services des fournisseurs d'infrastructure pour l'atténuation des attaques DDoS devraient s'intégrer aux solutions réseau existantes des clients, quel que soit le niveau de service choisi par le client.

À mesure que de nouveaux produits et outils sont disponibles, les acteurs de l'écosystème doivent comprendre comment leur comportement peut favoriser - ou entraver - leur efficacité. Un réseau de plus en plus intelligent peut segmenter automatiquement différents types de trafic, afin d'isoler ou d'atténuer les applications ou les appareils qui sont des sources et des cibles d'attaques. Les entreprises sont de plus en plus capables de faire face aux attaques au niveau des applications grâce à des outils appropriés, et les fournisseurs de ces outils devraient travailler avec les clients et les fournisseurs d'applications concernés pour rendre les décisions de sécurité plus faciles et plus efficaces.

Une mise en œuvre accrue d'un certain nombre de technologies existantes contribuera à atténuer ces attaques. Une partie de l'infrastructure existante repose sur des protocoles plus anciens, tels que le réseau IPv4 et les anciens protocoles de routage. Une adoption plus large des normes et des meilleures pratiques actuelles apportera des avantages en matière de sécurité. Par exemple, le réseau IPv6 peut mieux permettre la reconnaissance spécifique des appareils sur le réseau afin de détecter les comportements aberrants au niveau des appareils. [29] Les petites et moyennes entreprises devraient intégrer les meilleures pratiques de l'industrie et, à mesure que de nouvelles normes et pratiques d'infrastructure sont nécessaires et éprouvées, les fournisseurs d'infrastructure devraient les adopter efficacement.

Au cœur de l'infrastructure, les acteurs clés partagent déjà des informations sur la nature évolutive des menaces. Si bon nombre de ces organisations emploient des experts qui coordonnent leurs activités avec celles de leurs pairs dans le monde entier, à l'avenir, le partage de l'information devra s'étendre aux acteurs plus petits, moins bien financés ou spécialisés, grâce à de nouveaux outils et pratiques automatisés. Des mesures incitatives pourraient encourager les investissements dans une détection plus efficace du trafic malveillant, ainsi que des engagements publics plus nombreux pour éviter de transporter du trafic malveillant. Ces engagements s'appuieraient sur les relations existantes au sein de la communauté pour aider à construire un réseau mondial plus stable.

Réseaux d'entreprise : État actuel

Les réseaux qui soutiennent les entreprises (*par exemple, les* moyennes et grandes entreprises, les agences gouvernementales et les institutions académiques) constituent un autre domaine technique clé de l'écosystème Internet et des communications. Ces réseaux sont souvent complexes, avec des routeurs BGP (Border Gateway Protocol) appartenant à l'entreprise et exploités par elle, des résolveurs DNS et des applications qui reposent sur un mélange de services locaux et en nuage. Les appareils de périphérie comprennent souvent des serveurs puissants, des appareils informatiques personnels, des téléphones mobiles et des appareils IoT gérés et non gérés par l'entreprise. Les appareils des réseaux d'entreprise peuvent utiliser un mélange de services statiques ou en nuage.

[29] La solution de rechange actuelle pour IPv4, la traduction d'adresses de réseau (NAT), offre des avantages en matière de pare-feu, en particulier au niveau du réseau domestique. Il convient toutefois de noter qu'une fois l'IPv6 mis en œuvre, les attaquants pourraient identifier les adresses spécifiques de dispositifs ciblés qui auraient été auparavant plus difficiles à reconnaître derrière la NAT. Les experts ont également exprimé certaines inquiétudes quant à la sécurité de certaines mises en œuvre d'IPv6.

des adresses attribuées dynamiquement à partir d'une ou plusieurs plages d'adresses IP publiques (par *exemple, des* adresses acquises auprès d'un RIR) ainsi que des adresses attribuées à partir de plages d'adresses IP privées administrées localement. La présence importante de réseaux d'entreprise connectés à l'Internet signifie qu'ils ne sont pas seulement des victimes potentielles mais aussi des sources de risque.

De nombreuses attaques DDoS bien connues, telles que celles qui ont visé des banques américaines en 2012 et 2013, ont ciblé des services en contact avec la clientèle associés à de grandes entreprises. [30] Tout comme les attaques Mirai de 2016 ont permis à certaines entreprises de faire preuve de résilience face à la vulnérabilité, les attaques de 2012-2013 ont incité le secteur financier et ses partenaires à découvrir des faiblesses et à montrer des voies vers une plus grande résilience. Ces attaques ont été perturbatrices, mais le secteur en a atténué les effets grâce à un investissement accru dans la technologie et les ressources, ainsi qu'à une collaboration active au sein de la communauté, y compris avec ses fournisseurs de services réseau et ses partenaires techniques, ainsi qu'avec le gouvernement. Les organisations ont partagé les leçons apprises à mesure que les attaques se poursuivaient, et des institutions telles que le Centre d'analyse et de partage de l'information (ISAC) des services financiers et la Table ronde des services financiers ont facilité le partage de l'information et la coordination avec les principaux fournisseurs de services Internet. L'ampleur des attaques a inspiré un leadership aux plus hauts niveaux de la direction et a favorisé une relation plus durable avec les experts gouvernementaux, ainsi qu'un engagement à investir dans les outils et les services.

Les ressources associées aux réseaux d'entreprise sont également un facteur important dans l'exécution de menaces automatisées et distribuées. Les appareils au niveau de l'entreprise, allant des appareils IoT aux serveurs des centres de données, peuvent être compromis et incorporés dans des botnets. Les ressources d'entreprise mal administrées, telles que les résolveurs DNS ouverts, sont souvent exploitées pour amplifier les attaques. Pour certaines entreprises, il peut être difficile de maintenir tous les systèmes et appareils patchés et mis à jour sur l'ensemble de leurs réseaux mondiaux. Les routeurs exploités par les entreprises qui n'appliquent pas le filtrage à l'entrée et à la sortie ont facilité les attaques par usurpation d'adresse, permettant aux participants du botnet de cacher leur véritable emplacement. Dans le cas des fournisseurs de services en nuage, des ressources d'entreprise ont été louées (généralement avec des cartes de crédit volées) pour constituer rapidement des réseaux de zombies importants. Dans de nombreux pays, les problèmes liés aux systèmes existants sont aggravés par l'utilisation généralisée de logiciels piratés, qui ne sont généralement pas corrigés et sont donc vulnérables aux exploits connus. Les entreprises qui utilisent beaucoup de logiciels piratés sont extrêmement difficiles à protéger, car elles fournissent aux acteurs malveillants un réservoir de systèmes qu'ils peuvent facilement assembler en menaces distribuées.

Les entreprises qui ont été confrontées à des attaques DDoS, ou qui appartiennent à des secteurs largement touchés par ces attaques, intègrent souvent les attaques potentielles dans leur modèle de risque et utilisent une combinaison de mesures d'atténuation des attaques DDoS proposées par les fournisseurs d'infrastructure et de mesures d'atténuation sur site gérées par l'entreprise. Les entreprises qui comprennent les risques et mettent en œuvre ces mécanismes sont l'exception. De nombreuses entreprises à risque n'ont pas conscience de l'impact potentiel des attaques DDoS sur leurs opérations. Ces entreprises peuvent ne pas comprendre pleinement leur capacité à protéger leurs réseaux, à répondre à une attaque et à s'en remettre. Par exemple, elles peuvent ne pas comprendre les limites de leurs contrats avec les fournisseurs d'infrastructure, ou la disponibilité des produits et services pour atténuer les attaques DDoS. Ils peuvent également ne pas comprendre pleinement le coût de la récupération après une telle attaque.

En l'absence d'une attaque en cours, les entreprises se concentrent traditionnellement sur la disponibilité, les fonctionnalités et le coût. En conséquence, les entreprises sont susceptibles de s'appuyer sur des dispositifs existants qui ne peuvent plus être sécurisés de manière adéquate, ou de déployer des dispositifs IoT et autres qui n'ont jamais été conçus pour être sécurisés. Où

[30] *Voir* David Goldman, *Major Banks Hit With Biggest Cyberattacks in History*, CNN (28 septembre 2012, 9:27 AM ET), http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

Lorsque les mises à jour de sécurité sont disponibles, les entreprises peuvent avoir des processus extrêmement onéreux pour évaluer les correctifs ou de longues périodes entre les maintenances programmées, ce qui élargit la fenêtre de vulnérabilité. [31]

Alors que les entreprises disposent généralement d'un personnel professionnel chargé des opérations informatiques, l'expertise spécifique à la cybersécurité fait souvent défaut. Cette difficulté est souvent aggravée par un manque de sensibilisation similaire chez les décideurs des organisations, qui sont responsables de l'affectation des ressources aux opérations informatiques au sein de leur organisation ou de la supervision de ces opérations. Les équipes chargées des opérations informatiques ne sont souvent pas conscientes des risques liés aux résolveurs ouverts et aux autres sources d'amplification des attaques, ni de l'importance du filtrage à l'entrée et à la sortie. Lorsque les FAI, par exemple, signalent à leurs clients une compromission potentielle, ils constatent souvent que l'entreprise ne peut pas identifier ou localiser les dispositifs compromis, et même si l'entreprise peut identifier et localiser les dispositifs, elle peut ne pas disposer des outils ou de l'expertise nécessaires pour rétablir un état sécurisé. Les entreprises peuvent avoir du mal à travailler en collaboration avec les fournisseurs de services lorsqu'elles sont attaquées. Si elles ne mettent pas en œuvre des procédures de sauvegarde de base, les entreprises risquent davantage d'avoir du mal à se remettre d'un ransomware distribué par des botnets.

Les entreprises peuvent contribuer à un écosystème plus résilient en combinant les technologies actuelles et émergentes, les politiques opérationnelles et d'approvisionnement, ainsi que la sensibilisation et l'éducation du personnel informatique et des décideurs.

Vision de l'avenir des réseaux d'entreprise

Une étape fondamentale vers cette vision consisterait à accroître l'application par les entreprises des principes contenus dans le cadre de cybersécurité du NIST (CSF). [32] La plupart des actions nécessaires peuvent être attribuées aux cinq fonctions simultanées et continues du cadre :

- **Identifier.** Les entreprises localisent les anciens appareils et les autres appareils qui ne peuvent pas être sécurisés. Dans la mesure du possible, elles retirent ces appareils à haut risque du service et les remplacent par des appareils qui sont intrinsèquement sûrs ou qui peuvent être sécurisés.
- **Protéger.** L'architecture du système fournit des couches de protection supplémentaires à tous les dispositifs à haut risque restants (par *exemple, l'*accès aux dispositifs existants serait limité par l'architecture du réseau). Les entreprises déploient ou se procurent des services d'atténuation des attaques DDoS sur site ou hors site. Les architectures réseau des entreprises limitent l'exposition des dispositifs aux acteurs malveillants et limitent les dommages causés par les attaques DDoS.
  les dispositifs compromis. Des filtres d'entrée et de sortie sont mis en place pour empêcher l'usurpation d'adresse réseau et les amplificateurs d'attaque (*par exemple, les* résolveurs ouverts) sont reconfigurés. Des processus de mise à jour efficaces minimisent la fenêtre de vulnérabilité de tous les dispositifs du réseau. Les infrastructures multilocataires appliquent également un filtrage à l'entrée et à la sortie afin de réduire l'impact des réseaux de zombies basés dans les nuages.
- **Détecter.** Une combinaison de services de détection basés sur les FAI et de surveillance des réseaux et des services exploités par les entreprises permet de détecter le trafic malveillant sortant et les attaques entrantes, et d'identifier les dispositifs compromis en temps quasi réel.
- **Répondre. Les** entreprises disposent de politiques et de procédures pour traiter les dispositifs compromis (par *exemple,* remplacer, atténuer ou patcher un dispositif participant à un botnet) lorsqu'ils sont détectés par l'entreprise ou

[31] *Voir* Dan Goodin, *Failure to Patch Two-month-old Bug Led to Massive Equifax Breach*, Ars Technica (13 sept. 2017), https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch- two-month-old-bug/. *Voir également* Federal Trade Commission, *Mobile Security Updates : Understanding the Issues* (février 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.

[32] National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cybersecurity- framework (dernière visite le 4 avril 2018).

FAI. Les entreprises ont également mis en place des processus pour contacter leur(s) FAI ou d'autres fournisseurs de services anti-DDoS lorsque des attaques sont détectées localement. Les ressources opérationnelles clés continuent de fonctionner avec des ressources limitées.

- **Récupérer.** Les entreprises ont la possibilité de reconstituer les systèmes compromis (par *exemple,* à partir d'une sauvegarde) plutôt que de payer des rançongiciels pour reprendre leurs activités.

Les technologies et les politiques opérationnelles décrites ci-dessus ne sont réalistes que si elles sont soutenues par une combinaison appropriée de politiques d'approvisionnement et d'initiatives de sensibilisation et d'éducation. Le personnel et la direction de l'entreprise doivent être conscients des risques que les menaces distribuées font peser sur les ressources de l'entreprise, ainsi que des options de protection, de réponse et de récupération. Le personnel informatique doit posséder les compétences nécessaires pour mettre en œuvre les options d'atténuation et de prévention retenues. Les politiques d'achat des organisations doivent garantir que les questions relatives au cycle de vie de la sécurité figurent en bonne place dans les décisions d'achat, afin d'éviter que des produits non sécurisés soient ajoutés au système ou y restent connectés. Pour avoir un impact significatif sur l'écosystème, ces changements doivent se produire dans les entreprises à l'échelle mondiale, et pas seulement au niveau national.

Dispositifs de pointe : État actuel

Les appareils constituent un domaine technique diversifié et en pleine expansion de l'écosystème. L'internet prend simultanément en charge des systèmes informatiques multi-utilisateurs, des dispositifs informatiques personnels et mobiles, des technologies opérationnelles (par *exemple,* des systèmes de contrôle et d'acquisition de données [SCADA] dans des environnements industriels ou de fabrication) et des dispositifs IoT dans tout l'écosystème. En règle générale, les périphériques jouent deux rôles diamétralement opposés en ce qui concerne les menaces distribuées : les acteurs malveillants compromettent les périphériques pour créer des menaces distribuées, et les périphériques peuvent également être la cible de la menace (par *exemple*, les attaques de ransomware distribuées par des botnets). Les points d'extrémité mal sécurisés peuvent être à la fois les sources et les victimes des attaques.

Les acteurs malveillants sont motivés pour construire des botnets aussi bon marché et efficaces que possible. Au fil des ans, les cibles ont évolué, allant des machines professionnelles aux appareils domestiques mal sécurisés, en passant par les systèmes vulnérables gérés par les hébergeurs et les fournisseurs de services en nuage et, plus récemment, par les appareils IoT. Ces changements de cibles reflètent les promesses et les défis offerts par ce domaine technique en ce qui concerne la création d'un écosystème plus résilient. Les ordinateurs personnels et les appareils mobiles sont plus sûrs que par le passé. Parallèlement, les appareils connectés ont atteint un niveau de sophistication et de densité qui facilite leur ciblage par un code automatisé, alors que les avantages des outils de sécurité modernes font défaut à ces appareils.

Les dispositifs de bord peuvent être vulnérables à la compromission pour diverses raisons :

- Souvent, les dispositifs n'ont pas été conçus en tenant compte de la sécurité. Les développeurs ne connaissent pas les bonnes pratiques de conception en matière de sécurité, supposent que le dispositif sera inaccessible (*par exemple,* sur un réseau local inaccessible depuis Internet) ou veulent éviter les solutions de sécurité qui imposent des coûts supplémentaires, augmentent le temps de mise sur le marché ou rendent le dispositif plus difficile à utiliser pour les consommateurs. Les choix de conception qui en résultent, tels que les mots de passe administratifs codés en dur, créent des dispositifs intrinsèquement peu sûrs. Dans d'autres cas, des contrôles de sécurité appropriés sont présents mais la facilité d'utilisation et les interfaces utilisateur donnent lieu à des configurations moins sûres.

[33] Gartner, *Gartner Says 8,4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, (Feb. 7, 2017), *disponible à l'adresse* : https://www.gartner.com/newsroom/id/3598917.

- Les techniques courantes de développement de logiciels aboutissent, de manière optimiste, à une faille toutes les 2 000 lignes de code34 - ou plus selon de nombreux autres paramètres. [35] Bon nombre de ces bogues créent des vulnérabilités de sécurité exploitables, telles que des débordements de mémoire tampon.
- Lorsque les bogues sont découverts après le déploiement des produits, il peut être difficile, voire impossible, de les corriger. Ces vulnérabilités sont souvent beaucoup plus faciles à exploiter qu'à corriger.
- Les systèmes livrés avec des paramètres de configuration par défaut inappropriés, tels que des mots de passe codés en dur, sont plus vulnérables en fonctionnement.
- Les systèmes peuvent également être vulnérables parce que le support n'est pas disponible. C'est souvent le cas pour les anciens appareils.
- L'ampleur et la diversité des dispositifs déployés rendent difficile la mise en place de solutions simples et offrent des surfaces d'attaque supplémentaires pour les activités malveillantes.

Un certain nombre de grands développeurs de logiciels ont pris ces leçons à cœur et ont établi de meilleures pratiques actuelles qui peuvent réduire considérablement les vulnérabilités des dispositifs périphériques. Par exemple, le cycle de vie du développement logiciel de Microsoft, ou SDLC, garantit que la sécurité est prise en compte dès le début.
Les outils de développement de logiciels sécurisés, tels que le fuzzing36 ou l'analyse statique[37], réduisent le nombre de vulnérabilités dans les logiciels. Les services de mise à jour sécurisés peuvent corriger les vulnérabilités après leur découverte. [38] Les systèmes sont livrés dans des configurations plus sûres, de sorte que les paramètres par défaut n'ont pas besoin d'être modifiés. Par conséquent, les serveurs, ordinateurs de bureau, ordinateurs portables et téléphones intelligents modernes offrent beaucoup moins de possibilités de compromission.
Cela s'applique également à l'environnement en nuage, les dispositifs périphériques plus sécurisés devenant une possibilité pratique. Les racines matérielles de confiance, qui démontrent que les systèmes n'ont pas été altérés, sont une autre innovation qui apparaît dans les systèmes modernes.

Malheureusement, les appareils IoT manquent souvent cruellement de fonctionnalités axées sur la sécurité. Ces systèmes offrent désormais la cible la plus attrayante pour les acteurs malveillants, et constituent un pourcentage de plus en plus important des appareils de l'écosystème. En fait, le rapport sur la mobilité d'Ericsson de novembre 2016 prévoit que les appareils IoT dépasseront les téléphones mobiles en tant que plus grande catégorie d'appareils connectés en 2018.[39] Compte tenu du niveau de sécurité des appareils IoT, il s'agit d'une prédiction décourageante.

[34] *Voir Coverity Scan : Open Source Report 2014*, Synopsys, page 4, (2015), http://go.coverity.com/rs/157-LQW- 289/images/2014-Coverity-Scan-Report.pdf.
[35] *Voir, par exemple,* Steve McConnell, *Code Complete : A Practical Handbook of Software Construction*, pages 521, 652, (Microsoft Press, 2e éd. 2004), ISBN : 0735619670.
[36] "Le test fuzz (fuzzing) est une technique d'assurance qualité utilisée pour découvrir les erreurs de codage et les failles de sécurité dans les logiciels, les systèmes d'exploitation ou les réseaux. Il consiste à introduire des quantités massives de données aléatoires, appelées fuzz, dans le sujet du test pour tenter de le faire planter." TechTarget - SearchSecurity.com, définition de fuzz testing (fuzzing), https://searchsecurity.techtarget.com/definition/fuzz-testing (dernière mise à jour en mars 2010).
[37] "L'analyse statique, également appelée analyse statique du code, est une méthode de débogage de programmes informatiques qui se fait en examinant le code sans exécuter le programme." TechTarget - SearchWinDevelopment.com, définition de l'analyse statique (analyse du code statique), https://searchwindevelopment.techtarget.com/definition/static-analysis (dernière mise à jour en novembre 2006).
[38] Le Software Assurance Forum for Excellence in Code (SAFECode), un consortium industriel, a publié un rapport pour codifier ces leçons et offrir des conseils supplémentaires sur le modèle SDLC. Mark Belk et al, *Fundamental Practices for Secure Software Development : A Guide to the Most Effective Secure Development Practices in Use Today*, SAFECode, (2nd ed.) (8 février 2011), *disponible à l'adresse* https://www.safecode.org/wp- content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf.
[39] Ericsson, *Ericsson Mobility Report : On the Pulse of the Networked Society*, (nov. 2016), https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november- 2016.pdf.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

En outre, ce domaine de l'écosystème n'est pas composé uniquement d'appareils modernes. De nombreux serveurs, ordinateurs de bureau, ordinateurs portables et téléphones mobiles anciens sont utilisés aujourd'hui, et il en sera ainsi dans un avenir prévisible. Les appareils anciens ne sont plus pris en charge par leurs fabricants, de sorte que leurs vulnérabilités ne peuvent être facilement corrigées. [40] Pour aggraver les choses, les outils d'attaque pour ces appareils ou leurs composants de code vulnérables restent largement disponibles.

Enfin, des pourcentages élevés de systèmes informatiques personnels sur Internet utilisent des logiciels piratés ; les statistiques d'une association industrielle pour 2015 allaient de 17 % aux États-Unis à 70 % en Chine et 84 % en Indonésie. [41] Les fabricants limitent généralement la distribution de correctifs de sécurité aux seuls systèmes exécutant des logiciels achetés légalement, de sorte que ces systèmes ne peuvent pas être sécurisés contre les vulnérabilités connues. Bien que l'on ne puisse raisonnablement attendre des fournisseurs qu'ils fournissent une assistance pour les logiciels sans licence, ces systèmes non protégés constituent une autre catégorie de cibles faciles pour les acteurs malveillants, et soulignent la nature internationale de ce défi.

Les dispositifs non sécurisés ne sont généralement pas le résultat des limitations de la technologie sous-jacente. Bien qu'imparfaites, les meilleures pratiques actuelles, lorsqu'elles sont appliquées correctement, sont assez efficaces, permettent d'obtenir des dispositifs raisonnablement sûrs à la livraison et comprennent des outils pour maintenir ce niveau de sécurité tout au long du cycle de vie du dispositif. Les secteurs commerciaux qui ont adopté ces pratiques, comme les développeurs de systèmes d'exploitation, ont démontré des améliorations significatives en matière de sécurité et de résilience. [42] Malheureusement, ces pratiques de sécurité sont mises en œuvre de manière incohérente. De nombreux produits sont livrés avec des bogues connus, ne comportent pas de mécanisme de mise à jour et/ou ne suivent pas les meilleures pratiques actuelles en matière d'accès administratif.

Une partie de ce problème peut être résolue par une sensibilisation et une éducation accrues. Certains développeurs de produits ne savent pas comment exploiter les outils actuellement disponibles pour le développement de produits sécurisés. Les développeurs de produits technologiques opérationnels comprennent leur gamme de produits (*par exemple, les* réfrigérateurs), mais peuvent ne pas comprendre les exigences de sécurité de base pour la connectivité réseau de leurs produits. Les entreprises clientes prennent des décisions d'achat sans tenir compte des coûts du cycle de vie complet, ni des externalités d'un réseau non sécurisé. Les consommateurs finaux ne disposent pas toujours des outils nécessaires pour comprendre comment certaines caractéristiques des produits les protègent des risques de sécurité ou comment leurs appareils peuvent avoir un impact négatif sur l'écosystème.

Les incitations du marché semblent exacerber le problème. Les concepteurs de produits privilégient le délai de mise sur le marché et les fonctionnalités innovantes au détriment de la sécurité et de la résilience. Les caractéristiques de sécurité ne sont pas facilement comprises ou communiquées au consommateur, ce qui rend difficile la création d'une demande.

[40] Par exemple, Microsoft a cessé de prendre en charge Windows XP, vieux de douze ans, en avril 2014. Deux ans plus tard, entre 7,4 et 10,9 % de tous les ordinateurs de bureau fonctionnaient encore sous XP et étaient décrits comme des "canards assis que les cybercriminels pouvaient attaquer." John Zorabedian, *Millions of People Are Still Running Windows XP*, Naked Security (11 avril 2016), https://nakedsecurity.sophos.com/2016/04/11/millions-of-people-are-still-running-windows-xp/.

[41] *Voir* BSA | The Software Alliance, *Seizing Opportunity Through License Compliance : BSA Global Software Survey*, (mai 2016), http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

[42] *Voir* Steven J. Vaughan-Nichols, *Security 2014 : The Holes Are in the Apps, not the Operating Systems*, ZDNet (28 février 2014, 19:46 GMT), http://www.zdnet.com/article/security-2014-the-holes-are-in-the-apps-not-the- operating-systems/.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Vision de l'avenir des dispositifs de pointe

De grandes avancées dans le domaine technique des périphériques sont à la fois possibles et essentielles si nous voulons construire un écosystème Internet et de communication plus résilient. Pour être efficaces, ces avancées doivent être mondiales, car la majorité des dispositifs Internet sont situés en dehors des États-Unis. Cette action mondiale nécessitera des normes et des pratiques de sécurité acceptées au niveau mondial, qui devront être solides, largement comprises et appliquées de manière omniprésente. Ces normes doivent être flexibles, s'inscrire dans un calendrier approprié, être ouvertes, volontaires et orientées par l'industrie.

Les appareils doivent pouvoir résister aux attaques tout au long de leur cycle de vie - au moment de l'expédition, pendant l'utilisation et jusqu'à la fin de leur vie. Pour ce faire, la sécurité doit devenir une exigence de conception primordiale. Les fournisseurs ne doivent pas livrer de dispositifs présentant des failles de sécurité graves connues, doivent inclure un mécanisme de mise à jour sécurisé et doivent suivre les meilleures pratiques actuelles (par *exemple,* pas de mots de passe codés en dur, désactivation des fonctions logicielles qui ne sont pas essentielles au fonctionnement) pour la configuration et l'administration du système.
Les fournisseurs doivent communiquer aux clients la durée minimale de l'assistance et les fabricants de dispositifs doivent maintenir des services de mise à jour sécurisés pendant la durée promise. [43]

Les racines matérielles de la confiance et les technologies d'exécution de confiance font désormais partie intégrante de nombreuses plates-formes informatiques prêtes à l'emploi. Les produits futurs devront tirer parti de ces technologies pour démontrer l'authenticité et l'intégrité lors du déploiement initial et tout au long de la période d'utilisation. Les techniques de développement modernes reposent sur une combinaison de composants open source et de composants disponibles dans le commerce. Pour répondre aux futures exigences de sécurité, ces composants doivent être traçables tout au long de la chaîne d'approvisionnement et offrir une plus grande assurance.

Ces progrès nécessiteront des avancées significatives en matière de sensibilisation et d'éducation des développeurs de produits. Tous les développeurs de produits doivent être dotés des connaissances et des compétences nécessaires pour appliquer les outils disponibles pour le développement de produits sécurisés. Les kits d'outils et les composants utilisés par ces fournisseurs doivent refléter les préoccupations en matière de sécurité afin d'atteindre l'échelle et de suivre le rythme de l'évolution de la main-d'œuvre des développeurs, et les partenariats et consortiums à l'origine de la technologie normalisée doivent permettre aux développeurs de prendre et de communiquer des décisions en matière de sécurité. Pendant ce temps, les développeurs de produits technologiques opérationnels doivent ajouter des exigences de sécurité de base à leurs connaissances et compétences spécifiques aux produits. Dans le même temps, les clients doivent disposer de connaissances et d'informations suffisantes pour choisir des produits conçus pour être sécurisés dans leurs environnements, et doivent être conscients des risques présentés par tous les dispositifs, y compris les dispositifs hérités.

Enfin, les incitations du marché devront s'aligner sur ces progrès en matière de sécurité, de sorte que les développeurs de produits qui accordent la même priorité à la sécurité et à la résilience qu'aux délais de commercialisation et aux fonctionnalités innovantes soient récompensés. Des signaux clairs concernant la sécurité et la résilience des produits, accessibles aux clients, contribueront à améliorer ces incitations. Cependant, la proposition de valeur pour une meilleure sécurité commencera probablement dans l'environnement de l'entreprise en raison de ses économies d'échelle ; une fois qu'il existe une posture de sécurité généralement acceptée dans une classe de produits donnée, peu de fabricants seront susceptibles de l'ignorer.

[43] *Voir, par exemple*, le processus multipartite de la NTIA sur la capacité de mise à jour et de correction de la sécurité de l'Internet des objets - Groupe de travail sur la communication de la capacité de mise à jour et l'amélioration de la transparence, *Communiquer la capacité de mise à jour de la sécurité des dispositifs IoT pour améliorer la transparence pour les consommateurs*, (14 juillet 2017), https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-._jul_14_2017_-_ntia_multistakeholder_process.pdf (aider les fabricants à partager les détails des mises à jour de sécurité avec les consommateurs, et donner aux consommateurs les outils pour savoir ce qu'il faut rechercher).

Réseaux domestiques et de petites entreprises : État actuel

Les réseaux des particuliers et des petites entreprises sont de plus en plus complexes. Les appareils informatiques traditionnels interagissent avec le cloud et d'autres fournisseurs de services pour prendre en charge un éventail toujours plus large d'applications professionnelles et personnelles. Les dispositifs IoT prolifèrent déjà en grand nombre dans les foyers des consommateurs, qu'il s'agisse de dispositifs domotiques tels que les lumières, les ouvreurs de portes de garage et les thermostats, d'appareils électroménagers connectés ou de moniteurs de santé et de fitness personnels. Cette prolifération est également le cas dans les petites entreprises, où les entrepreneurs et les dirigeants peuvent chercher à tirer parti de la technologie disponible sur le marché, mais ne disposent pas d'un administrateur ou de stratégies ou politiques informatiques concertées. Selon toutes les estimations, le nombre d'appareils connectés destinés aux consommateurs devrait augmenter.

Malheureusement, ce domaine de croissance est aussi un domaine dans lequel la sécurité fait sérieusement défaut. La grande majorité des particuliers et des petites entreprises ne sont pas conscients des risques de cybersécurité, et beaucoup ne prennent pas les mesures de sécurité les plus élémentaires lorsqu'ils connectent des appareils à leur réseau. Les décisions relatives à la sécurité peuvent être prises sans l'avis ou la connaissance du client si le dispositif est installé et configuré par quelqu'un d'autre en son nom ou si le dispositif utilise un réseau autre que le propre réseau du consommateur (par exemple, un réseau cellulaire). Parallèlement, le partage des informations sur les menaces est un défi pour les petites entreprises, qui ne disposent généralement pas des ressources des grandes organisations pour recevoir et traiter les informations sur les menaces.

Comme dans les domaines détaillés ci-dessus, de nombreux outils existent généralement pour atténuer les risques liés à la cybersécurité, mais il n'est pas réaliste d'attendre de la population générale qu'elle soit capable de s'y retrouver dans l'environnement complexe de la sécurité. Les petites entreprises et les particuliers peuvent être victimes d'attaques DDoS - souvent en échange d'une rançon pour faire cesser les attaques - ou être les hôtes involontaires de dispositifs utilisés dans un botnet. Les produits pour réseaux domestiques ne sont généralement pas conçus de manière à permettre aux utilisateurs de segmenter facilement les réseaux ou de configurer les politiques de sécurité. De nombreux particuliers utilisent des appareils anciens ou des systèmes sans licence. En outre, lorsque l'appareil d'un particulier fait partie d'un botnet, il est souvent difficile pour le fournisseur de réseau de savoir quel appareil transmet, car la fonction NAT, qui permet aux particuliers de partager une seule adresse IPv4 entre de nombreux appareils derrière un routeur domestique, masque l'appareil qui est exploité. [44]

Sur le marché des particuliers et des petites entreprises, la plupart des appareils domestiques ne sont pas gérés et sont donc peu susceptibles d'être mis à jour manuellement, si les fonctions de mise à jour automatique ne sont pas disponibles. Les appareils grand public sont souvent livrés avec des logiciels obsolètes contenant des vulnérabilités connues ou des mots de passe administratifs codés en dur. L'utilisateur type peut ne pas être en mesure de déterminer si le logiciel de l'appareil est mis à jour ou s'il dispose même d'un mécanisme de mise à jour logicielle - ce qui n'est pas le cas de nombreux appareils grand public. L'utilisateur lambda n'est peut-être même pas conscient de l'importance de cet aspect, et n'a peut-être pas accès à des informations substantielles sur le logiciel d'un appareil donné.

Même si le réseau de la maison ou de la petite entreprise est bien architecturé et dispose de contrôles de sécurité solides, certains des appareils pris en charge sont susceptibles d'être mobiles et de se connecter à plusieurs réseaux au cours d'une journée normale. Ces réseaux peuvent ne pas être aussi bien gérés et les appareils peuvent être compromis lorsqu'ils se trouvent sur le réseau extérieur. Ces appareils présentent un risque supplémentaire en matière de cybersécurité, car ils permettent l'introduction de codes malveillants tout en contournant les contrôles locaux.

En général, les particuliers et les petites entreprises n'ont pas facilement accès aux informations dont ils ont besoin pour choisir des produits sûrs, et ils ne disposent généralement pas d'outils pour gérer les produits qu'ils possèdent. Alors que

[44] Nous notons également que la technologie NAT offre certains avantages en matière de sécurité en limitant l'accès du trafic entrant à des points d'extrémité spécifiques. Cela permet d'entraver (mais pas d'éliminer complètement) la menace que représentent les outils d'analyse et d'infection automatisés.

Les passerelles d'entreprise sont plus susceptibles de fournir des offres de sécurité intégrées, mais il est peu probable que les utilisateurs domestiques aient accès au même niveau de service, et pour ceux qui y ont accès, beaucoup ne sont pas conscients des offres de sécurité ou de la raison pour laquelle ces services devraient être mis en œuvre. Les mesures de sécurité fondamentales, telles que la modification du mot de passe par défaut d'un appareil ou l'activation d'un cryptage sécurisé, échappent souvent à la connaissance ou aux capacités des consommateurs. Dans certains cas, une mauvaise application de ces exigences peut contrarier les efforts des utilisateurs pour mettre en œuvre ces pratiques de base.

On craint que les consommateurs ne paient pas davantage pour des appareils offrant une meilleure sécurité. En réalité, les expériences des consommateurs ne sont généralement pas directement affectées par la compromission de leurs appareils ; en fait, le consommateur peut ne jamais savoir que son appareil fait partie d'un botnet. Du point de vue du consommateur, la webcam continue de fonctionner ou le réfrigérateur continue de refroidir. Pour cette raison, il peut être difficile de tenir les propriétaires responsables si leurs appareils sont utilisés dans un botnet. L'absence de conséquences claires de l'infection incite les consommateurs à prendre des mesures pour améliorer la sécurité, par exemple en mettant à jour les appareils qui peuvent l'être.

Vision de l'avenir des réseaux domestiques et des réseaux de petites entreprises

Il n'est pas réaliste d'attendre des utilisateurs privés et des propriétaires de petites entreprises qu'ils deviennent des experts en sécurité. Cependant, il existe des mesures que les acteurs du secteur et d'autres peuvent prendre pour améliorer la situation. Outre les efforts de sensibilisation et d'éducation visant à modifier le comportement des consommateurs, une autre approche consiste à concevoir des appareils en tenant compte du comportement des utilisateurs. Idéalement, les appareils commercialisés auprès des consommateurs devraient être conçus en intégrant la sécurité. Les produits grand public devraient être conçus de manière aussi sûre que possible, inclure des mécanismes de mise à jour automatisés et sécurisés, et n'avoir que peu ou pas d'exigences en matière de gestion des produits.

Dans l'idéal, les consommateurs auront accès à des offres commerciales qui mettent en œuvre les meilleures pratiques actuelles en matière de sécurité, et ils seront en mesure de reconnaître facilement ces offres. De même, les propriétaires de petites entreprises seront en mesure de faire correspondre leurs achats à leurs préoccupations et obligations uniques en matière de sécurité. Ils seront conscients des différents risques liés aux dispositifs IoT non sécurisés et choisiront des dispositifs plus sûrs.
Des organisations à but non lucratif et des entités commerciales ont commencé à évaluer les produits du point de vue de la protection de la vie privée et de la sécurité des données ; des efforts de ce type permettront de sensibiliser le public et, à mesure que la sensibilisation augmentera, les fabricants d'appareils devraient s'intéresser au développement sécurisé. Au fil du temps, il devrait devenir plus facile et moins coûteux pour les fabricants et les intégrateurs d'adopter un cycle de vie de développement sécurisé.

Si les utilisateurs domestiques ne sont pas particulièrement motivés par la crainte que leurs appareils soient utilisés dans un botnet, ils peuvent se sentir plus contraints par la crainte que leur vie privée, leurs données ou leur accès aux services ne soient compromis. De nombreux appareils connectés utilisent des services en nuage pour la gestion et le stockage des informations, ce qui a des implications supplémentaires en matière de sécurité et de confidentialité. Heureusement, la plupart des mesures qu'ils prendraient pour améliorer la sécurité de leur vie privée ou de leurs données et garantir un accès ininterrompu aux services réduiraient également le risque que leurs appareils fassent partie d'un botnet.

Avec des incitations correctement appliquées, les forces du marché peuvent jouer un rôle clé dans l'amélioration de la sécurité des dispositifs. Pour que les consommateurs adoptent largement des dispositifs plus sécurisés, ces derniers ne doivent pas coûter beaucoup plus cher que les dispositifs de sécurité.

[45] Bruce Schneier, *Security Economics of the Internet of Things*, Schneier on Security (10 oct. 2016, 10:26 AM) https://www.schneier.com/blog/archives/2016/10/security_econom_1.html (dernière mise à jour le 17 oct. 2016).
[46] Consumer Reports, *Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security*, (6 mars 2017), *disponible sur* https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating- products-services-for-privacy-and-data-security/.

des appareils non sécurisés. Les produits et services grand public devraient être conçus en intégrant des protections de base en matière de confidentialité et de sécurité. Des guides d'achat faciles à comprendre et fournissant des recommandations pratiques, ciblées sur les besoins spécifiques des particuliers et des petites entreprises, peuvent générer les signaux de marché nécessaires pour récompenser les développeurs et les vendeurs qui investissent dans la sécurité.

Les routeurs et les pare-feu intelligents devraient être largement utilisés pour atténuer les attaques et détecter lorsqu'un appareil a été compromis. À mesure que les appareils IoT des particuliers passent à des adresses IPv6 publiquement adressables, les FAI auront plus de facilité à identifier les appareils finaux transmettant du trafic malveillant. Les réseaux des particuliers appliquent la segmentation des réseaux virtuels. Limiter les capacités des appareils en fonction de leur utilisation prévue - par exemple, limiter les activités d'un grille-pain connecté sur le réseau aux seules activités nécessaires à l'exécution de ses tâches de grillage - limiterait considérablement la capacité des botnets à capturer les appareils domestiques. Un déclin mondial de l'utilisation domestique des produits anciens et des logiciels piratés limiterait aussi considérablement les possibilités des auteurs de botnets.

Les utilisateurs domestiques devraient être en mesure d'identifier les dispositifs de leurs réseaux qui augmentent leur risque de cybersécurité. Des travaux de recherche et développement sont en cours pour aider les consommateurs soucieux de sécurité à mieux gérer leurs réseaux. En 2017, l'IoT Home Inspector Challenge de la Federal Trade Commission (FTC) a décerné son premier prix à une proposition d'outil basé sur une application mobile qui aiderait les utilisateurs à gérer les appareils IoT de leur domicile. L'appli signalerait les appareils dont le logiciel n'est pas à jour et d'autres vulnérabilités courantes et fournirait des instructions sur la façon de mettre à jour le logiciel de chaque appareil et de corriger les autres vulnérabilités. [47]

L'éducation des consommateurs devra devenir plus efficace, même si les appareils sont mieux adaptés au niveau de compétence attendu des consommateurs. Entre-temps, il existe une possibilité de créer une nouvelle main-d'œuvre pour répondre aux besoins des consommateurs et des petites entreprises en matière de réseaux ; ce rôle pourrait devenir une nouvelle vocation, plus proche de celle des électriciens que de celle des ingénieurs électriciens, avec une formation appropriée. Les industries des réseaux et des dispositifs peuvent également rendre le soutien plus facile et moins coûteux grâce à la normalisation et à la coordination.

Gouvernance, politique et coordination

Étant donné que les attaques automatisées et distribuées sur l'internet mondial constituent un problème à l'échelle de l'écosystème, cette question nécessitera une coordination des solutions politiques et de gouvernance entre les secteurs. Aucun acteur ou secteur n'est responsable à lui seul de la gestion de ces risques, et aucune entité ne peut prétendre que ces risques sont le problème de quelqu'un d'autre. Par exemple, si de nombreuses solutions impliquent une coordination active avec les fournisseurs d'accès à Internet, le fait de placer la responsabilité exclusive au niveau du réseau rendrait imprudemment tout le trafic dépendant de cette couche connective pour déterminer à quoi ressemble le "bon" trafic, obligeant les fournisseurs d'accès à décider ce qui est fondamentalement autorisé ou non sur l'Internet. De plus, cette prise de décision des FAI bloquerait invariablement le trafic qui est en fait "bon", et manquerait le trafic qui devrait être bloqué ; le trafic crypté exacerberait le problème.

Étant donné la nature en réseau des risques, une véritable coordination est nécessaire pour comprendre pleinement le problème et identifier des pistes de solutions. Si les secteurs des technologies de l'information et des communications s'emploient activement à comprendre les risques pour la sécurité, certains secteurs éprouvent des difficultés à partager les informations et à se coordonner en dehors de leur propre secteur. Certaines entités coordonnent leur action au niveau national ou régional, mais il est nécessaire de partager davantage d'informations sur les menaces, les solutions, leur adoption et leur efficacité à l'échelle mondiale. Sur le site

[47] Federal Trade Commission, *IoT Home Inspector Challenge*, https://www.ftc.gov/iot-home-inspector-challenge (dernière visite le 4 avril 2018).

Dans de nombreux cas, le manque de clarté concernant les rôles et les responsabilités a entravé l'action collective, entraînant des défaillances en matière de sécurité.

Certains gouvernements s'appuient sur des réglementations trop spécifiques qui deviennent rapidement obsolètes, entravent l'innovation et limitent les avantages pour le consommateur dans les secteurs dynamiques. Les exigences de conformité, ou la mise en place de réglementations spécifiques, peuvent permettre de faire face à certains risques, mais elles peuvent entraîner une charge plus lourde tout en laissant l'écosystème plus large dans l'insécurité ou en envoyant le signal que la conformité à la réglementation est suffisante plutôt que le minimum nécessaire. Le tableau réglementaire est encore compliqué par la réglementation nationale ou locale des dispositifs périphériques, de la technologie opérationnelle et de l'infrastructure. Les solutions spécifiques à certains pays ou juridictions mettent en danger la nature globale d'un écosystème où les bits et les produits circulent avec une relative facilité, et peuvent désavantager les innovateurs locaux.

Ce problème est encore aggravé par la nature inter-domaines de la technologie en réseau. Les frontières se sont estompées entre la technologie grand public, les outils et les dispositifs de niveau entreprise dont dépendent les organisations, et la technologie critique pour la sécurité dont peuvent dépendre des vies. Le même matériel et les mêmes logiciels peuvent être utilisés dans l'ensemble de l'écosystème. Les services d'infrastructure clés peuvent être utilisés aussi bien par un réseau de jeux vidéo que par le réseau d'entreprise d'une société.

Dans le domaine de l'application de la loi, la coopération de l'industrie dans le démantèlement des botnets s'améliore, mais n'est pas encore monnaie courante. Les récents démantèlements réussis de botnets ont nécessité une importante collaboration avec l'industrie dans les cas, par exemple, de Kelihos, Gameover Zeus et Coreflood. Une collaboration active entre les forces de l'ordre et le secteur privé a permis de perturber les activités en saisissant des actifs clés de commandement et de contrôle. Aux États-Unis, en 2016, la règle fédérale de procédure pénale 41(b)(6) a été modifiée pour répondre aux défis uniques des enquêtes sur les activités des botnets, en précisant que les tribunaux peuvent délivrer des mandats autorisant la perquisition de plusieurs ordinateurs lorsque les ordinateurs identifiés sont situés dans plusieurs districts judiciaires. En outre, la capacité des services fédéraux d'application de la loi à obtenir des injonctions civiles - ce qui s'est avéré indispensable dans le cadre de démantèlements antérieurs de botnets - est limitée aux affaires comportant des éléments d'écoute électronique ou certains types de fraude. Le démantèlement des botnets de manière sûre et sécurisée est un processus long et laborieux. En outre, les forces de l'ordre ont du mal à identifier et à poursuivre les acteurs malveillants responsables des botnets, en particulier ceux qui opèrent en dehors des États-Unis.

Vision pour l'avenir de la gouvernance, des politiques et de la coordination

À l'avenir, les acheteurs - qu'il s'agisse de consommateurs finaux ou d'entreprises sophistiquées - devraient être mieux à même de comprendre les risques et les propriétés de sécurité des appareils connectés. Il est nécessaire d'adopter des approches de l'IdO et des dispositifs informatiques qui contribueront non seulement à sensibiliser les consommateurs, mais aussi à stimuler le marché, en augmentant l'adoption générale et l'utilisation de meilleures pratiques de cybersécurité par les fabricants de dispositifs. Cela dit, le risque de sécurité évolue rapidement ; ce qui est considéré comme sûr aujourd'hui peut ne pas l'être demain, et il est peu probable qu'il le soit dans dix ans. Les solutions de transparence du marché peuvent permettre aux acheteurs de prendre de bonnes décisions, mais elles doivent également tenir compte du contexte et de l'échelle de temps du cycle de vie du produit. Les institutions qui se sont appuyées sur des approches qui reflétaient traditionnellement un risque statique, comme les exigences d'achat ou les assurances, devront s'adapter pour refléter la nature évolutive du risque de cybersécurité. Une meilleure transparence des composants logiciels et matériels des systèmes sera utile, tout comme des incitations appropriées pour comprendre les risques pertinents dans un contexte donné et pour l'écosystème dans son ensemble.

Les acteurs de l'infrastructure partageront et analyseront mieux les données afin de favoriser une connaissance commune des réputations dans l'ensemble de l'écosystème et d'évaluer dans quelle mesure les partenaires du réseau traitent les risques de manière évolutive, efficace et décentralisée. Les mécanismes de partage de l'information devraient s'appuyer sur les mécanismes existants.

les mécanismes multipartites et les communautés, créant ainsi de nouvelles possibilités d'engagement au niveau local et mondial.

À mesure que les menaces distribuées évoluent, de nouvelles normes, directives et mesures peuvent être nécessaires pour répondre à des questions nouvelles et émergentes telles que : Comment les tiers peuvent-ils évaluer au mieux les produits pour les avantages des consommateurs d'une manière suffisamment agile pour suivre l'évolution rapide des pratiques de sécurité ? Quelles mesures et quelle visibilité sur les pratiques de gestion des réseaux peuvent nous informer sur les investissements dans les infrastructures ? Des attentes plus formelles mais adaptables en matière de sécurité nous permettront d'introduire une certaine responsabilité dans les pratiques de sécurité. Des mécanismes tels que les cadres volontaires peuvent contribuer à la fois à créer des incitations à une conception plus sûre et à responsabiliser les personnes qui ne prennent pas en compte la sécurité et n'investissent pas dans des dispositifs sûrs. Tout mécanisme de responsabilisation doit récompenser ceux qui prennent de bonnes décisions fondées sur le risque, tout en reconnaissant que la sécurité parfaite n'existe pas.

Pour faire face à l'éventail des menaces, toutes les parties prenantes, nationales et internationales, doivent s'attaquer plus complètement aux attaques automatisées et distribuées. Il s'agit essentiellement de réduire le nombre de dispositifs non sécurisés ayant accès à l'Internet afin de limiter la taille des réseaux de zombies et de mettre au point des mécanismes permettant de partager les informations sur les systèmes compromis et les nouvelles tendances en matière d'attaques, en amont et en aval de la pile de réseaux, avec la ou les parties les mieux placées pour répondre à la menace.

Le déploiement des technologies étant véritablement transnational et les informations circulant au-delà des frontières internationales, rien de tout cela ne peut être accompli sans collaboration internationale. Dans le domaine international, le gouvernement américain plaide vigoureusement en faveur d'approches dirigées par l'industrie et de normes volontaires, fondées sur le consensus. Comme l'indique le rapport du NSTAC, les solutions dépendent à la fois des normes et de l'innovation au niveau des réseaux et de l'infrastructure Internet. Bien qu'il existe une variété de normes, de cadres et de meilleures pratiques pertinents, ils ne sont pas pleinement exploités dans le monde entier.

Les gouvernements peuvent influencer de manière constructive le développement de produits plus sûrs en prenant des mesures telles que le soutien de normes ouvertes, volontaires et axées sur l'industrie, et en prenant leurs propres décisions en matière d'acquisition de technologies et de dispositifs de manière à créer des incitations commerciales en faveur de produits plus sûrs.
La sécurité peut également être favorisée par un engagement multipartite accru entre les communautés de lutte contre les abus et d'infrastructure de réseau mondial, ainsi qu'entre les éléments de cybersécurité et de technologie opérationnelle des industries qui ne sont pas traditionnellement axées sur les TI (par *exemple,* les services publics ou les appareils médicaux). Par exemple, l'engagement opérationnel et multipartite lié aux ressources Internet utilisées par les gestionnaires de botnets pour le commandement et le contrôle est essentiel à la signalisation des menaces pour la gestion des réseaux et la détection des botnets. Les États-Unis devraient accroître leur engagement international dans ce domaine, en particulier avec les pays qui sont déjà actifs sur cette question.

En outre, l'industrie et les services répressifs devraient s'efforcer de trouver des moyens de se coordonner plus souvent et plus tôt pour détecter et prévenir les activités menaçantes, et pour gérer les incidents qui se produisent. De nouveaux outils et processus pourraient améliorer le partage de l'information entre les organismes internationaux d'application de la loi. Les services répressifs et les groupes industriels devraient communiquer plus efficacement sur ce qui est nécessaire pour réussir à perturber les réseaux malveillants et poursuivre les acteurs qui en sont à l'origine, tout en gardant à l'esprit les préoccupations en matière de protection de la vie privée. Les politiques de protection des données, tant aux États-Unis qu'au niveau international, ne devraient pas perturber les outils existants, tels que la base de données WHOIS, largement utilisée pour les données relatives à la propriété des domaines.

Paysage juridique

Certaines parties prenantes ont souligné l'importance de minimiser l'incertitude et le risque juridique pour encourager la collaboration du secteur privé avec les organismes chargés de l'application de la loi, un plus grand partage des informations, la divulgation des vulnérabilités et la capacité à mener des contre-mesures efficaces. Beaucoup ont également souligné la nécessité d'harmoniser les approches juridiques entre les secteurs afin d'éviter un patchwork de lois qui pourrait entraver le marché de l'IdO.

Des efforts sont déjà en cours pour améliorer les relations public-privé. Le Centre national d'intégration de la cybersécurité et des communications (NCCIC) du DHS sert de lieu central où un ensemble diversifié de partenaires du secteur privé et du gouvernement impliqués dans la cybersécurité coordonnent leurs efforts[48], y compris le partage d'informations, la collaboration et l'assistance technique. [49] Le droit fédéral comprend déjà une structure permettant de répondre à une partie de l'incertitude et du risque juridique. La loi de 2015 sur le partage des informations en matière de cybersécurité (CISA), par exemple, accorde une protection en matière de responsabilité et d'autres protections juridiques - telles que des protections antitrust, des exceptions aux lois sur la divulgation et à certaines utilisations réglementaires, et des protections contre les renonciations aux privilèges - aux entités privées qui partagent des indicateurs de cybermenaces et des mesures défensives conformément à la loi. [50] La CISA désigne le NCCIC comme centre de partage des indicateurs de cybermenaces et des mesures défensives avec le gouvernement fédéral. Ces capacités de cybersécurité du NCCIC et les protections juridiques de la CISA s'appliquent à la cybersécurité de l'IdO de la même manière qu'elles s'appliquent à la cybersécurité en général. En outre, rien dans la CISA n'empêche les entités privées de partager avec les forces de l'ordre des informations solides dans le cadre du déroulement normal d'une enquête criminelle ; en effet, la CISA autorise le partage d'indicateurs de cybermenace et de mesures défensives avec les forces de l'ordre - ou toute autre entité fédérale - et, en outre, sa protection en matière de responsabilité s'applique lorsque ces informations sont partagées avec les forces de l'ordre dans certaines circonstances.

De nombreuses parties prenantes ont également souligné l'importance des incitations commerciales pour sécuriser les dispositifs IdO. Certains se sont demandé si un régime de responsabilité fondé sur des normes et des pratiques exemplaires communes pourrait améliorer la responsabilité en matière de sécurité des dispositifs IdO. Bien que le présent rapport ne s'engage pas dans une analyse exhaustive de la responsabilité liée à la sécurité des dispositifs IdO, nous pensons que cette question continuera à susciter de l'intérêt à mesure que l'utilisation des dispositifs connectés - des dispositifs qui peuvent avoir un impact sur le monde physique - augmentera et que des questions concernant les préjudices, les problèmes de confidentialité, la protection des consommateurs, les chaînes de causalité, la gestion des risques et les actions possibles des États et des tribunaux émergeront. La responsabilité est un domaine complexe du droit, tout comme le marché émergent de l'IdO, et il faut veiller à éviter les exigences de conformité statiques et inefficaces, en particulier au milieu d'un paysage dynamique de cybersécurité. Des investissements doivent être réalisés pour faire face aux risques par le biais de pratiques innovantes, et avec des parties prenantes engagées dans une coordination intersectorielle. La pression pour aborder directement cette question augmentera si l'incertitude juridique est endémique et persistante.

Certaines parties prenantes ont noté que tout nouveau régime juridique ou réglementaire pourrait avoir des effetsnégatifs involontaires sur le secteur des TI si des orientations claires ne sont pas incluses concernant ce qu'un fournisseur peut faire pour limiter son exposition. Toutefois, les défenseurs mettent en garde contre les protections générales en matière de responsabilité sans gains sociaux clairs découlant de l'amélioration des processus de sécurité. Certaines parties prenantes, y compris des organisations de la société civile, ont demandé des éclaircissements supplémentaires sur la manière dont les lois existantes dans diverses juridictions s'appliquent dans ce domaine, sur la manière dont ces lois peuvent ou doivent affecter les différentes parties prenantes le long des chaînes d'approvisionnement et de distribution, et sur la manière de traiter correctement les préjudices. Alors que ce domaine continue d'évoluer, il est essentiel que le gouvernement fédéral comprenne mieux l'interaction entre la responsabilité et les incitations du marché, ainsi que la manière dont tout changement proposé pourrait modifier cette dynamique. Il faut veiller à ce que nos lois sur la responsabilité profitent aux consommateurs, protègent les parties prenantes le cas échéant et évitent de freiner l'innovation dans l'environnement numérique actuel. Au fur et à mesure que la collaboration entre les secteurs public et privé se poursuit dans ce domaine, le gouvernement fédéral

devrait continuer à vérifier si la protection contre la responsabilité liée au partage d'informations est suffisante dans l'environnement actuel pour faire face efficacement aux menaces actuelles et nouvelles.

III. Objectifs et actions

Ces objectifs et actions visent à présenter un portefeuille d'actions se renforçant mutuellement qui, si elles sont mises en œuvre, amélioreront considérablement la résilience de l'écosystème. Les actions recommandées comprennent des activités en cours qui devraient être poursuivies ou étendues, ainsi que de nouvelles initiatives. Aucun investissement ou activité ne peut à lui seul atténuer toutes les menaces, mais les discussions organisées et les commentaires des parties prenantes nous permettront d'évaluer plus avant et de hiérarchiser ces activités en fonction du retour sur investissement attendu et de leur capacité à avoir un impact mesurable sur la résilience de l'écosystème. Nous attendons des parties prenantes de l'ensemble de l'écosystème qu'elles collaborent avec le gouvernement pour mettre en œuvre les activités proposées, saisir les occasions de soutien et de leadership, et supprimer les obstacles à la mise en œuvre.

Objectif 1 : définir une voie claire vers un marché technologique adaptable, durable et sûr.

Pour renforcer la résilience de l'écosystème de l'Internet et des communications, il est essentiel que notre marché technologique soutienne et récompense le développement, l'adoption et l'évolution continus de technologies et de processus de sécurité innovants. Lorsque les incitations du marché encouragent les fabricants à présenter les innovations en matière de sécurité comme un complément équilibré aux fonctionnalités et aux performances, cela favorise l'adoption d'outils et de processus qui aboutissent à des produits plus sûrs. Au fur et à mesure que ces caractéristiques de sécurité deviennent plus populaires, la demande accrue stimule la recherche. Au fur et à mesure que ces outils sont perfectionnés, il devient moins coûteux pour les fabricants, les intégrateurs et les propriétaires/exploitants de systèmes d'adopter les composants d'un cycle de développement sécurisé, ce qui encourage davantage de fabricants à différencier leurs produits en fonction de la qualité de leurs fonctions de sécurité et permet ainsi une plus grande concurrence. Cette section identifie les actions que les principales parties prenantes peuvent entreprendre pour établir un marché technologique adaptable, durable et sécurisé.

Action 1.1 : à l'aide de processus inclusifs dirigés par l'industrie, établir des lignes de base de capacités IoT applicables au niveau international pour assurer la sécurité du cycle de vie des applications domestiques et industrielles, sur la base de normes internationales volontaires dirigées par l'industrie.

[48] *Voir* 6 U.S.C. § 148.
[49] *Id.* § 148(c).
[50] *Voir* Consolidated Appropriations Act, 2016, Division N - Cybersecurity Act of 2015 (Pub. L. No. 114-113, 129 Stat. 2242) (codifié à 6 U.S.C. §§ 1501-1510).
[51] La CISA offre une série de protections juridiques pour les indicateurs de cybermenaces et les mesures défensives qui sont partagés avec une entité fédérale conformément à la loi. Par exemple, elle prévoit une protection contre la responsabilité antitrust (6 U.S.C. § 1503(e)) ; les lois fédérales et étatiques sur la divulgation (6 U.S.C. §§ 1504(d)(3) et 1503(d)(4)(B)) ; la renonciation aux privilèges (6 U.S.C. § 1504(d)(1)) ; et l'utilisation réglementaire fédérale et étatique (6 U.S.C. §§ 1503(d)(4)(C) et 1504(d)(5)(D)). Lorsque les indicateurs de cybermenace et les mesures défensives sont partagés avec le NCCIC par le biais de la capacité du gouvernement fédéral et du processus géré par le DHS, ce partage bénéficie également de protections supplémentaires en matière de responsabilité. 6 U.S.C. § 1504(c)(1)(B). Ces protections supplémentaires en matière de responsabilité sont également disponibles pour le partage avec d'autres entités fédérales dans des circonstances limitées. *Voir* 6 U.S.C. § 1504(c)(1)(B)(i) et (ii).

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Les normes de sécurité, les lignes de base et les meilleures pratiques ont évolué au fil du temps pour les dispositifs informatiques traditionnels, augmentant le coût de l'assemblage de botnets avec ces dispositifs. L'augmentation rapide du déploiement de dispositifs IoT non sécurisés a eu l'effet secondaire pernicieux de permettre le développement rentable de botnets extrêmement importants et largement distribués. Par exemple, les botnets Mirai ont compromis des centaines de milliers d'appareils grâce à des mots de passe administratifs codés en dur. Plus récemment, le botnet Reaper a compromis des appareils en ciblant des vulnérabilités logicielles bien connues. Bien qu'il existe des mesures d'atténuation, de nombreux appareils touchés ne peuvent être corrigés. Comme les mots de passe ne peuvent pas être changés et que les vulnérabilités ne peuvent pas être corrigées, ces appareils resteront vulnérables tout au long de leur cycle de vie. Ces vulnérabilités pourraient être atténuées dans les futurs systèmes IdO si les meilleures pratiques actuelles en matière de sécurité pour les appareils informatiques traditionnels, telles que des configurations par défaut sécurisées et des mécanismes efficaces de mise à jour des logiciels, étaient appliquées aux appareils IdO.

L'impact des botnets passés a été atténué par les mesures prises par les fournisseurs d'infrastructure tels que les FAI - principalement des actions de cessation et d'abstention et l'absorption du trafic excessif - mais les mesures d'atténuation passées étaient principalement de nature réactive, et l'augmentation exponentielle des dispositifs et systèmes IoT indique que les rendements de ces stratégies d'atténuation traditionnelles diminuent. L'écosystème doit devenir plus résilient aux menaces distribuées, en commençant par une approche proactive et ciblée sur la réduction des vulnérabilités connues des appareils connectés à l'internet tout au long de leur cycle de vie.

Les bases de capacités de sécurité basées sur les performances - qui identifient des suites de normes, de spécifications et de mécanismes de sécurité volontaires représentant la combinaison des meilleures pratiques de sécurité du cycle de vie pour un environnement de menace particulier - sont nécessaires pour accélérer le développement et le déploiement d'appareils et de systèmes IoT moins vulnérables à la compromission tout au long de leur cycle de vie. [52] Par exemple, une base de référence pour les environnements domestiques pourrait inclure des mécanismes de mise à jour sécurisés, tels que l'application automatique de correctifs de sécurité et des configurations sécurisées par défaut, qui minimisent la nécessité d'une intervention de l'utilisateur. Une base de référence en matière de sécurité pour une industrie peut supposer un personnel de sécurité dévoué et compétent qui utilise des processus tels que des mises à jour gérées de manière centralisée. Ces lignes de base doivent être suffisamment souples pour s'appliquer lorsque les dispositifs IoT sont à la fois un produit et un service (c'*est-à-dire* lorsque les services en nuage font partie intégrante du fonctionnement du produit) et lorsque les capacités de sécurité sont réparties sur un système de dispositifs IoT.

Lors de l'élaboration de ces lignes de base, nous devons mettre en balance l'investissement dans les exigences de base et les coûts de la non-utilisation des lignes de base (c'*est-à-dire* les coûts pour les personnes potentiellement lésées, les coûts pour le fabricant du produit et les coûts pour les autres parties prenantes). Les lignes de base des capacités doivent être pragmatiques afin de garantir que les fabricants puissent répondre aux exigences de manière rentable, tout en offrant un avantage clair au client et à l'écosystème. Pour atteindre cet équilibre, ces lignes de base doivent être élaborées sous la direction de l'industrie, en collaboration avec le client visé (*par exemple,* un consortium représentant un secteur industriel, ou des groupes de défense des consommateurs et de la société civile représentant les utilisateurs domestiques) et avec la contribution et la participation actives des gouvernements, le cas échéant. La collaboration dans l'élaboration des lignes de base permet aux fabricants de disposer d'un temps d'avance et d'un aperçu précoce des attentes des clients, et augmente la probabilité que des produits conformes soient disponibles en temps voulu. La participation des clients à l'élaboration des lignes de base peut également indiquer au marché que les acheteurs préfèrent des dispositifs IdO conçus pour être sécurisés dans leurs environnements cibles et permettre l'alignement des activités d'éducation décrites ci-dessous. Les capacités spécifiées dans la ligne de base devenant la norme de facto, cela favorisera un marché durable pour des dispositifs plus sûrs.

[52] Les normes fondées sur les performances décrivent *ce qui* doit être réalisé, plutôt que la *manière d'*y parvenir, ce qui réduit ou élimine les impacts négatifs sur l'innovation.

Pour que les coûts d'opportunité d'innovation perdus n'écrasent pas la valeur de la base de référence, les bases de référence de la sécurité de l'IdO qui identifient un petit nombre de capacités de sécurité flexibles doivent imposer des contraintes minimales (le cas échéant) sur la conception et la mise en œuvre. [53] La spécification des capacités en termes de performance plutôt que de conception (c'*est-à-dire* une approche fondée sur les résultats plutôt que prescriptive) aidera à gérer les coûts associés aux programmes d'évaluation correspondants. La limitation de l'ensemble des fonctionnalités présente un avantage supplémentaire : il devient également plus pratique pour les plateformes de développement communes d'intégrer ces ensembles de fonctionnalités dans les composants de l'IdO, ce qui simplifie le développement de produits conformes.

Un fondement pour les futures bases de référence

Plusieurs spécifications ont été publiées récemment et offrent, au minimum, une base solide pour les futures lignes de base des capacités de sécurité de l'IdO. Ces efforts vont de spécifications de haut niveau à des documents extrêmement détaillés et ciblent un éventail d'environnements d'application. Parmi les exemples notables de spécifications de haut niveau axées sur les appareils de qualité grand public, toutes publiées depuis juin 2017, citons le cadre de sécurité IoT de l'Online Trust Alliance[54], la norme numérique (élaborée par une coalition comprenant Consumer Reports, Ranking Digital Rights et le Cyber Independent Testing Lab),[55] et *Secure by Design : Improving the cyber security of consumer Internet of Things56* du ministère britannique du numérique, de la culture, des médias et du sport. Un exemple de spécification de base détaillée est constitué par les *recommandations de sécurité de base pour l'IdO dans le contexte des infrastructures d'information* critiques[57], publiées en novembre 2017 par l'Agence de l'Union européenne pour la sécurité des réseaux et de l'information, qui identifie 83 mesures techniques et bonnes pratiques de sécurité applicables à la sécurité de l'IdO. Un autre exemple est le document "Security Tenets for Life Critical Embedded Systems", élaboré par un groupe de travail intersectoriel composé de membres de la base industrielle de la défense et du secteur des technologies de l'information. [58]

Action 1.2 Le gouvernement fédéral devrait s'appuyer, le cas échéant, sur les lignes de base de capacités développées par l'industrie pour établir des lignes de base de capacités pour les dispositifs IoT dans les environnements du gouvernement américain, afin de répondre aux exigences de sécurité fédérales, de promouvoir l'adoption de lignes de base dirigées par l'industrie et d'accélérer la normalisation internationale.

L'action 1.1 est axée sur le développement, sous la direction de l'industrie, de bases de référence de capacités pour les dispositifs IdO dans différents environnements de menace. Cette approche crée de multiples défis, allant du développement de multiples profils concurrents à l'absence de toute base de référence pour un environnement critique. En outre, lorsque les efforts menés par l'industrie sont axés sur le plan national, il peut être difficile de les faire accepter au niveau international. Le gouvernement fédéral peut accélérer la convergence là où il existe de multiples bases de référence, lancer de nouveaux efforts

[53] Par exemple, une ligne de base peut spécifier une exigence de gestion des correctifs sans surveillance sans préciser un modèle pull ou push, si les correctifs doivent être chiffrés ou le type exact de protection de l'intégrité appliqué au correctif.[54] *Voir* Online Trust Alliance, *Internet of Things*, https://otalliance.org/initiatives/internet-things (dernière visite le 4 avril 2018).

[55] The Digital Standard, *The Standard*, https://www.thedigitalstandard.org/the-standard (dernière visite le 4 avril 2018). [56] Département du numérique, de la culture, des médias et du sport, *Secure by Design : Improving the cyber security of consumer Internet of Things*, (7 mars 2018), *disponible sur* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_. pdf.

[57] Agence de l'Union européenne pour la sécurité des réseaux et de l'information, *Recommandations de sécurité de base pour l'Internet des objets dans le contexte des infrastructures d'information critiques*, (20 novembre 2017), *disponible à l'adresse* https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[58] Département de la sécurité intérieure des États-Unis, *Security Tenets for Life Critical Embedded Systems*, https://www.dhs.gov/publication/security-tenets-lces (dernière publication le 12 janvier 2017).

en établissant un projet de discussion lorsqu'il n'existe pas de base de référence, et encourager la normalisation internationale en établissant des bases de référence fédérales en matière d'IdO.

En établissant des bases de référence fédérales pour les capacités de sécurité de l'IdO en coordination avec l'industrie, la société civile et les partenaires internationaux, le gouvernement fédéral peut démontrer le caractère pratique et l'efficacité des capacités spécifiées, contribuer aux incitations du marché et établir une base pour des programmes d'évaluation pratiques (voir actions 5.1 et 5.2). Cette approche garantira également que les bases de référence du gouvernement fédéral reflèteront l'état de l'art et évolueront en fonction de l'évolution de l'industrie et du marché. Le National Institute of Standards and Technology (NIST) est chargé d'élaborer des normes et des lignes directrices en matière de sécurité des informations, y compris des exigences minimales pour les systèmes fédéraux. Le NIST devrait identifier les exigences de sécurité pour les dispositifs et systèmes IdO dans les environnements fédéraux. Lorsque des lignes de base consensuelles dirigées par l'industrie existent, le NIST devrait évaluer leur applicabilité aux exigences de sécurité fédérales et, le cas échéant, élaborer une norme fédérale par référence. Ces bases de référence des capacités fédérales seraient similaires (et suivraient la progression) aux bases de référence industrielles développées dans l'action 1.1. Si une base de référence appropriée n'est pas disponible, le NIST devrait rechercher des partenaires industriels pour le développement d'une base de référence pratique et d'un projet de discussion pour les efforts futurs de l'industrie.

Au fur et à mesure que l'efficacité de ces lignes de base est prouvée, le gouvernement et l'industrie des États-Unis devraient également s'engager conjointement avec les développeurs de normes et de spécifications internationales volontaires dirigées par l'industrie afin d'établir des normes pertinentes à l'échelle mondiale. Au fur et à mesure de l'émergence de ces normes et spécifications, des lignes de base fédérales devraient être créées, mises à jour ou remplacées, le cas échéant.

Le lieu de normalisation de ces lignes de base doit être choisi avec soin. Les lignes de base en matière de sécurité et toutes les normes et spécifications connexes doivent être élaborées par des organismes du secteur privé ouverts à la participation de toutes les parties intéressées. Elles doivent être élaborées de manière transparente, en utilisant des processus équilibrés fondés sur le consensus et en adoptant, dans la mesure du possible, une approche fondée sur les résultats plutôt que sur les exigences. Ces normes fondées sur les performances sont les mieux adaptées pour relever les défis posés par un espace technologique en évolution rapide, tel que l'IdO. Ces processus n'excluent pas la participation du gouvernement, mais garantissent que les intérêts du gouvernement, de l'industrie, de la société civile et des utilisateurs sont tous bien représentés, et que les solutions qui en résultent reflètent l'état de l'art dans cet espace technologique.
La flexibilité de ces processus permet également de mettre à jour les normes à mesure que la technologie, les menaces et les solutions évoluent. La forte concordance entre l'utilisation par les entreprises des normes qu'elles ont contribué à élaborer et le soutien des gouvernements au développement de ces outils facilite l'adoption de ces normes à grande échelle.

Il est important de reconnaître que, compte tenu de l'ampleur de l'espace technologique, aucun organisme de développement de normes ou de spécifications ne peut à lui seul développer toutes les solutions. Les gouvernements du monde entier doivent soutenir la coopération et la coordination entre les organismes de normalisation et de spécification qui disposent de l'expertise et de l'expérience nécessaires et qui développent des produits selon les principes évoqués ci-dessus, afin de garantir des solutions solides, opportunes et adaptées. Aux États-Unis, le NIST devrait continuer à diriger et à coordonner l'engagement des agences fédérales dans les activités de normalisation connexes, y compris l'engagement avec le secteur privé, en explorant une stratégie du gouvernement fédéral à l'appui des normes internationales pour relever les défis des botnets et autres menaces automatisées et distribuées.

Des actions complémentaires de la part du gouvernement américain et du secteur privé pourraient renforcer considérablement les effets de ces bases de référence fédérales en matière de capacités IoT. Le gouvernement fédéral peut utiliser les règles d'acquisition et les directives de passation de marchés pour amplifier le signal du marché en exigeant les capacités de la ou des lignes de base (cf.

Action 2.3) et, le cas échéant, préférer les produits qui sont également conformes à un système d'étiquetage donné du secteur privé (voir actions 5.1 et 5.2).

Action 1.3 L'industrie doit adopter plus largement des outils et des processus de développement de logiciels permettant de réduire considérablement l'incidence des failles de sécurité dans les logiciels commerciaux. Le gouvernement fédéral devrait collaborer avec l'industrie pour encourager l'amélioration et l'application de ces pratiques et pour améliorer l'adoption et la responsabilité du marché.

Les techniques courantes de développement de logiciels produisent des logiciels comportant au moins un bogue pour 2 000 lignes de code[59], et les systèmes modernes comprennent des dizaines de millions de lignes de code. Cela implique des dizaines de milliers de bogues dans un système, dont beaucoup créent des failles de sécurité. Les mécanismes de mise à jour sécurisée (notés comme une caractéristique de base importante dans l'action 1.1) permettent aux fournisseurs de corriger ces erreurs après une période de vulnérabilité relativement brève. Cependant, éviter complètement ces vulnérabilités aurait un impact encore plus important en termes de réduction du risque de sécurité. S'il est possible de développer un code comportant un très petit nombre d'erreurs, lorsque l'importance de la mission mérite une réduction significative de la productivité, le défi consiste à développer des mécanismes qui produisent un code nettement meilleur sans réduire indûment la productivité.

Un groupe de travail interagences (documenté dans le rapport NIST Interagency/Internal Report [NISTIR] 815160) a identifié de nombreuses approches pour développer des logiciels présentant moins de vulnérabilités, en mettant en œuvre trois stratégies de base :

- Arrêter les vulnérabilités avant qu'elles ne se produisent, notamment en améliorant les méthodes de spécification et de construction des logiciels ;
- la découverte de vulnérabilités, notamment par l'amélioration des techniques de test et l'utilisation plus efficace de méthodes de test multiples
- Réduire l'impact des vulnérabilités en construisant des architectures plus résilientes, de sorte que les vulnérabilités ne puissent pas être exploitées de manière significative.

Des outils pour soutenir ces approches sont maintenant disponibles[61] et ont été adoptés par quelques entreprises avant-gardistes62. Les développeurs de logiciels devraient commencer à adopter ces outils immédiatement, en se concentrant d'abord sur les produits qui présentent le plus de risques. Le DHS et la FTC offrent également des ressources aux petits développeurs de logiciels. [63]

[59] *Voir Coverity Scan, supra* note 34, à la page 4.
[60] Paul E. Black, Lee Badger, Barbara Guttman et Elizabeth Fong, Dramatically *Reducing Software Vulnerabilities : Report to the White House Office of Science and Technology Policy*, (Nov. 2016), NIST Interagency/Internal Report No. 8151, *disponible sur* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf.
[61] *Voir, par exemple*, *CWE/SANS Top 25 Most Dangerous Software Errors*, SANS Institute, https://www.sans.org/top25- software-errors/ (dernière mise à jour le 27 juin 2011).
[62] Par exemple, le Software Assurance Marketplace (SWAMP) vise à faciliter le test systématique de la qualité et de la sécurité de ces applications et à apporter un changement transformateur au paysage de l'assurance logicielle en réduisant le nombre de faiblesses déployées dans les logiciels. Pour plus d'informations, voir Software Assurance Marketplace, https://continuousassurance.org/ (dernière visite le 4 avril 2018).
[63] Le DHS a soutenu le développement du SWAMP, qui propose à la fois des outils d'assurance logicielle basés sur le cloud et des outils open source. Pour plus d'informations, voir Software Assurance Marketplace, *About Swamp*, https://continuousassurance.org/about-us/ (dernière visite le 4 avril 2018) ; Federal Trade Commission, *Careful Connections : Building Security in the Internet of Things*, (janvier 2015),

Le gouvernement fédéral devrait soutenir l'adoption de ces outils par l'industrie en améliorant le retour sur investissement ou en créant des incitations commerciales pour les secteurs ou les groupes industriels en retard, comme le NSTAC l'a également recommandé dans son rapport. Le gouvernement fédéral devrait promouvoir le développement d'outils pour des pratiques de codage sécurisées en parrainant ou en effectuant des recherches ciblées (voir Action 1.4), et en parrainant des concours pour des chaînes d'outils sécurisées (processus multi-outils pour le développement de logiciels) afin de démontrer leur efficacité et leur productivité. Le gouvernement fédéral devrait également collaborer avec l'industrie et la société civile pour élaborer des stratégies qui rendent l'adoption de ces approches plus facile et moins coûteuse - y compris l'éducation et la formation abordées en détail ci-dessous - en gardant à l'esprit les exigences des petites entreprises, et travailler avec l'ensemble des parties prenantes pour rendre ce processus observable et vérifiable par des tiers.

À titre d'exemple, les produits modernes utilisent de nombreux composants logiciels, bibliothèques et modules, dont certains peuvent être obsolètes ou vulnérables et ne sont pas toujours suivis de près par les fabricants dans le cadre du cycle de développement rapide. Si la notion de transparence autour des composants logiciels n'est pas nouvelle, elle n'a pas été largement soutenue et adoptée. La NTIA devrait engager diverses parties prenantes dans l'examen des stratégies et des politiques nécessaires pour favoriser un marché pour une plus grande transparence des composants logiciels, y compris l'identification et l'exploration du marché et d'autres obstacles qui peuvent entraver les progrès dans ce domaine. Savoir quels logiciels ont été intégrés dans un produit est une étape fondamentale pour pouvoir le maintenir à jour et atténuer les menaces lorsqu'elles se présentent.

Action 1.4 L'industrie devrait accélérer le développement et le déploiement de technologies innovantes pour la prévention et l'atténuation des menaces distribuées. En conséquence, le cas échéant, les pouvoirs publics devraient accorder la priorité à l'utilisation des fonds de recherche et de développement et aux efforts de transition technologique pour soutenir les progrès en matière de prévention et d'atténuation des DDoS, ainsi que les technologies de base pour empêcher la création de botnets. Le cas échéant, la société civile devrait amplifier ces efforts.

La croissance rapide de la capacité DDoS offerte par les botnets basés sur l'IoT met en péril l'efficacité des techniques actuelles d'atténuation des DDoS. La recherche et le développement de techniques d'atténuation plus proches de la source ou exploitant de nouvelles analyses de données, l'apprentissage automatique ou l'intelligence artificielle (IA) sont nécessaires de toute urgence pour devancer les acteurs malveillants. Des innovations seront nécessaires pour lutter contre d'autres activités malveillantes soutenues par les botnets, telles que les ransomwares et la propagande informatique. Des technologies de base permettant de prévenir, de détecter et de récupérer la compromission et l'incorporation dans un botnet seront nécessaires pour faire face à ces attaques et à celles à venir.

Pour renforcer la résilience de l'écosystème, il faut capitaliser sur les succès de la recherche et du développement par un déploiement agressif. Les technologies innovantes en matière de dispositifs, telles que les racines de confiance matérielles ou les mécanismes améliorés d'authentification des dispositifs, offrent la possibilité de renforcer considérablement la sécurité tout au long du cycle de vie des produits. Les progrès des outils de réseau, tels que la description de l'utilisation par le fabricant (MUD), une norme actuellement en cours de développement au sein de l'[IETF64], pourraient améliorer la résilience du réseau en gérant les communications pour la sécurité et en rendant la gestion granulaire du réseau plus efficace.

https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections- buildingsecurityinternetofthings.pdf.

[64] *Voir* E. Lear, R. Droms & D. Romascanu, *Manufacturer Usage Description Specification (*Draft), Internet Engineering Task Force - Network Working Group, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ (dernière mise à jour le 19 avril 2018).

moins cher et plus facile. L'adoption accélérée de ces technologies innovantes améliorerait la résilience de l'écosystème, mais la commercialisation et l'adoption de résultats de recherche prometteurs pour créer des produits viables ou des services commercialisables sont notoirement difficiles. La société civile et les groupes à but non lucratif peuvent également amplifier les nouvelles plates-formes ou solutions, comme l'ont fait l'Internet Society et la Global Cyber Alliance pour leurs initiatives respectives de promotion de la sécurité du routage[65,66] et l'American Civil Liberties Union pour son initiative sur la vie privée et la technologie[67]. [67]

En tant que source essentielle de financement de la recherche fondamentale en matière de cybersécurité, le gouvernement fédéral devrait soutenir cette action par un financement ciblé et des activités de transition technologique en collaboration. Les ministères et les agences parrainent également la recherche appliquée à l'appui des exigences de la mission et une variété d'activités de transition technologique. [68] Les agences devraient donner la priorité au développement et au déploiement d'innovations qui augmenteraient la résilience de l'écosystème et coordonner ces investissements par le biais du programme Networking and Information Technology Research and Development (NITRD). [69] Comme pour l'utilisation de toute technique d'atténuation, des mesures doivent être prises pour s'assurer que ces technologies innovantes n'exposent pas les consommateurs à des risques inutiles pour la vie privée. Pour ce faire, on peut utiliser les outils d'évaluation des risques pour la vie privée décrits dans la norme NISTIR 806270 ou procéder à une évaluation des incidences sur la vie privée[71]. [71]

Action 1.5 Les pouvoirs publics, les entreprises et la société civile devraient collaborer pour faire en sorte que les meilleures pratiques, les cadres et les lignes directrices existants en matière d'IdO, ainsi que les procédures visant à garantir la transparence, soient plus largement adoptés dans l'ensemble de l'écosystème numérique. Les risques émergents dans l'espace IoT doivent être abordés de manière ouverte et inclusive.

Plusieurs initiatives antérieures ont donné lieu à des orientations et à des meilleures pratiques concernant les botnets et l'amélioration de la sécurité de l'IdO, mais les botnets restent un problème. Par exemple, les parties prenantes du processus multilatéral de la NTIA sur la mise à niveau et le correctif de la sécurité de l'IdO ont élaboré un ensemble de documents proposant des solutions à la fois pour l'offre et la demande du marché des consommateurs de l'IdO, mais les parties prenantes ont également souligné le rôle partagé dans la promotion de ces idées au sein de la communauté IdO. La publication de documents ne suffit pas : nous devons veiller à ce qu'ils soient largement adoptés par l'écosystème. La communauté de l'IdO doit travailler en collaboration pour identifier et adopter les meilleures pratiques, les cadres et les lignes directrices existants qui sont

[65] *Voir* Internet Society, *MANRS : Mutually Agreed Norms for Routing Security*, https://www.internetsociety.org/issues/manrs/ (dernière visite le 4 avril 2018).
[66] *Voir* Global Cyber Alliance, *Quad9 : quatre étapes simples vers la sécurité, la confidentialité et la performance*, https://www.globalcyberalliance.org/initiatives/quad9.html (dernière visite le 4 avril 2018).
[67] *Voir* ACLU, *Privacy & Technology,* https://www.aclu.org/issues/privacy-technology (dernière visite le 4 avril 2018).
[68] Le projet Distributed Denial of Service Defense du DHS est un exemple de ces recherches. *Voir le* ministère américain de la Sécurité intérieure, *Distributed Denial of Service Defense*, https://www.dhs.gov/science-and-technology/csd-ddosd (dernière visite le 4 avril 2018). *Voir également* National Science Foundation, *Secure and Trustworthy Cyberspace (SaTC)*, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709 (dernière visite le 4 avril 2018).
[69] Le programme de recherche et développement sur les réseaux et les technologies de l'information, https://www.nitrd.gov/ (dernière visite le 4 avril 2018).
[70] Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman et Ellen Nadeau, An *Introduction to Privacy Engineering and Risk Management in Federal Systems, (*janv. 2017), NIST Interagency/Internal Report n° 8062, *disponible sur* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[71] Pour plus d'informations sur un type d'évaluation des incidences sur la vie privée, voir U.S. Department of Homeland Security, *Privacy Impact Assessment Guidance*, https://www.dhs.gov/publication/privacy-impact-assessment-guidance (dernière publication le 13 avril 2018).
[72] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (dernière mise à jour le 7 novembre 2017).

pertinents pour l'IdO. La communauté de l'IdO devrait également s'efforcer de faire connaître ces meilleures pratiques, cadres et directives. Le rapport du NSTAC fait également état de ce besoin, en lien avec sa recommandation selon laquelle l'industrie devrait travailler avec le DHS et le Commerce pour accélérer l'adoption de directives de sécurité.

Le gouvernement fédéral devrait soutenir l'adoption généralisée des meilleures pratiques en engageant la communauté à déterminer pourquoi les recommandations antérieures n'ont pas été largement mises en œuvre ou ont échoué, à identifier les voies appropriées pour favoriser une mise en œuvre réussie et à se concentrer sur des outils et des leviers pratiques et éprouvés. Par exemple, les pratiques de développement actuelles mettent l'accent sur la réutilisation des logiciels libres et commerciaux, qui peuvent être obsolètes ou vulnérables, mais ces attributs de l'(in)sécurité sont cachés aux développeurs et aux clients. Le processus multipartite de la NTIA sur la transparence des composants logiciels (voir l'action 1.3) peut explorer les moyens d'accroître les garanties qu'aucune vulnérabilité connue n'est livrée avec les produits.

Un problème particulièrement contrariant qui nécessitera la contribution des parties prenantes est la question du code hérité et orphelin, ou "logiciel mort". Les parties prenantes au processus multipartite de la NTIA sur les correctifs ont identifié l'importance de communiquer la période pendant laquelle les mises à jour de sécurité seraient fournies, mais n'ont pas offert d'orientation explicite sur ce qui se passerait lorsque les mises à jour de sécurité ne seraient plus offertes. [73] Comme les biens durables ayant une longue durée de vie sont de plus en plus liés à un code fragile, ce problème va s'amplifier. Un expert en sécurité est même allé jusqu'à préconiser que les logiciels abandonnés soient rendus open source. [74] L'accès au code n'est cependant qu'un obstacle. Les mises à jour doivent encore être écrites et testées. Les fournisseurs en faillite présentent des défis supplémentaires si les certificats de signature ou les fichiers MUD (voir Action 1.4) sont liés aux domaines. L'initiative Core Infrastructure propose un modèle pour traiter les externalités des logiciels insuffisamment pris en charge[75], mais la perspective de faire face systématiquement aux systèmes non maintenus distribués dans le monde entier nécessitera la contribution d'un large éventail de parties prenantes.

Des pratiques transparentes et vérifiables de gestion des actifs logiciels (SAM) peuvent aider les entreprises à identifier les logiciels qui ne peuvent pas être corrigés parce que les mises à jour ne sont plus disponibles ou que les licences ont expiré. Une fois identifiées, les entreprises peuvent remédier à ces vulnérabilités en remplaçant les produits ou en réorganisant les réseaux pour gérer les risques. Les entreprises et les acteurs gouvernementaux devraient adopter des pratiques SAM fondées sur les normes internationales en matière d'approvisionnement et de gestion des actifs, ainsi que des procédures pour atténuer les risques identifiés grâce à ces pratiques.

Des efforts complémentaires visant à sensibiliser et à éduquer les développeurs et les fabricants de produits pourraient renforcer considérablement l'impact de ces meilleures pratiques, cadres et lignes directrices, comme décrit dans les actions 5.3, 5.4 et 5.5.

[73] Le rapport de la FTC sur les mises à jour de sécurité mobile recommande aux entreprises d'envisager la divulgation de la période d'assistance minimale et les notifications avant la fin de la période d'assistance de sécurité. Commission fédérale du commerce, *Mobile Security Updates : Understanding the Issues*, (fév. 2018), https://www.ftc.gov/system/files/documents/reports/mobile- security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf . [74] Dan Geer, discours liminaire à Black Hat USA 2014 : *Cybersecurity as Realpolitik*, (6 août 2014), *disponible à l'adresse* http://geer.tinho.net/geer.blackhat.6viii14.txt (ébauche de livraison nominale). Vidéo disponible à l'adresse : https://www.blackhat.com/us-14/video/cybersecurity-as-realpolitik.html.

[75] Initiative pour une infrastructure de base, https://www.coreinfrastructure.org/ (dernière visite le 4 avril 2018).

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Objectif 2 : promouvoir l'innovation dans l'infrastructure pour une adaptation dynamique à l'évolution des menaces.

Afin d'établir un écosystème Internet et de communication plus résilient, les normes et pratiques qui dissuadent, préviennent et/ou atténuent les réseaux de zombies et les menaces distribuées doivent être continuellement mises en œuvre et améliorées dans tous les domaines de l'écosystème en réponse et en anticipation de l'évolution de la menace. Cette section identifie les actions à la disposition des parties prenantes pour soutenir le développement d'une infrastructure efficace et dynamique.

Action 2.1 Les fournisseurs de services Internet et leurs partenaires d'échange de trafic[76] devraient étendre le partage d'informations actuel afin de parvenir à un partage plus rapide et plus efficace des informations sur les menaces exploitables, tant au niveau national que mondial.

Une fois établis, les botnets sont revendus ou loués à plusieurs clients et redirigés pour attaquer de nouvelles cibles. Cela signifie que de nombreux FAI et leurs partenaires d'échange de trafic seront confrontés à des attaques similaires au fil du temps. Lorsqu'un FAI est confronté pour la première fois à une menace particulière, il doit analyser les comportements anormaux et élaborer des méthodes d'atténuation. Les botnets sont généralement répartis entre de nombreux FAI, chacun d'entre eux pouvant contribuer aux activités d'atténuation si les connaissances sont suffisantes. Le partage des techniques de gestion de réseau et des tactiques défensives efficaces contre des menaces particulières est un autre moyen pour les grands fournisseurs de réseaux d'augmenter la valeur préventive des informations partagées.

Les accords actuels de partage d'informations entre les FAI et leurs partenaires d'échange de trafic sont très efficaces dans leur domaine. En partageant les informations sur les menaces connues, en cours et émergentes, les FAI sont en mesure de réagir plus efficacement. Cependant, les accords actuels de partage d'informations sont souvent motivés par des relations personnelles et ne sont pas complets, en particulier lorsqu'il s'agit de menaces plus nuancées ou plus sensibles. L'évolution du paysage des réseaux et l'évolution de la portée, de l'échelle, de l'orientation et de la diversité des acteurs des réseaux ont également un impact sur l'efficacité des relations de partage. La collaboration entre les FAI et leurs partenaires d'échange de trafic doit être formalisée et inclure le partage de la détection, de la notification et des méthodes d'atténuation prévues ou utilisées au sein du réseau. Lorsque le partage est entravé par des préoccupations d'ordre commercial, les FAI doivent chercher des moyens d'aborder les dispositions de partage et la coordination des réponses dans leurs accords d'échange de trafic et de transit.

L'industrie devrait diriger les efforts visant à étendre la portée et l'utilité du partage d'informations entre les FAI et leurs partenaires d'échange de trafic et à combler les lacunes dans l'opérationnalisation des informations partagées. En particulier, l'industrie doit travailler en collaboration avec la société civile et le gouvernement pour améliorer les réponses coordonnées aux informations exploitables et diriger le développement, le perfectionnement et la normalisation des protocoles de partage d'informations afin d'augmenter la vitesse et de permettre une réponse automatisée. Une attention particulière doit être accordée à l'engagement et à l'inclusion des petits fournisseurs de services Internet et aux développements de protocoles qui améliorent leur participation.

Bien que l'industrie joue un rôle de premier plan, le gouvernement fédéral peut faciliter cette activité à l'échelle nationale par l'entremise du Centre d'analyse et de partage de l'information sur les communications (ISAC) (c*.-à-d.* le Centre national de coordination des communications [NCC]), en forgeant des partenariats avec les groupes d'exploitants de réseaux (NOG), à l'échelle internationale par un engagement continu dans le Forum of Incident Response and Security Teams (FIRST), et en élargissant les accords de partage de l'information avec des pairs internationaux comme Telecom ISAC Japan. Le gouvernement peut jouer un rôle important dans ces discussions, en convoquant

[76] Cela inclut les entreprises qui exploitent leurs propres routeurs BGP et serveurs DNS.

des réunions multipartites si nécessaire, en fournissant une vue d'ensemble et en veillant à ce que le processus soit équitable pour toutes les parties prenantes. Les équipes nationales de réponse aux incidents de sécurité informatique (CSIRT) peuvent également assurer une coordination directe et catalyser la réponse des gestionnaires de ressources et des acteurs de l'infrastructure au niveau local.

Action 2.2 Les parties prenantes et les experts en la matière, en consultation avec le NIST, devraient diriger l'élaboration d'un profil CSF pour la prévention et l'atténuation des attaques DDoS en entreprise.

Les entreprises sensibilisées aux attaques DDoS qui souhaitent atténuer l'impact de futures attaques DDoS et réduire la probabilité que des ressources internes soient incorporées dans des botnets pour attaquer d'autres entreprises constatent que des directives complètes ne sont pas facilement disponibles. Les grandes entreprises sont obligées de consacrer d'importantes ressources en personnel à l'identification et à l'acquisition ou au déploiement de mécanismes appropriés. Les petites entreprises manquent souvent d'expertise ou ne peuvent se permettre de consacrer ces ressources à l'élaboration d'une stratégie anti-DDoS. Les solutions globales sont complexes et nécessitent souvent une combinaison de services commerciaux externes et gérés localement. Il est donc essentiel de communiquer les besoins aux fournisseurs.

Le Cadre pour l'amélioration de la cybersécurité des infrastructures critiques (connu sous le nom de CSF) version 1.0 a été développé par le NIST avec une contribution importante du secteur privé, tout comme la version 1.1, publiée en avril 2018. Le CSF fournit une approche flexible de la gestion du risque de cybersécurité qui intègre les normes et les meilleures pratiques de l'industrie, est suffisamment général pour permettre une large applicabilité dans une variété d'environnements - y compris l'IdO - et a été largement accepté par l'industrie. Le CSF peut être complété par des profils de cadre, qui appliquent les composantes du cadre à une situation spécifique. En particulier, les secteurs industriels peuvent utiliser des profils pour documenter les meilleures pratiques de protection contre des menaces spécifiques. Le CSF est conçu pour évoluer au fil du temps, à mesure que l'environnement de la cybersécurité change.

Les entreprises qui souhaitent améliorer la résilience de leurs propres réseaux contre les attaques DDoS et se protéger contre les botnets qui incorporent leurs ressources bénéficieraient grandement de la disponibilité d'un profil CSF[77] pour la prévention et l'atténuation des attaques DDoS en entreprise. Un effort mené par l'industrie, en consultation avec le NIST, le monde universitaire et d'autres experts en la matière, devrait développer un profil CSF pour la prévention et l'atténuation des attaques DDoS en entreprise, en se concentrant sur l'état souhaité de la cybersécurité organisationnelle pour atténuer les attaques DDoS. Le profil CSF fournirait des conseils aux entreprises et établirait un langage commun pour les discussions concernant les mécanismes de protection contre les attaques DDoS avec les fournisseurs de produits, les FAI et les autres fournisseurs d'infrastructure. Le profil aiderait les entreprises à identifier les possibilités d'améliorer l'atténuation des menaces DDoS et contribuerait à la hiérarchisation des priorités en matière de cybersécurité en comparant leur état actuel avec l'état cible souhaité. Le profil comprendrait probablement plusieurs niveaux pour soutenir les secteurs industriels ayant des exigences de résilience différentes.

Le champ d'application du profil CSF devrait inclure, au minimum, les mécanismes d'atténuation des attaques DDoS sur site et hors site, les fonctions de sécurité du routage (par *exemple, le* filtrage à l'entrée de la meilleure pratique actuelle [BCP] 38/84) et les conseils sur la fermeture des vecteurs de réflexion. Pour une applicabilité maximale, le profil doit être rédigé de manière à couvrir à la fois les grandes entreprises, qui peuvent exploiter les éléments clés de leurs stratégies d'atténuation des attaques DDoS, et les petites entreprises, qui dépendent souvent entièrement des fournisseurs de services.

[77] Les profils CSF sont des compilations de conseils et de meilleures pratiques autour de menaces particulières qui suivent le modèle CSF bien établi.

[78] La Coalition for Cybersecurity Policy & Law (Cybersecurity Coalition) a lancé un effort prometteur, actuellement sous forme de projet. *Voir* Cybersecurity Coalition, *Threat Profile for DDoS Attacks Using NIST Framework*, https://www.cybersecuritycoalition.org/threat-profile-ddos-nist-framework (28 juillet 2017).

Les parties prenantes du gouvernement devraient participer à l'élaboration de ce profil afin de s'assurer qu'il est assez largement applicable pour servir de profil CSF pour la prévention et l'atténuation des DDoS au niveau fédéral. Pour créer des incitations commerciales, cette action devrait être soutenue par une adoption agressive dans l'ensemble du gouvernement fédéral, comme spécifié dans l'action 2.3, soit par l'application directe du profil, soit par l'application des contrôles correspondants en utilisant le processus existant de la loi fédérale sur la modernisation de la sécurité de l'information.

Action 2.3 Le gouvernement fédéral devrait donner l'exemple et démontrer l'aspect pratique des technologies, en créant des incitations commerciales pour les premiers adoptants.

Après la publication des lignes de base pour la sécurité des dispositifs IoT (action 1.1), le gouvernement fédéral devrait établir des lignes directrices pour l'approvisionnement afin de fournir des incitations commerciales aux premiers utilisateurs. De nombreux fournisseurs de produits IoT ont formulé des plans pour améliorer la sécurité de leurs produits, mais les observateurs s'inquiètent du fait que les incitations du marché sont fortement axées sur le coût et le délai de mise sur le marché. S'il n'est pas prouvé que les clients absorberont les coûts supplémentaires liés au développement de produits plus sécurisés, l'industrie pourrait être incitée à une course vers le bas. Bien que les marchés publics fédéraux ne dominent plus le marché, leur pouvoir d'achat et leur influence sont encore forts, et le gouvernement américain peut montrer l'exemple. En élaborant des lignes directrices pour les marchés publics fédéraux fondées sur les bases de sécurité des dispositifs IdO, le gouvernement américain peut mettre en place des incitations commerciales pour les premiers utilisateurs. L'Office of Management and Budget, la General Services Administration (GSA) et le ministère de la Défense peuvent faciliter ces exigences d'approvisionnement par le biais de politiques et de modifications du calendrier de la GSA et des règlements d'acquisition fédéraux. [79]

Dès la publication d'un profil CSF approprié (action 2.2), le gouvernement fédéral devrait mettre en œuvre des mesures de prévention et d'atténuation DDoS de base pour tous les réseaux fédéraux afin de renforcer la résilience de l'écosystème et de démontrer le caractère pratique et l'efficacité du profil. Par le passé, des pirates ont exploité des réseaux fédéraux dans des attaques DDoS en utilisant des résolveurs ouverts et d'autres ressources d'agences pour amplifier leurs attaques. Le gouvernement fédéral doit montrer l'exemple, en veillant à ce que les ressources fédérales ne soient pas des participants involontaires et que les réseaux fédéraux soient préparés à détecter, atténuer et répondre si nécessaire. L'administration devrait rendre obligatoire la mise en œuvre du profil CSF fédéral pour la prévention et l'atténuation des attaques DDoS par toutes les agences gouvernementales dans un délai déterminé après l'achèvement et la publication du profil.

Le gouvernement fédéral devrait évaluer et mettre en œuvre des moyens efficaces pour inciter à l'utilisation d'outils et de processus de développement de logiciels qui réduisent considérablement l'incidence des vulnérabilités de sécurité dans tous les achats de logiciels fédéraux, par exemple par des exigences d'attestation ou de certification. Afin d'inciter le marché à développer des logiciels sécurisés, le gouvernement fédéral devrait établir des règles d'achat qui favorisent ou exigent des logiciels commerciaux développés à l'aide de tels processus, lorsqu'ils sont disponibles. Le gouvernement fédéral devrait également s'assurer que les projets de développement de logiciels financés par le gouvernement utilisent les meilleurs outils disponibles pour obtenir un aperçu de l'impact de ces réglementations.

[79] Le groupe de travail sur la sécurité de l'IdO du Conseil de coordination des technologies de l'information (Information Technology Coordinating Council), dirigé par le DHS, rédige actuellement des conseils à l'intention des responsables des achats sur les questions à poser à leurs clients, à leurs équipes informatiques et de sécurité, ainsi qu'aux fournisseurs, afin de s'assurer qu'un appareil connecté acheté s'inscrit dans la posture de gestion des risques de l'agence. Ces conseils viendront compléter, mais ne seront pas identiques, aux directives de conformité élaborées en fonction des bases de sécurité.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Action 2.4 L'industrie, les pouvoirs publics et la société civile doivent collaborer avec l'ensemble des parties prenantes pour continuer à améliorer et à normaliser les protocoles de partage des informations.

Pour faire face aux menaces automatisées et distribuées, les parties prenantes doivent partager des informations solides en temps quasi réel. Le rapport du NSTAC indique que la collaboration entre les secteurs public et privé est essentielle pour atténuer les réseaux de zombies. Les protocoles de partage d'informations actuellement utilisés ont été mis au point par le gouvernement fédéral, avec la participation active d'un large éventail de parties prenantes, mais ils ne répondent pas nécessairement aux besoins de toutes les parties prenantes.

Par exemple, les petites entreprises sont sous-représentées ; elles ne contribuent pas à la plupart des accords actuels de partage d'informations et n'en bénéficient pas. Pour répondre aux besoins des petites entreprises, qui ne disposent généralement pas d'une équipe interne solide en matière de cybersécurité, les protocoles devront peut-être permettre une action automatisée. Par exemple, les fournisseurs d'accès à Internet peuvent souvent identifier le réseau client associé à un dispositif compromis, mais n'ont pas la visibilité nécessaire pour identifier des dispositifs spécifiques. Les petites entreprises peuvent ne pas être en mesure d'identifier ces appareils si elles sont contactées par leur FAI. Des protocoles de partage d'informations permettant aux FAI de partager des informations sur les dispositifs compromis détectés avec les routeurs des petites entreprises pourraient permettre une identification automatisée et un contrôle plus solide des clients sur leurs dispositifs en réseau. Les clients pourraient également choisir de partager les résultats de toute mesure d'atténuation avec leurs FAI, de la même manière qu'ils partagent les informations sur les défaillances logicielles avec les fournisseurs.

Pour répondre aux besoins de coordination et de collaboration d'une infrastructure hautement résiliente, ces protocoles de partage de l'information doivent avoir une portée globale, être accessibles à un large éventail d'entreprises et être suffisamment précis pour permettre un traitement et une réponse automatisés. Pour garantir l'atteinte de ces objectifs, l'industrie devrait diriger les efforts, en collaboration avec le gouvernement fédéral et d'autres parties prenantes, afin d'améliorer les protocoles de partage de l'information pour répondre aux besoins des parties prenantes et établir des normes internationales pour faciliter la coordination mondiale.

Action 2.5 Le gouvernement fédéral devrait collaborer avec les fournisseurs d'infrastructures américains et mondiaux pour étendre les meilleures pratiques en matière de gestion du trafic réseau à l'ensemble de l'écosystème.

Si l'on ne peut attendre des fournisseurs de réseaux qu'ils jouent le rôle de gendarmes du trafic et identifient tous les mauvais paquets, les outils et les pratiques, tant courants que nouveaux, peuvent contribuer à filtrer certains types de mauvais trafic. De nombreux acteurs du marché utilisent soit des signaux de réputation informels, soit des accords d'échange de trafic et de transit plus formels pour gérer le trafic. Une large coalition d'experts nationaux et internationaux, issus de l'industrie, du monde universitaire, de la société civile et des pouvoirs publics, devrait examiner dans quelle mesure les accords d'échange de trafic et de transit entre systèmes autonomes et réseaux Internet pourraient améliorer la responsabilité en matière de gestion du trafic, par exemple en ce qui concerne la lutte contre l'usurpation d'identité et le filtrage. La communauté des universitaires et des ingénieurs devrait étudier comment les nouveaux outils et pratiques en cours de développement pourraient également être intégrés et mis en œuvre. L'industrie, le monde universitaire, la société civile et le gouvernement fédéral devraient s'appuyer sur ces résultats pour étendre les politiques constructives et les meilleures pratiques en matière de gestion du trafic réseau à l'ensemble de l'écosystème, en tenant compte des exigences des petites entreprises. Les outils et cadres existants, tels que le code de conduite anti-bots des États-Unis pour les fournisseurs d'accès Internet et les normes volontaires Mutually Agreed Norms for Routing Security (MANRS), devraient être révisés, et de nouvelles solutions devraient être explorées dans le cadre d'un processus multipartite incluant une représentation diversifiée des acteurs du réseau qui correspondent à l'environnement de l'écosystème actuel.

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Objectif 3 : promouvoir l'innovation à la périphérie du réseau pour prévenir, détecter et atténuer les attaques automatisées et distribuées.

Pour établir un écosystème Internet et de communication résilient, les services d'infrastructure conçus pour se protéger contre les attaques devraient être complétés par une détection et une atténuation accrues des dispositifs compromis dans les réseaux domestiques ou d'entreprise, et là où ces réseaux se connectent à l'Internet. Une meilleure connaissance du contexte local peut améliorer la détection, et il peut être plus facile de se contenter de déconnecter ou de mettre en place un pare-feu pour certains appareils ou services au comportement anormal. Cette section identifie les actions que les parties prenantes peuvent entreprendre pour gérer l'impact des dispositifs compromis utilisés dans les attaques automatisées et distribuées.

Action 3.1 L'industrie des réseaux devrait étendre les efforts actuels de développement et de normalisation des produits pour une gestion efficace et sûre du trafic dans les environnements domestiques et d'entreprise.

L'industrie des réseaux cherche à mettre en place divers mécanismes propriétaires ou basés sur des normes pour mieux gérer le trafic au sein des réseaux d'entreprise. Ces mécanismes visent à empêcher les communications avec des systèmes suspects ou à limiter les communications aux hôtes spécifiquement requis pour un fonctionnement correct.
Ces systèmes peuvent tirer parti de l'IA ou de l'apprentissage automatique, des méthodes de détection et d'atténuation des menaces fournies par des services commerciaux externes, ou des informations spécifiques aux appareils. L'industrie devrait étendre ces efforts pour accélérer la fourniture d'une sécurité réseau efficace et rentable pour les environnements domestiques et professionnels.

Les concentrateurs et les passerelles du réseau local80 peuvent jouer le rôle de gestionnaires de trafic, en identifiant et en empêchant le trafic malveillant d'accéder aux dispositifs IoT et en limitant le trafic nuisible émanant des dispositifs du réseau local. Les fournisseurs de services en nuage développent également des solutions qui pourraient être superposées à ces solutions axées sur les passerelles, ce qui pourrait fournir de multiples contrôles et équilibres dans la pile du réseau pour mieux sécuriser l'écosystème IdO. Au fur et à mesure de l'émergence de ces innovations en matière de sécurité, le gouvernement et les parties prenantes devraient s'associer pour sensibiliser les consommateurs, les petites et moyennes entreprises et les partenaires internationaux aux solutions de sécurité. Lorsqu'il existe des obstacles spécifiques à l'adoption ou à l'avancement, le gouvernement et les parties prenantes doivent se réunir pour identifier les obstacles, promouvoir le déploiement des normes émergentes et examiner les politiques de pare-feu pratiques pour l'espace produit plus large.

Action 3.2 Les produits informatiques et IoT domestiques devraient être faciles à comprendre et simples à utiliser en toute sécurité.

Les produits informatiques et IoT domestiques devraient réduire ou éliminer les connaissances requises pour les utiliser en toute sécurité et en privé. Les réseaux d'entreprise bénéficient de l'attention du personnel professionnel chargé de maintenir la sécurité du réseau et des systèmes. Ce personnel est souvent conscient et suffisamment compétent pour configurer ces appareils selon une base de référence sécurisée. Les interfaces d'administration de la plupart des dispositifs informatiques et IoT sont conçues pour le personnel ayant ce bagage et ce niveau de compétence.

Les propriétaires de réseaux domestiques et de petites entreprises sont moins susceptibles de bénéficier d'un tel soutien, avec pour résultat inévitable des réseaux et des produits déployés de manière non sécurisée. Plutôt que d'attendre des consommateurs qu'ils deviennent des experts en sécurité, les secteurs de l'informatique et de l'IdO devraient donner la priorité à des processus de déploiement et de configuration simples et directs pour les appareils commercialisés auprès des particuliers et des petites entreprises. Pour

[80] Les passerelles sont des composants de l'architecture du réseau qui se situent entre les sous-composants du réseau. *Voir la* section II *ci-dessus* pour des discussions sur les passerelles intelligentes, etc.

Par exemple, si le processus d'installation ne force pas la mise à jour des mots de passe administratifs, ces produits continueront d'être des cibles faciles à incorporer dans les botnets. Les configurations par défaut doivent être les plus sûres pour le champ d'utilisation prévu, et les interfaces basées sur le cloud ou les applications doivent être intuitives et reposer sur les meilleures pratiques de conception actuelles. L'installation des correctifs de sécurité doit être automatique ou très facile à gérer (par *exemple, elle* ne doit pas nécessiter de téléchargement sur des lecteurs flash).

Action 3.3 Les entreprises devraient migrer vers des architectures de réseau qui facilitent la détection, la perturbation et l'atténuation des menaces automatisées et distribuées. Elles doivent également tenir compte de la façon dont leurs propres réseaux mettent les autres en danger.

Divers produits et services anti-DDoS efficaces sont actuellement disponibles, et de nouveaux produits innovants (tels que ceux décrits dans l'action 3.1) sont apparus récemment. Cependant, la plupart des entreprises ont conçu leurs réseaux dans un souci de simplicité et de performance plutôt que de sécurité. En combinaison avec le profil CCA pour la prévention et l'atténuation des attaques DDoS, les entreprises ont l'opportunité de ré-architecturer leurs réseaux pour isoler les dispositifs non sécurisés, gérer les flux de communication, et généralement améliorer la résilience de leurs zones de l'écosystème. Par exemple, les entreprises qui dépendent de systèmes anciens doivent architecturer leurs réseaux de manière à ce que ces dispositifs non sécurisés ne soient pas exposés aux attaques de l'Internet général.

Les risques provenant des réseaux d'entreprise vont au-delà du danger des appareils IoT détournés. Certains services basés sur le réseau permettent aux acteurs malveillants d'amplifier une attaque par le biais de " réflecteurs ", ou de services capables d'envoyer de grandes quantités de trafic vers une cible usurpée. S'ils sont mal configurés pour permettre des requêtes depuis n'importe où sur Internet, les services vulnérables tels que les serveurs DNS permettent aux attaquants d'envoyer d'énormes volumes de trafic contre les victimes. En 2018, l'une des plus grandes attaques DDoS observées à ce jour a exploité une vulnérabilité récemment découverte dans le logiciel relativement obscur MemCacheD. [81] Ces failles sont souvent plus problématiques car les systèmes vulnérables se trouvent sur des machines et des réseaux à l'échelle de l'entreprise, avec une haute disponibilité et une bande passante élevée. Les organisations devraient suivre les meilleures pratiques pour les outils orientés vers l'Internet, et s'assurer qu'ils sont à jour.

Une partie de cette évolution vers de meilleures pratiques de réseau peut se produire organiquement, à mesure que les entreprises intègrent davantage de dispositifs IoT dans leurs environnements en réseau et prennent conscience des risques des applications tournées vers l'extérieur. Cependant, les pouvoirs publics, l'industrie et la société civile doivent s'efforcer d'améliorer les connaissances des utilisateurs et des entreprises sur les menaces et les meilleures pratiques de sécurité, par le biais de collaborations telles que des campagnes de partenariat et des activités d'engagement stratégique. Lorsque ces connaissances seront formalisées, on pourra envisager de les inclure dans les futures versions du cadre de cybersécurité du NIST.

Action 3.4 Le gouvernement fédéral devrait étudier comment un déploiement plus large d'IPv6 peut modifier l'économie de l'attaque et de la défense.

L'Amérique du Nord a épuisé les adresses IPv4 inutilisées et facilement distribuables en 2015, mais très peu de consommateurs et de petites entreprises profitent actuellement de l'espace et des capacités des adresses IPv6. Le gouvernement et l'industrie ont planifié et travaillé en vue d'une adoption plus large de l'IPv6, mais ils devraient également considérer comment cela changera l'espace d'attaque potentiel et l'ampleur des attaques automatisées et distribuées.

[81] Lili Hay Newman, *GitHub a survécu à la plus grande attaque DDoS jamais enregistrée*, Wired (1er mars 2018, 11 h 01), https://www.wired.com/story/github-ddos-memcached/.

L'une des difficultés rencontrées pour informer les consommateurs qu'un appareil de leur réseau est lié à une activité malveillante est le grand nombre d'appareils généralement connectés à un réseau domestique ou de petite entreprise. Les routeurs dotés de la fonction NAT, qui peuvent donner l'impression que de nombreux appareils ont la même adresse IP, peuvent entraver la notification. Avec le passage à l'IPv6, les fournisseurs d'accès Internet grand public seront peut-être mieux placés pour observer le mauvais comportement de certains appareils lorsque les adresses IPv6 ne seront pas soumises au NAT. Ces informations peuvent, à leur tour, être mises en correspondance avec d'autres solutions axées sur la périphérie.

La mise en œuvre de routeurs compatibles NAT au niveau des particuliers et des petites entreprises a parfois servi de protection clé pour les points d'extrémité vulnérables. Les outils NAT agissent comme un pare-feu accessoire, empêchant les dispositifs domestiques d'être directement atteints par le type d'outils de balayage de masse qui propagent les logiciels malveillants et conduisent à une infection généralisée ; les caméras de sécurité étaient une cible commune du botnet Mirai parce qu'elles ne se trouvent généralement pas derrière un routeur compatible NAT. Dans les architectures actuelles, un réseau basé sur IPv6 permettrait probablement à chaque appareil d'être adressable. En théorie, l'espace d'adressage IPv6 est si vaste qu'il ne pourrait pas être scanné par les outils existants, mais les experts ont observé que les modèles permettraient aux nouvelles techniques de scannage de découvrir des dispositifs vulnérables.

La NTIA devrait travailler avec les parties prenantes pour identifier les leçons apprises de l'industrie et d'autres pays, en examinant plus en détail les obstacles et les options pour aligner les incitations afin d'encourager les FAI à effectuer une transition complète vers IPv6 plus rapidement. Pour assurer la défense et atténuer les risques, il faudra continuer à innover à la périphérie du réseau. Comprendre cela plus tôt permettra de trouver de meilleures solutions lorsque l'utilisation d'IPv6 se généralisera.

Objectif 4 : Promouvoir et soutenir les coalitions entre les communautés de la sécurité, des infrastructures et des technologies opérationnelles au niveau national et international.

Pour améliorer la résilience de l'internet et des infrastructures de communication, il faut faciliter la mise en œuvre d'actions coordonnées qui dépassent les frontières géopolitiques, publiques-privées, sectorielles et techniques. Cette section identifie des actions clés pour accroître l'engagement entre les communautés de parties prenantes critiques.

Action 4.1 Les FAI et les grandes entreprises devraient accroître le partage d'informations avec les agences gouvernementales et entre elles afin de fournir des informations plus opportunes et exploitables concernant les menaces automatisées et distribuées.

Si bon nombre des actions décrites dans ce rapport augmenteront le coût ou réduiront l'efficacité des attaques automatisées et distribuées, les actions des forces de l'ordre ont un impact unique sur la communauté des botnets. En mettant hors service les systèmes de commande et de contrôle, les forces de l'ordre peuvent rapidement "lobotomiser" une menace distribuée. Les poursuites engagées contre les principaux acteurs de l'économie des botnets ne font pas que ralentir le développement des menaces distribuées par les participants actuels, elles découragent également les développeurs potentiels.

Les forces de l'ordre comptent sur les FAI, grands et petits, les équipes de réponse aux incidents, les sociétés de cybersécurité et de réponse aux incidents, les fournisseurs d'antivirus, les entités commerciales et les sociétés de renseignement sur les cybermenaces pour soutenir les enquêtes en cours et les autres efforts de lutte contre les menaces automatisées en fournissant des informations exploitables sur les menaces et les tendances affectant leurs réseaux et leurs clients. En fournissant des informations encore plus opportunes et exploitables, les FAI et les autres fournisseurs d'infrastructures clés peuvent faciliter, soutenir et accélérer les actions des forces de l'ordre, y compris celles qui touchent les réseaux de zombies distribués sur le territoire de l

globe. Par exemple, les parties prenantes ont suggéré que l'élargissement des rapports d'incidents pour inclure les attaques infructueuses pourrait fournir des alertes précoces et permettre une intervention plus rapide des forces de l'ordre. Ce type de données aiderait également la communauté de la sécurité à mieux comprendre le paysage des risques.

Les services répressifs peuvent identifier de manière proactive les types de données qui les aideront à enquêter et à poursuivre les mauvais acteurs, et travailler avec les fournisseurs d'infrastructures pour rendre le partage de ces informations avec le gouvernement moins coûteux et plus facile, tout en protégeant la vie privée des internautes. [82] L'amélioration du partage des informations sur la cybersécurité reste l'un des éléments clés pour prévenir et atténuer les problèmes actuels et émergents de la cybercriminalité. Pour promouvoir la confiance et des relations plus larges qui se sont avérées utiles, les services répressifs devraient poursuivre leurs efforts de sensibilisation auprès des communautés de la sécurité et des réseaux pour les aider à identifier et à comprendre les bons partenaires au sein du gouvernement.

Les organismes publics, y compris les services répressifs, doivent continuer à améliorer l'actualité et la pertinence des informations de cybersécurité qu'ils partagent afin de prévenir et d'atténuer les cyberincidents. Les forces de l'ordre traitent les entreprises victimes d'une intrusion ou d'une attaque distribuée comme des victimes d'un crime, et mènent leurs enquêtes sur ces crimes signalés avec discrétion pour éviter, dans la mesure du possible, la diffusion injustifiée d'informations concernant l'incident. En outre, les organisations privées doivent partager les informations relatives à la cybersécurité au sein de leur secteur d'activité par l'intermédiaire des organisations de partage et d'analyse de l'information et avec les agences gouvernementales, le cas échéant, tout en identifiant clairement les informations qui doivent être partagées avec d'autres entités pour éviter tout préjudice supplémentaire.

Les RIR et les bureaux d'enregistrement peuvent faciliter l'attribution des mauvais acteurs en maintenant des bases de données WHOIS exactes. En outre, le gouvernement fédéral devrait s'engager auprès de ses homologues européens pour s'assurer que l'accès rapide à aux informations WHOIS est préservé, à mesure que les protections européennes de la confidentialité des données sont appliquées, afin de préserver un outil essentiel pour les efforts nationaux et mondiaux d'investigation des botnets. Les gouvernements peuvent collaborer avec les entités du secteur privé chargées du respect des réglementations relatives à la protection de la confidentialité des données, ainsi qu'avec les entités participant aux enquêtes sur les botnets, afin de s'assurer que les deux équités sont préservées (conformité et enquêtes sur les botnets).

Action 4.2 Le gouvernement fédéral devrait promouvoir l'adoption internationale des meilleures pratiques et des outils pertinents par le biais d'un engagement international bilatéral et multilatéral.

Des améliorations significatives de la résilience de l'écosystème ne peuvent être obtenues par une action nationale seule. Les États-Unis devraient s'engager régulièrement avec des partenaires internationaux sur la cybersécurité, aux niveaux bilatéral, régional et international, en tirant parti de l'expertise des agences fédérales. Pour les questions liées au DNS, la NTIA devrait coordonner son action avec les agences fédérales et représenter les positions américaines dans les forums multipartites, tels que l'Internet Corporation for Assigned Names and Numbers (ICANN) et l'Internet Governance Forum.

La normalisation internationale pourrait être particulièrement bénéfique. Les normes internationales pour les produits et services IoT ainsi que les normes qui pourraient autrement perturber les attaques automatisées et distribuées pourraient élargir le marché des produits qui contribuent à la résilience de l'écosystème. Comme le recommande le rapport du NSTAC, l'industrie et les agences fédérales qui participent à l'élaboration des normes devraient

[82] *Voir, par exemple,* Information Sharing and Analysis Organization (ISAO) Standards Organization, *ISAO SP 4000 : Protecting Consumer Privacy in Cybersecurity Information Sharing v1.0*, (26 juillet 2017), https://www.isao.org/products/isao-sp-4000-protecting-consumer-privacy-in-cybersecurity-information-sharing-v1- 0/.

coordonner une stratégie pour s'engager au sein des organismes internationaux de normalisation appropriés, dirigés par l'industrie, afin de garantir la représentation et le leadership des États-Unis et, grâce à cette participation, défendre une série de normes internationales flexibles et interopérables pour la sécurité de l'IdO.

Action 4.3 Les organismes de réglementation sectoriels, le cas échéant, devraient collaborer avec l'industrie pour garantir une commercialisation non trompeuse et favoriser les considérations de sécurité propres au secteur.

En raison de la complexité et de la diversité du paysage de l'IdO, il est difficile d'envisager un ensemble de règles uniques qui pourraient garantir la sécurité tout en suivant le rythme du changement et la nature dynamique de l'environnement des menaces. Les organismes de réglementation sectoriels peuvent toutefois promouvoir la résilience de l'écosystème en collaborant avec l'industrie pour garantir que la sécurité des produits déployés est adaptée à leur utilisation. Par exemple, la Food and Drug Administration a établi des directives pour les dispositifs médicaux qui dissocient les mises à jour de sécurité de base des régimes de certification des produits existants. [83] Ces lignes directrices sont bénéfiques pour les consommateurs, car les dispositifs médicaux dont ils dépendent deviennent plus résistants aux menaces de cybersécurité, et pour les fabricants, qui bénéficient d'une plus grande clarté quant aux exigences de certification. Les parties prenantes ont souligné que le gouvernement fédéral pourrait bénéficier d'un mécanisme de coordination interagences pour l'IdO afin de promouvoir et de partager ces types de pratiques innovantes et d'enseignements tirés, et d'éviter les conflits réglementaires.

Des mesures d'application judicieuses peuvent profiter aux consommateurs et aux participants honnêtes du marché. La FTC a pris des mesures dans de nombreux cas liés à la vie privée et à la sécurité, les dispositifs IdO figurant dans certaines de ces actions. [84] En arrêtant et en décourageant le marketing trompeur, la FTC peut renforcer la confiance des consommateurs dans les déclarations de sécurité des fournisseurs de technologies IdO et informatiques et soutenir les incitations positives du marché. La FTC a également utilisé son autorité en matière de déloyauté en vertu de la section 5 de la loi FTC pour contester les pratiques de sécurité déraisonnables, y compris dans l'espace IoT. En outre, des agences sectorielles, telles que le ministère américain de la santé et des services sociaux, appliquent les réglementations en matière de sécurité des informations dans les secteurs concernés. Ces politiques peuvent contribuer au débat plus large sur la sécurité des écosystèmes et en bénéficier.

Action 4.4 La communauté doit identifier les points de levier et prendre des mesures concrètes pour perturber les outils et les incitations des attaquants, y compris le partage et l'utilisation actifs des données de réputation.

De nombreuses menaces découlent d'asymétries qui favorisent les attaquants en répartissant l'exploitation entre des acteurs diffus dans l'écosystème. Les défenseurs peuvent utiliser des mesures de partage des données et des informations pour suivre les outils des attaquants et peuvent utiliser l'incidence des dommages pour identifier les outils et les acteurs. Dans certains cas, des efforts de coordination relativement légers devraient permettre de perturber des classes d'attaques plus larges. La section 3.3 souligne l'importance pour les organisations d'identifier les réflecteurs qui amplifient les attaques DDoS. La communauté peut suivre la présence de ces menaces pour aider à cibler la sensibilisation et la réduction des menaces. Ce type de partage a permis de lutter contre des menaces telles que le spam, et peut être exploité contre d'autres vecteurs d'attaque.

[83] Food and Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, (28 déc. 2016), *disponible sur* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. [84] *Voir, par exemple,* Federal Trade Commission, *In the Matter of TRENDnet, Inc.* , FTC Matter/File Number 122 3090, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (dernière mise à jour le 7 février 2014).

"L'hébergement fast-flux" est la modification automatisée et rapide des adresses IP attribuées aux hôtes dans le DNS pour masquer l'emplacement de sites web soutenant des activités malveillantes, illégales ou criminelles. En 2008, un avis du comité consultatif sur la sécurité et la stabilité (SSAC)85 a examiné les mesures que certains bureaux d'enregistrement et registres mettent en œuvre aujourd'hui : surveillance des modifications apportées aux enregistrements DNS qui indiquent un hébergement fast-flux, restriction de la fréquence des modifications DNS et des plages de valeurs, et surveillance de l'accès aux comptes des titulaires de noms de domaine pour empêcher l'automatisation. Elle a également examiné comment les bureaux d'enregistrement pourraient appliquer ces mesures pour accélérer les processus de suspension des sites web et des noms de domaine illégaux. Ces mesures pourraient faire une différence substantielle dans les efforts visant à réduire l'activité des réseaux de zombies, mais elles n'ont pas été largement mises en œuvre. Les nouvelles avancées des attaquants, notamment les "réseaux à double flux", nécessitent davantage d'innovation et de collaboration au niveau des réseaux. La communauté au sens large, y compris le gouvernement fédéral, devrait plaider au sein des forums multipartites concernés (par *exemple,* l'ICANN et les RIR) en faveur d'une mise en œuvre plus large de ces mesures, ou de mécanismes alternatifs pour atteindre cet objectif.

Certaines menaces pour l'écosystème sont alimentées par des marchés illicites particuliers. Le marché actif des DDoS pour le compte de tiers est florissant dans les communautés de joueurs. La collaboration entre les sociétés de jeux et les processeurs de paiement peut potentiellement permettre de suivre et de punir ceux qui utilisent ces services, ce qui assèche le marché. De même, le marché des justificatifs d'identité volés peut être perturbé en rendant la validation des données plus difficile. [86] L'utilisation d'outils basiques d'anti-automatisation sur le web peut augmenter le coût pour les attaquants de la vérification de la valeur des informations d'identification volées, réduisant ainsi le profit tiré de leur vol et de leur utilisation. Plus généralement, les recherches suggèrent que le fait de cibler les partenaires en amont en les informant des vulnérabilités exposées peut jouer un rôle clé dans la mise en place de mesures correctives. [87]

L'investissement du gouvernement peut être un autre levier. Les agences ont été réceptives aux mesures et à la transparence autour des questions de sécurité telles que l'adoption de HTTPS. [88] Avec un peu d'orientation et de contrôle, la réputation de l'hygiène du réseau pourrait être incluse comme facteur dans le processus d'acquisition du gouvernement. Le gouvernement britannique a commencé à expérimenter cette approche. [89]

Action 4.5 La communauté de la cybersécurité devrait continuer à s'engager auprès de la communauté des technologies opérationnelles pour promouvoir la sensibilisation et accélérer l'incorporation des technologies de cybersécurité.

L'intégration de fonctionnalités de mise en réseau dans les technologies opérationnelles (OT) (*par exemple,* les systèmes SCADA dans les environnements industriels) a introduit de nouveaux défis en matière de cybersécurité qui ne peuvent être relevés que grâce à l'expertise combinée des communautés de la cybersécurité et des OT. Les exigences primaires associées aux cas d'OT sont souvent hors de portée des experts en cybersécurité, et les experts en OT sont souvent peu familiers avec les pratiques de cybersécurité de base.

[85] Comité consultatif sur la sécurité et la stabilité de l'ICANN, *SAC 025 : Avis du SSAC sur l'hébergement à flux rapide et le DNS*, (mars 2008), https://www.icann.org/en/system/files/files/sac-025-en.pdf.

[86] *Voir* Timothy Peacock et Allan Friedman, *Automation and Disruption in Stolen Payment Card Markets, (*2014), *disponible sur* http://www.econinfosec.org/archive/weis2014/papers/PeacockFriedman-WEIS2014.pdf.

[87] *Voir, par exemple,* Orcun Cetin, Carlos Gañán, Maciej Korczyński et Michel van Eeten, Make *Notifications Great Again : Learning How to Notify in the Age of Large-Scale Vulnerability Scanning*, (2017), *disponible à l'adresse* http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_17.pdf.

[88] *Voir, par exemple*, Eric Mill, *Tracking the U.S. Government's Progress on Moving to HTTPS*, General Services Administration - 18F, (4 janvier 2017), https://18f.gsa.gov/2017/01/04/tracking-the-us-governments-progress-on- moving-https/.

[89] *Voir* Ian Levy, *Active Cyber Defence-One Year On*, UK National Cyber Security Centre, (5 février 2018), *disponible sur* https://www.ncsc.gov.uk/information/active-cyber-defence-one-year.

Le gouvernement fédéral peut faciliter ce processus en élargissant les engagements actuels qui réunissent les communautés de la cybersécurité et de l'OT pour partager les connaissances et l'expertise, et qui favorisent la sensibilisation et accélèrent l'adoption des technologies de la communauté de la cybersécurité. Les agences sectorielles travaillent en étroite collaboration avec leurs secteurs pour comprendre les risques liés à la cybersécurité, pour mettre les secteurs en relation avec les ressources fédérales et pour promouvoir la planification de la résilience. L'équipe d'intervention d'urgence pour les systèmes de contrôle industriel (ICS-CERT) s'efforce de réduire les risques au sein de tous les secteurs d'infrastructures critiques et collabore avec les équipes d'intervention en cas d'incident informatique (CIRT) internationales et du secteur privé pour partager les incidents de sécurité liés aux systèmes de contrôle et les mesures d'atténuation. La communauté de la cybersécurité du gouvernement fédéral poursuit actuellement des engagements spécifiques aux dispositifs avec des communautés OT spécifiques, sur des sujets tels que les mises à jour sécurisées pour les pompes à perfusion. La communauté des technologies de l'information devrait participer aux actions industrielles citées dans ce rapport afin de trouver des solutions sectorielles aux cyberrisques qui lui sont propres.

Objectif 5 : accroître la sensibilisation et l'éducation dans l'ensemble de l'écosystème.

Pour renforcer la résilience de l'écosystème de l'internet et des communications face aux menaces distribuées, toutes les parties prenantes doivent comprendre leurs rôles et responsabilités et être prêtes à les assumer. Cette section identifie les actions spécifiques aux menaces distribuées qui permettraient de combler les écarts entre les compétences et les responsabilités actuelles.

Ces actions proposées ne remplacent pas les efforts généraux visant à accroître la sensibilisation et l'éducation en matière de cybersécurité. Les parties prenantes ont indiqué que ces initiatives générales de sensibilisation et d'éducation à la cybersécurité sont essentielles pour accroître la résilience de l'écosystème de manière durable. Par exemple, l'importance de commencer l'éducation à la cybersécurité dès la maternelle a été soulignée à plusieurs reprises dans les commentaires publics et les contributions aux réunions et ateliers.

L'initiative nationale pour l'éducation à la cybersécurité90 (NICE), dirigée par le NIST du ministère américain du commerce, est un partenariat entre le gouvernement, le monde universitaire et le secteur privé axé sur l'éducation, la formation et le développement de la main-d'œuvre en matière de cybersécurité. Sa mission consiste à dynamiser et à promouvoir un réseau robuste et un écosystème d'éducation, de formation et de développement de la main-d'œuvre en matière de cybersécurité, en mettant l'accent sur les travailleurs de ce secteur. Les programmes vont de l'enseignement de la cybersécurité de la maternelle à la 12e année et des filières universitaires, telles que les centres nationaux d'excellence académique en cybersécurité91, à l'élaboration et à la gestion de programmes d'évaluation et de formation axés sur les performances. Le ministère de la sécurité intérieure complète les contributions de NICE, en jouant un rôle essentiel dans les efforts de sensibilisation par le biais de la campagne STOP. PENSER. CONNECT. [92].

Les actions suivantes s'appuient sur ces efforts plus généraux de sensibilisation et d'éducation à la cybersécurité, en identifiant les possibilités de sensibilisation et d'éducation spécifiquement liées à l'atténuation ou à la prévention des menaces distribuées.

[90] National Initiative for Cybersecurity Education, National Institute of Standards and Technology, https://www.nist.gov/itl/applied-cybersecurity/nice (dernière visite le 4 avril 2018).
[91] Centres d'excellence académique en cybersécurité, Agence de sécurité nationale, https://www.nsa.gov/resources/educators/centers-academic-excellence/ (dernière visite le 10 avril 2018). [92] Arrêtez-vous. Pensez. Connect, https://www.stopthinkconnect.org/ (dernière visite le 4 avril 2018).

Renforcer la résilience de l'Internet et de l'écosystème des communications contre les botnets et autres menaces automatisées

Action 5.1 Le secteur privé devrait établir et administrer des outils d'information volontaires pour les dispositifs IoT domestiques, soutenus par un processus d'évaluation évolutif et rentable, auxquels les consommateurs peuvent se fier et qu'ils comprennent intuitivement.

Le secteur privé, en consultation avec la société civile et les experts gouvernementaux, devrait concevoir une approche efficiente et efficace d'évaluation et d'étiquetage des dispositifs IoT afin que les consommateurs soucieux de sécurité puissent faire des choix éclairés et créer des incitations commerciales pour le développement de produits sécurisés dès la conception. De nombreux produits IoT disponibles dans le commerce n'ont pas été conçus en tenant compte de la sécurité. Ces appareils créent un risque systémique pour tous les membres de l'écosystème et mettent en danger la vie privée et la sécurité des consommateurs. Dans un monde idéal, les consommateurs préféreraient des produits IoT qui protègent également leur sécurité et leur vie privée, mais les consommateurs soucieux de sécurité ne peuvent pas facilement identifier les produits IoT qui ont été conçus pour être sécurisés.
Sans ces informations, leurs critères de sélection se limitent au prix et à l'ensemble des fonctionnalités.

Le secteur privé est le plus à même de créer et de maintenir des mécanismes légers et agiles, mais il peut souvent bénéficier du pouvoir de convocation du gouvernement. Le gouvernement fédéral devrait réunir les parties prenantes de l'industrie, de la société civile et du gouvernement dans un processus multipartite afin d'explorer les exigences d'une approche viable de l'étiquetage. Cet effort peut s'appuyer sur les succès initiaux de programmes tels que le processus multipartite de la NTIA sur la mise à niveau et les correctifs de sécurité de l'IdO, qui a produit un document détaillant les éléments clés que les fabricants devraient envisager de communiquer aux consommateurs avant et après l'achat. [93] Les parties prenantes devraient examiner si un mécanisme reposant sur l'affirmation du fournisseur est viable et répond aux besoins des consommateurs domestiques. La viabilité d'un tel mécanisme pourrait reposer en partie sur les interdictions existantes en matière de tromperie commerciale. Par exemple, la Federal Trade Commission pourrait protéger l'intégrité du mécanisme d'évaluation en prenant des mesures contre le marketing trompeur (par *exemple, les* fausses déclarations de conformité), sachant que les assurances de sécurité dans cet espace ne peuvent pas offrir des garanties similaires à celles des affirmations de sécurité qui restent statiques dans le temps. Le DHS pourrait également soutenir le programme d'évaluation par le biais de ses activités de sensibilisation existantes, telles que STOP. PENSER. CONNECT. (Voir Action 5.3). [94]

Bien que la sécurité et la confidentialité de l'IdO ne soient pas parfaitement analogues, des mécanismes tels que les programmes NHTSA 5-Star Safety Rating et Energy Star ont réussi à sensibiliser les clients et à créer des marchés pour les véhicules sûrs et les appareils à haut rendement énergétique, ce qui étaye l'hypothèse selon laquelle une approche d'étiquetage bien conçue permettrait de réduire les attaques automatisées et distribuées. Toutefois, le grand nombre de dispositifs IoT différents et la période de vente relativement brève de nombre de ces dispositifs (par rapport aux voitures et aux chauffe-eau) indiquent qu'un mécanisme plus léger et plus agile sera nécessaire. Compte tenu de la nature mondiale des affaires aujourd'hui, le mécanisme d'évaluation devrait, dans la mesure du possible, être basé sur des normes reconnues au niveau international. En outre, toute utilisation d'une approche d'évaluation et d'étiquetage de la sécurité devrait refléter les différences entre les assertions de sécurité, qui restent statiques dans le temps, et les assertions de sécurité, qui ne peuvent offrir des garanties similaires. Le DHS pourrait compléter ces mécanismes d'application générale en explorant les possibilités d'un régime de certification qui pourrait être efficace pour répondre aux besoins des infrastructures critiques.

L'évaluation subjective des dispositifs IdO et de leur facilité d'utilisation joue également un rôle. Les organismes de test orientés vers les consommateurs complètent souvent les analyses basées sur les caractéristiques et les historiques de réparation par des évaluations plus subjectives du confort ou de la convivialité. La facilité d'utilisation des interfaces de gestion de la sécurité est une question particulièrement délicate.

[93] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (dernière mise à jour le 7 novembre 2017). [94] Arrêtez. Pensez. Connect, https://www.stopthinkconnect.org/ (dernière visite le 4 avril 2018).

problème difficile. En incluant des évaluations réfléchies de la convivialité, les organismes de test orientés vers les consommateurs peuvent aider ces derniers à identifier les produits qui conviennent à leur niveau de compétence.

Action 5.2 Le secteur privé devrait établir des systèmes de labellisation volontaire pour les applications industrielles de l'IdO, soutenus par un processus d'évaluation évolutif et rentable, afin d'offrir une assurance suffisante pour les applications d'infrastructures critiques de l'IdO.

Les infrastructures critiques et les applications industrielles de l'IdO présentent des risques nettement plus élevés pour la nation que les applications domestiques dans le cadre d'attaques automatisées et distribuées. Ces dispositifs sont également déployés dans des environnements très différents, soutenus par des administrateurs professionnels. Le mécanisme volontaire d'évaluation légère envisagé dans l'action 5.1 n'offrirait pas un niveau d'assurance suffisant pour ces clients, et des fonctionnalités supplémentaires seront probablement nécessaires. Les fonctions d'évaluation telles que l'authentification des dispositifs, les racines de confiance matérielles ou les fonctions de mise à jour gérées nécessiteraient une interaction directe avec les produits, voire un examen du code source.

Des exemples de réussite d'un tel processus existent tant dans le secteur public que dans le secteur privé. Par exemple, le programme de validation des modules cryptographiques du NIST fait appel à des laboratoires d'essai indépendants pour évaluer la sécurité des modules cryptographiques par rapport à la norme FIPS 140 (Federal Information Processing Standards) depuis plus de deux décennies. Dans le secteur privé, la société de sécurité et de certification UL dispose d'une variété de systèmes de certification et de conformité pour les marchés commerciaux et de consommation, avec plus de 20 milliards de marques UL apparaissant sur les produits en 2016. Cependant, un étiquetage fragmenté ou trop complexe peut se retourner contre vous. La FTC, qui dispose d'une expertise considérable en matière d'étiquetage, est favorable à des informations claires, mais met en garde contre le fait que "de mauvaises informations, y compris des informations trop détaillées, peuvent en fait empêcher les consommateurs de faire des choix éclairés "[95].

Le secteur privé devrait mettre en place un processus d'évaluation efficace mais solide pour s'assurer que les dispositifs IoT destinés à ces secteurs offrent une résilience renforcée à un niveau d'assurance approprié. L'établissement d'une liste de produits évalués permettra aux entreprises soucieuses de la sécurité de faire des choix éclairés et de créer des incitations commerciales pour des processus robustes de cycle de vie de développement sécurisé.

Action 5.3 Le gouvernement devrait encourager les secteurs de l'enseignement et de la formation à intégrer pleinement les pratiques de codage sécurisé dans les programmes d'informatique et les programmes connexes.

Comme indiqué dans l'Action 1.3, de nombreuses vulnérabilités courantes en matière de sécurité (par *exemple,* les dépassements de tampon) peuvent être évitées ou corrigées pendant le développement du produit en utilisant des outils de développement de sécurité appropriés, tels que les fuzzers, les analyseurs statiques et les langages de programmation sûrs. Bien que les établissements universitaires, les camps d'entraînement au codage et les programmes de reconversion professionnelle créent une main-d'œuvre de codage plus importante, leurs diplômés sont rarement compétents dans ces langages ou aptes à utiliser ces outils de développement. Au lieu de cela, les étudiants acquièrent une expérience significative avec des outils de développement de logiciels qui ne prennent pas en compte la sécurité, et des méthodologies de développement de logiciels qui ne donnent pas la priorité à la sécurité, créant ainsi un état d'esprit de "boulonnage" parmi la main-d'œuvre de développement de logiciels.

Les entreprises qui souhaitent améliorer les pratiques de codage peuvent être dissuadées par une main-d'œuvre non préparée et parfois résistante - les codeurs qualifiés peuvent facilement changer d'emploi s'ils ne sont pas intéressés par l'apprentissage des nouvelles méthodes de codage.

[95] Commission fédérale du commerce, *Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers",* à la page 6, (2017), *disponible sur* https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications- information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

et peuvent être difficiles à remplacer. En enseignant des méthodologies de conception de logiciels sécurisés et en encourageant l'utilisation de chaînes d'outils de développement de logiciels axés sur la sécurité dans l'ensemble du programme d'études en informatique et en cybersécurité, nous pouvons préparer notre main-d'œuvre à créer des logiciels de meilleure qualité et accroître l'acceptation des chaînes d'outils de développement de logiciels axés sur la sécurité.

Le gouvernement fédéral peut faciliter ces changements grâce aux relations existantes avec le monde universitaire et l'industrie de la formation. En particulier, le NICE devrait s'engager avec le monde universitaire et le secteur privé à intégrer les principes de conception sécurisée et les outils de soutien à chaque étape du cursus. La catégorie "fourniture sécurisée" du cadre des effectifs de cybersécurité de NICE (NICE Framework) comprend les connaissances, les compétences et les aptitudes nécessaires au développement de logiciels et de produits sécurisés. NICE devrait s'associer aux prestataires d'enseignement et de formation pour les encourager à utiliser le NICE Framework comme outil de référence pour l'élaboration du contenu des cours. Autre exemple, la FTC accueille chaque année la conférence PrivacyCon, qui offre une vitrine aux travaux des universitaires et des chercheurs en sécurité sur la vie privée et la sécurité. [96]

Action 5.4 Le secteur universitaire, en collaboration avec l'initiative nationale pour l'éducation à la cybersécurité, devrait faire de la cybersécurité une exigence fondamentale dans toutes les disciplines de l'ingénierie.

L'intégration de l'informatique dans toute la gamme de produits et de services fait apparaître des menaces de cybersécurité dans de nouvelles catégories de produits. Les concepteurs de produits n'ont souvent pas conscience des risques qui peuvent être introduits lors de l'intégration de l'informatique dans les lignes de produits traditionnelles. Il est de plus en plus nécessaire qu'ils comprennent la gestion des risques liés à la cybersécurité, car nous intégrons des capteurs dans de nombreux environnements, notamment le sol, les autoroutes et les bâtiments. Par exemple, les caméras de télévision en circuit fermé (CCTV) sont disponibles dans le commerce depuis 1949, mais n'ont évolué que récemment vers des dispositifs connectés à Internet. En 2016, le botnet Mirai a compromis plus de 100 000 caméras CCTV pour soutenir des attaques DDoS. Dans d'autres cas, des caméras connectées à Internet utilisées comme moniteurs pour bébés ont été piratées en exploitant les mots de passe administratifs par défaut, violant ainsi la vie privée des propriétaires. [97]

Pour s'assurer que les concepteurs de produits sont conscients des risques introduits dans la technologie opérationnelle, les établissements universitaires enseignant l'ingénierie et les disciplines connexes devraient intégrer la cybersécurité de base dans le programme d'études requis. Comme ci-dessus, le NICE devrait s'engager avec le monde universitaire et le secteur privé pour intégrer les principes dans le cursus de l'ingénierie et des disciplines connexes.

Action 5.5 Le gouvernement fédéral devrait mettre en place une campagne de sensibilisation du public pour soutenir la reconnaissance et l'adoption de la base de référence et de la marque de sécurité des dispositifs IoT domestiques.

Pour avoir un impact, la base de sécurité des dispositifs IoT domestiques doit être reconnue et privilégiée par les consommateurs soucieux de sécurité, ce qui renforce la résilience des réseaux domestiques où les dispositifs sont installés et crée des incitations commerciales pour les fournisseurs soucieux de sécurité. Le gouvernement fédéral mène depuis longtemps des campagnes de sensibilisation du public, avec le soutien des parties prenantes, sur des sujets très variés : comment prévenir les feux de forêt, l'utilité de la ceinture de sécurité et l'importance du dépistage du VIH. La campagne Stop. Pensez. Connect. est une campagne nationale de sensibilisation du public, parrainée par le DHS, qui vise à accroître le nombre d'utilisateurs de l'Internet.

[96] *Voir* Federal Trade Commission, *PrivacyCon 2018*, https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018 (dernière visite le 4 avril 2018).
[97] *Voir* Darlene Storm, *Hacker Hijacks Wireless Foscam Baby Monitor, Talks and Freaks Out Nanny*, Computerworld (2 février 2015, 12:09 PM PT), https://www.computerworld.com/article/2878741/hacker-hijacks- wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html.

compréhension des cybermenaces et de donner au public américain les moyens d'être plus sûr et plus sécurisé en ligne. Le gouvernement fédéral devrait envisager de tirer parti de Stop. Think. Connect. ou mettre en place une campagne complémentaire de sensibilisation du public pour alerter les utilisateurs domestiques et les petites organisations sur l'importance de la base de référence des dispositifs IoT domestiques et les éduquer sur la façon d'identifier des produits plus sûrs. Plus généralement, une meilleure sensibilisation des utilisateurs au risque de cybersécurité est essentielle à un écosystème résilient, et le gouvernement devrait accroître son engagement stratégique et son pouvoir de rassemblement avec des communautés d'utilisateurs ciblées et la société civile pour améliorer l'adoption de la sécurité et la sensibilisation, en accueillant toute partie prenante non gouvernementale qui souhaite jouer un rôle plus important.

*** * ***

Prochaines étapes initiales pour l'action des parties prenantes

La section ci-dessus détaille 24 actions conçues pour atteindre cinq objectifs. Ces cinq objectifs se renforcent mutuellement ; ils doivent tous être atteints pour accroître durablement la résilience de l'écosystème de l'internet et des communications. De nombreuses actions se renforcent également mutuellement par conception, même entre les objectifs, de sorte que l'exclusion ou l'omission d'une action pourrait potentiellement retarder la réalisation de plusieurs objectifs. Cependant, nous ne nous attendons pas à ce que toutes les actions se déroulent simultanément, en raison de considérations telles que les contraintes de ressources dans les communautés de parties prenantes concernées. En outre, certaines actions sont déjà en cours, tandis que d'autres dépendent de facteurs extérieurs. Le gouvernement fédéral ne dirigera pas la mise en œuvre des actions spécifiques à l'industrie. Cependant, comprenant que dans certains cas, il peut falloir du temps au secteur privé pour s'organiser, le gouvernement américain commencera immédiatement à coordonner les étapes initiales décrites ci-dessous.

Élaborer une feuille de route hiérarchisée pour des actions coordonnées visant à accroître la résilience de l'internet et de l'écosystème des communications face aux menaces distribuées.

Afin de s'assurer que les actions les plus importantes sont dotées de ressources adéquates et exécutées efficacement par les parties prenantes, les communautés de parties prenantes ont fortement encouragé le gouvernement fédéral à délimiter clairement les priorités d'action. [98] En particulier, certaines actions n'impliquent pas directement le gouvernement fédéral, mais soutiennent, ou sont soutenues par, des actions qui dépendent de la participation ou du leadership du gouvernement fédéral. En indiquant ses propres priorités, le gouvernement fédéral peut accroître la confiance des parties prenantes dans le fait que les ressources investies dans des actions dirigées par l'industrie et dépendant du gouvernement fédéral donneront des résultats productifs.

En plus des dépendances fédérales, certaines actions ont un ordre temporel naturel : par exemple, les programmes d'évaluation dans les actions 5.1 et 5.2 dépendent de l'établissement de bases de capacités de sécurité appropriées dans l'action 1.1. D'autres actions sont mûres pour la priorisation parce que le travail préparatoire est en cours, tel que le profil CSF décrit dans l'action 2.2. Enfin, certaines actions sont particulièrement urgentes en raison de leur long délai d'exécution (*par exemple, les* actions 1.3, 5.3 et 5.4) ou des développements qui réduisent la possibilité pour les États-Unis d'influencer la direction (action 1.2).

Les ministères du commerce et de la sécurité intérieure, en coordination avec l'industrie, la société civile et en consultation avec les partenaires internationaux, devraient être chargés d'élaborer une feuille de route initiale avec des actions prioritaires dans les 120 jours suivant l'approbation du présent rapport. Cette feuille de route devrait s'aligner sur

[98] Cette demande a été soulignée à la fois dans les réponses des parties prenantes à la demande de commentaires du 5 janvier 2018 et dans l'atelier du 28 février au 1er mars 2018.

Les priorités de l'administration telles qu'elles ont été définies après l'achèvement des tâches assignées en vertu du décret 13800. Le gouvernement et le secteur privé travailleront ensemble pour s'assurer que la feuille de route est mise à jour et maintenue à mesure que les parties prenantes accomplissent les actions identifiées.

Le gouvernement fédéral donnera l'exemple.

Les parties prenantes ont indiqué que le leadership fédéral par l'exemple est essentiel à la mise en œuvre du rapport par les autres parties prenantes. Les parties prenantes ont indiqué que l'adoption par le gouvernement fédéral de pratiques de "bon voisinage" qui profitent principalement à l'écosystème et aux activités d'approvisionnement constituerait une base pour d'autres activités visant à réduire les menaces automatisées et distribuées. En particulier, les mesures prises par les agences fédérales pour mettre en œuvre le filtrage de sortie afin d'empêcher l'usurpation d'adresse réseau, fermer les réflecteurs utilisés pour amplifier les volumes de trafic et mesurer la conformité des agences (et potentiellement nommer et faire honte aux mauvais acteurs) démontreraient la détermination fédérale et encourageraient les actions bénéfiques des autres parties. Le NIST, l'OMB et le DHS devraient étudier les mesures à prendre pour s'assurer que ces meilleures pratiques sont correctement prises en compte dans les politiques, les normes, les directives et la surveillance des agences fédérales.

De même, les activités de passation de marchés fédéraux rendant obligatoire l'acquisition de produits et de services plus sûrs ou plus résilients que ceux couramment disponibles aujourd'hui ont été considérées comme une étape importante vers la mise en place d'incitations commerciales. Les parties prenantes ont suggéré de se concentrer immédiatement sur les actions 1.1, 1.2 et 2.3 pour soutenir les orientations en matière de marchés publics fédéraux. Ce travail de conception peut ensuite conduire à une évaluation des orientations et des normes existantes en matière d'approvisionnement, ainsi qu'à des recommandations spécifiques pour mettre à jour ces orientations afin de refléter les exigences de sécurité.

Encourager le leadership du secteur privé et soutenir la coordination intersectorielle pour suivre la mise en œuvre de la feuille de route.

De nombreuses actions de la feuille de route devraient être dirigées par un secteur industriel, le monde universitaire ou la société civile. L'identification ou l'établissement de structures de gouvernance du secteur privé pour ces activités sera un facteur essentiel pour la durabilité et l'acceptation internationale des produits du travail (par *exemple, les* spécifications techniques ou les systèmes d'évaluation). Lorsque des organismes existants mènent déjà des actions connexes ou représentent déjà des communautés clés, il convient de les encourager à prendre la tête des opérations. Les actions peuvent nécessiter une inclusion au-delà des structures actuelles - par exemple, en ajoutant des participants ou des perspectives de la société civile ou internationale.

Au fur et à mesure que des communautés se forment pour mettre en œuvre ces actions, l'établissement d'un lieu de coordination régulière entre ces communautés sera de plus en plus important. La valeur d'une base de référence pour la sécurité de l'IdO est limitée si un schéma d'évaluation ne peut être établi en temps utile. L'alignement et la coordination des investissements sont nécessaires pour maximiser l'impact sur la résilience de l'infrastructure. Jusqu'à ce qu'une ou plusieurs parties du secteur privé soient identifiées d'un commun accord, le gouvernement fédéral fournira un mécanisme de coordination et de communication pour la poursuite de la mise en œuvre, et convoquera des réunions périodiques des parties concernées.

Fournir au président un rapport d'étape de 365 jours sur la mise en œuvre de la feuille de route.

Pour suivre les progrès accomplis, les ministères du commerce et de la sécurité intérieure élaboreront un rapport d'étape de 365 jours à l'intention du président, qui devra être remis un an après la publication initiale de la feuille de route. Cette mise à jour fera le point :
1) les progrès réalisés par l'ensemble de la communauté par rapport à la feuille de route ; 2) l'impact de ces activités de la feuille de route ; 3) une réévaluation de la menace d'attaques automatisées et distribuées, y compris la question de savoir si la stratégie de l'Union européenne en matière de sécurité et de protection de l'environnement est efficace.

La menace augmente ou diminue, et les raisons connues d'un tel changement ; et 4) si des ajustements doivent être apportés à la feuille de route.

Promouvoir la participation mondiale en renforçant l'engagement des parties prenantes et du gouvernement américain dans l'élaboration des politiques et des normes internationales.

La nature mondiale des menaces distribuées a été fréquemment soulignée au cours du processus exécuté par le Département et la Sécurité intérieure. Les parties prenantes ont souligné l'importance des normes, politiques et meilleures pratiques internationales pour promouvoir la participation et la collaboration internationales. En continuant à préconiser des approches dirigées par l'industrie et en participant activement à l'élaboration de normes internationales volontaires et consensuelles, le gouvernement fédéral peut contribuer à l'élaboration de normes pragmatiques et efficaces fondées sur les résultats qui répondent aux besoins de toutes les parties prenantes. Le gouvernement fédéral est également bien placé pour diriger l'engagement international requis pour établir des politiques et des pratiques exemplaires largement acceptées, et il améliorera la coordination avec les intervenants dans le cadre de ces efforts.

Annexe : Liste des acronymes

AI	Intelligence artificielle
BCP	Meilleure pratique actuelle
BGP	Protocole de passerelle frontalière
CCTV	Télévision en circuit fermé
CDN	Réseau de diffusion de contenu
CIRT	Équipe de réponse aux incidents informatiques
CISA	Loi de 2015 sur le partage des informations relatives à la cybersécurité
CSF	Cadre de cybersécurité du NIST
CSIRT	Équipe de réponse aux incidents de sécurité informatique
CSRIC	Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications
DDoS	Déni de service distribué
DHS	Département de la sécurité intérieure
DNS	Système de nom de domaine
FIPS	Normes fédérales de traitement de l'information
FIRST	Forum des équipes de sécurité et de réponse aux incidents
FTC	Commission fédérale du commerce
GSA	Administration des services généraux
HTTPS	Protocole de transfert hypertexte sécurisé
ICANN	Internet Corporation for Assigned Names and Numbers (Société pour l'attribution des noms de domaine et des numéros)
ICS-CERT	Équipe d'intervention en cas d'urgence cybernétique pour les systèmes de contrôle industriel
IETF	Groupe de travail sur l'ingénierie Internet
IoT	Internet des objets
IP	Protocole Internet
IPv4	Protocole Internet version 4
IPv6	Protocole Internet version 6
ISAC	Centre de partage et d'analyse des informations
ISP	Fournisseur de services Internet
IT	Technologies de l'information
LAN	Réseau local
MANRS	Normes mutuellement acceptées pour la sécurité du routage
MUD	Description de l'utilisation du fabricant
NAT	Traduction d'adresses de réseau
CCN	Centre national de coordination des communications
CCNIC	Centre national d'intégration de la cybersécurité et des communications
NHTSA	National Highway Traffic Safety Administration
NICE	Initiative nationale pour l'éducation à la cybersécurité
NIST	Institut national des normes et de la technologie
NISTIR	Rapport inter-agences/interne du NIST
NITRD	Recherche et développement en matière de réseaux et de technologies de l'information
NOG	Groupe d'opérateurs de réseau

NSTAC	Comité consultatif du Président sur les télécommunications pour la sécurité nationale
NTIA	Administration nationale des télécommunications et de l'information
OT	Technologie opérationnelle
PPD	Directive politique présidentielle
RFC	Demande de commentaires
RIR	Registre Internet régional
SAM	Gestion des actifs logiciels
SCADA	Contrôle de surveillance et acquisition de données
SSAC	Comité consultatif sur la sécurité et la stabilité