PROGRAMME DE SÉCURITÉ ET DE TECHNOLOGIE

Limiter l'utilisation à des fins malveillantes des menaces et vulnérabilités dans les TIC

Un aperçu des tendances actuelles, des dynamiques de propagation et des réponses du secteur privé

Camino Kavanagh

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

REMERCIEMENTS

L'UNIDIR remercie le gouvernement français pour son large soutien dans le cadre de cette étude.

Autant l'UNIDIR souhaite exprimer sa gratitude à François Delerue, Research Fellow Cyberdefence and International Law Institute for Strategic Research (IRSEM — Institut de recherche stratégique de l'École militaire), et à Chrystiane Roy, Premier secrétaire de la Mission permanente du Canada auprès de l'Office des Nations Unies et des autres organisations internationales à Genève, pour leur précieux apports dans la correction de la première version de ce travail.

L'UNIDIR souhaite exprimer encore un tout particulier merci à Sirine Hijal, Coordinatrice adjointe de la politique étrangère pour le cyberspace Affaires mondiales Canada, pour sa contribution inestimable correction du texte, dans sa globalité.

L'auteur souhaite remercier Evgeny Scherbakov (Doctorant au King's College de Londres et chercheur associé au programme international, Carnegie Corporation de New York), Nicolas Mazzucchi (Directeur de recherche, Fondation pour la recherche stratégique) et Ashley Sweetman (Doctorant au King's College de Londres) pour leurs contributions à cette recherche, ainsi que Madeline Carr (University College de Londres), John Mallery (MIT), Nathalie Van Raemdonck (EUISS), Oleg Demidov et Kerstin Vignard (UNIDIR) pour avoir commenté les versions successives du présent rapport.

À PROPOS DE L'AUTEUR

La Dr. Camino Kavanagh est chercheuse non-résidente auprès de l'UNIDIR et chercheuse invitée au Département des Études de guerre au King's College de Londres. Elle travaille également en qualité de consultante indépendante.

Camino Kavanagh a été consultante auprès du Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale en 2016 et 2017 et consultante principale auprès de l'Organisation pour la sécurité et la coopération en Europe dans le cadre d'une initiative portant sur les mesures de confiance, la prévention des conflits et les technologies de l'information et des communications (TIC). Au-delà de projets en cours, en qualité de consultante auprès d'organisations telles que les Nations Unies et l'Organisation des États américains, elle participe à un certain nombre d'initiatives stratégiques et de recherche sur les TIC et les technologies émergentes et leurs conséquences sur les conflits, le terrorisme et la criminalité.

Camino Kavanagh a obtenu un doctorat du département d'études sur la guerre de King's College à Londres en 2016 et s'est concentrée sur les technologies de l'information, la souveraineté et l'État, un sujet qui reste au centre de ses activités de recherche.

À PROPOS DE L'INSTITUT

L'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) est une institution autonome au sein des Nations Unies qui mène des recherches indépendantes sur le désarmement et les problèmes connexes, en particulier les questions de sécurité internationale. La vision de l'UNIDIR est celle d'un monde stable et plus sûr dans lequel les États et les peuples sont protégés contre les menaces de la violence liée aux armes. Le rôle de l'UNIDIR est de soutenir les États membres, les Nations Unies et les milieux politiques

et de la recherche afin de faire progresser les idées et les actions qui contribuent à un monde plus durable et plus pacifique.

REMARQUE

TABLE DES MATIÈRES

RÉSUMÉ ANALYTIQUE

Quelles sont les tendances récentes en matière de menaces et de vulnérabilités et comment sont-elles utilisées à des fins malveillantes ? Quelles sont les dynamiques permettant la propagation de ces menaces et vulnérabilités ? Quelles mesures le secteur privé, en particulier les entreprises de technologie, prend-t-il pour lutter contre ces menaces et vulnérabilités, limiter leur propagation et contrôler ou contrer une partie de ces dynamiques ?

Alors que nous approchons de la fin de la seconde décennie du XXIe siècle et que nos sociétés – tout comme nos conflits – deviennent de plus en plus dépendants des technologies numériques, les entreprises privées de technologie ont sans aucun doute une responsabilité et un rôle à jouer dans l'élaboration et la mise en œuvre des politiques de sécurité internationale. C'est certainement le cas lorsqu'il s'agit de limiter la propagation des menaces et des vulnérabilités liées aux technologies de l'information et des communications (TIC), dont l'utilisation malveillante a de plus en plus d'incidences sur les questions de sécurité nationale et internationale.

La première partie de ce rapport porte sur les tendances actuelles en matière de menaces et de vulnérabilités liées aux TIC et leurs incidences en termes de sécurité nationale. Celle-ci met en évidence les principaux outils utilisés par les groupes d'attaquants et les failles de sécurité exploitées à des fins malveillantes. La seconde partie traite de certaines des dynamiques qui continuent à permettre la propagation d'outils et de techniques malveillants. Celles-ci comprennent des dynamiques liées aux marchés noirs ou criminels, des dynamiques géopolitiques et de sécurité et nationale ainsi que des dynamiques propres au marché des technologies de l'information. Des discussions relatives à ces différentes dynamiques de propagation sont en cours depuis un certain temps et au cœur de l'élaboration des politiques publiques, mais les réponses, tant publiques que privées, entreprises jusqu'à présent ne semblent pas suffisantes. La dernière partie du rapport traite de la manière dont le secteur des TIC réagit aux menaces et aux vulnérabilités évoquées, en abordant la question sous l'angle de mesures *réactives* et *productives* : les premières sont de nature opérationnelle, alors que les dernières, plus normatives et gagnant en importance, cherchent à influencer le comportement des États et de l'industrie informatique afin de protéger leurs intérêts et, par extension, leurs utilisateurs.

Les principales conclusions de ce rapport suggèrent qu'il est tout d'abord urgent de déterminer si des leviers structurels publics et privés supplémentaires sont nécessaires pour gérer l'ampleur et la portée des menaces et des vulnérabilités liées aux TIC ainsi que les dynamiques de propagation qui y sont associées. Cela comprend les leviers assurant une plus grande sécurité dans la conception et le développement de produits et services numériques, ainsi que ceux pouvant répondre plus efficacement aux dynamiques

criminelles, géopolitiques, de sécurité nationale, et propres l'industrie des TIC abordées dans ce rapport.

Deuxièmement, il est nécessaire d'avoir de meilleurs mécanismes afin d'approfondir la réflexion et favorise la transparence sur les différentes initiatives soutenues par le secteur privé et proposées ou mises en œuvre pour répondre aux menaces et vulnérabilités des TIC. Une telle approche contribuerait à établir un climat de confiance et à convaincre les utilisateurs, les gouvernements et les autres parties concernées de la qualité des initiatives. Celle-ci pourrait également contribuer à recenser les lacunes existantes et émergentes dans les politiques, réglementations et pratiques actuelles ; ce qui contribuerait à déterminer si des leviers structurels supplémentaires, comprenant de la réglementation ou de la législation, sont nécessaires, ainsi qu'à informer ou contribuer aux processus intergouvernementaux au niveau international et régional.

Enfin, le rapport appelle les acteurs tant publics que privés à veiller à ce que leurs réponses demeurent liées au bien commun comme moyens de renforcer la paix et la sécurité internationales. Bien que cette recommandation soit particulièrement compliquée du fait de l'état actuel des relations internationales, il convient d'en faire une priorité.

INTRODUCTION

Au cours des dernières décennies, le secteur privé est devenu un élément de plus en plus pertinent en matière de politiques de sécurité internationale. Une telle évolution est dû à plusieurs facteurs. Premièrement, la mondialisation et l'augmentation des flux transnationaux de capitaux, de biens, de services, de personnes et d'information qui en ont résulté, ont remis en question le rôle de l'État sur plusieurs plans. Le secteur privé a ainsi adopté de nouveaux rôles et étendu son influence normative. Ensuite, la nature des conflits modernes implique que les entreprises du monde entier soient de plus en plus affectées par les crises politico-militaires et, dans de nombreux cas, que leurs activités soient exposées à des risques élevés. De même, il est bien établi que le comportement des entreprises du secteur privé peuvent également provoquer ou donner naissance à des conflits.

Manifestement, il est difficile d'évoquer le « secteur privé » en termes génériques, notamment parce que c'est un terme dont la signification varie selon les acteurs concernés. Dans de nombreux cas, la distinction entre les acteurs privés et les États devient de plus en plus floue. C'est particulièrement vrai pour les questions portant sur les technologies numériques et la sécurité internationale. En outre, les responsabilités existantes ou potentielles que les acteurs du secteur privé adoptent dans ce domaine sont souvent fortement influencés par des facteurs nationaux et juridictionnels ainsi que par la taille, la portée, la culture et les relations avec l'État dans lequel ils opèrent.

Ce document d'orientation concerne principalement les entreprises technologiques privées et les actions qu'elles prennent concernant les menaces et vulnérabilités liées aux technologies de l'information et des communications (TIC) découlant de leurs produits et services ou associées à ces derniers. Alors que nos sociétés sont de plus en plus dépendantes des TIC, les entreprises du secteur des technologies sont devenues des acteurs puissants et influents, avec certaines ayant des chiffres d'affaire supérieurs aux économies de nombreux pays. Dans de nombreux cas et contextes, ces sociétés complètent, voire remplacent, les fonctions traditionnelles de l'État. Cependant, leurs produits, leurs services et leurs infrastructures se trouvent également de plus en plus au cœur des conflits entre États, comme au demeurant les entreprises elles-mêmes.

Qui dit pouvoir accru dit aussi responsabilité accrue, particulièrement en matière de sécurité internationale. À cet égard, plusieurs processus intergouvernementaux internationaux et régionaux ont reconnu l'importance d'impliquer le secteur privé en ce qui concerne les TIC et la stabilité et la sécurité internationales. Par exemple, les Groupes d'experts gouvernementaux des Nations Unies (GGE) chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale ont averti des risques accompagnant les immenses opportunités économiques découlant des TIC. Cependant,

ils ont aussi souligné l'importance d'impliquer le secteur privé dans les mesures coopératives et de confiance qui sont formulées aux niveaux national et international pour répondre aux menaces et vulnérabilités liées aux TIC. L'Organisation pour la sécurité et la coopération en Europe (OSCE) a fait le même constat dans son travail sur les mesures de confiance. Pendant ce temps, pour revendiquer leur place, les acteurs du secteur privé se sont directement impliqués dans des initiatives comme la Commission mondiale sur la stabilité du cyberespace, aidant à identifier les défis émergeants et participant à la conception et à la mise en œuvre de réponses adéquates.

Dans le cadre de la recherche effectuée par UNIDIR sur le rôle existant et émergeant du secteur privé dans les politiques internationales de sécurité, ce rapport identifie les tendances en matière de menaces et vulnérabilités liées aux TIC et souligne certaines dynamiques inquiétantes (de nature criminelle, sécuritaire, géopolitique et commerciale) qui favorisent la persistance et la dissémination de ces menaces et vulnérabilités.

Ce rapport conclut avec certaines observations sur le rôle des sociétés de technologie en ce qui concerne leur réponse à ces tendances et facteurs de propagation des menaces et vulnérabilités. Ce rapport s'appuie sur de la recherche documentaire pour fournir un échantillon des rôles que certaines sociétés de technologie assument pour influencer les comportements des différentes prenantes ainsi que le marché des technologies de l'information. À cet égard, la section finale du rapport pose la question de savoir si l'autoréglementation et la multiplication d'initiatives déclaratoires mettant l'accent sur les principes impliquant le secteur technologique sont suffisantes pour gérer toute l'ampleur et l'étendue des défis et risques auxquels nous faisons face. Peut-être est-il désormais nécessaire d'effectuer un investissement plus important et plus responsable dans les leviers structurels (techniques, politiques, réglementaires et financiers) pertinents afin d'assurer une plus grande sécurité en matière de conception, de développement et d'utilisation des services et produits informatiques. Une discussion approfondie (et une plus grande transparence) sur l'impact des initiatives autoréglementaires existantes aiderait très probablement à identifier les lacunes, tout en informant et contribuant aux processus intergouvernementaux comme le Groupe de travail à composition non limitée et le Groupe des experts gouvernementaux des Nations Unies chargés d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale.

TENDANCES ACTUELLES EN MATIÈRE DE MENACES ET DE VULNÉRABILITÉS

L'environnement actuel des TIC est caractérisé par une « connectivité omniprésente entre des réseaux hétérogènes et divers systèmes et appareils ».[1] Cet espace partagé, interconnecté, hautement complexe et soutenant de multiples modèles d'utilisation, de connectivité et d'accès est devenu un support vital aux interactions économiques, sociales, culturelles et politiques dans le monde entier.[2] Les avantages issus de cet environnement sont significatifs, tout comme les risques pour l'économie mondiale, la vie privée et le maintien de la paix et sécurité internationales. Ces risques découlent des défaillances et vulnérabilités des TIC que divers acteurs exploitent, souvent de façon très créative, à des fins malveillantes et de la difficulté à contrer de tels comportements..[3]Cette section du rapport aborde certaines des tendances actuelles en matière de menaces et de vulnérabilités ainsi que la façon dont elles sont utilisées pour des fins malveillantes, et plus particulièrement celles qui ont (ou sont susceptibles d'avoir) un impact sur la sécurité internationale.

L'explosion de la demande en matière d'interconnectivité, d'intégration et de compatibilité des plateformes rend les matériels informatiques et les logiciels plus complexes et plus homogènes. Ces caractéristiques augmentent les probabilités de dissémination des menaces cybers et représentent de sérieux défis pour les gouvernements et les acteurs de l'industrie, même si ce sont les utilisateurs qui en assument principalement les coûts.

Au cours de la dernière décennie, un certain nombre de groupes ont élaboré des taxonomies, des cadres ou des modèles détaillés pour classer les différentes tendances et menaces cyber. Ceux-ci représentent un spectre d'approches et de méthodologies

[1] C. Vishik, M. Matsubara et A. Plonk, "Key Concepts in Cybersecurity: Towards a Common Policy and Technology Context", dans H. Roygas et A. Osula (eds), *International Cyber Norms: Policy, Legal, and Industry Perspective*, 2016.

[2] C. Demchak, "Resilience, Disruption, and a Cyber Westphalia: Options for National Security in a Cybered Conflict World", dans N. Burns and J. Price (eds), *Securing Cyberspace: A New Domain for National Security*, 2012; J.S. Nye Jr., "Normative Restraints on Cyber Conflict", Belfer Center for Science and International Affairs, 2018.

[3] Le groupe d'experts gouvernementaux des Nations unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale a identifié ce risque dans son rapport de 2015, recommandant que les « États... cherchent à empêcher la prolifération des outils et techniques de TIC malveillantes ». Même si celles-ci ainsi que d'autres recommandations normatives étaient adressées aux États, les acteurs de l'industrie et leurs actions ont un rôle majeur dans leur mise en œuvre.

utilisées par les organismes gouvernementaux,[4] les organisations régionales,[5] les sociétés et associations du secteur privé, ainsi que les organismes techniques.[6] Des grandes sociétés de cybersécurité comme Symantec, Trend Micro, Kaspersky Lab et bien d'autres produisent également leurs propres analyses sur les tendances actuelles et sur l'énumérations des menaces cyber.

Les récentes tendances en matière de menaces comprennent les logiciels malveillants, les attaques provenant du Web et d'applications en ligne, le hameçonnage, le déni de service ou le déni de service distribué, les pourriels, les réseaux de machines zombies ou Botnets, les vols ou détournement de données, les rançongiciels, et le cyber espionnage.[7]

Le logiciel malveillant, défini par l'Union Internationale des Télécommunications comme « un logiciel qui effectue intentionnellement des actions susceptibles d'endommager des données ou de perturber des systèmes »,[8] est un outil prévalent, qui est régulièrement utilisé par les groupes d'attaquants (« ensemble d'activités intrusives similaires qui sont désignées par une dénomination commune au sein de la communauté de sécurité »).[9] Il existe plusieurs types de programmes malveillants qui peuvent être classés par 'familles'

---

[4] Par exemple, les autorités de cybersécurité d'Australie, du Canada, de Nouvelle-Zélande, du Royaume-Uni et des États-Unis (le « Five Eyes » ou Groupe des cinq) ont récemment publié un rapport soulignant cinq techniques et outils fréquemment utilisés et disponibles pour le grand public qui ont été employés à des fins malveillantes dans de récents incidents cyber. Ceux-ci comprennent les troyens d'administration à distance (RAT), les scripts WebShell, les voleurs d'identifiants, les mouvements latéraux, et les outils d'obfuscation de commande et contrôle. Le rapport fournit un aperçu de la menace posée par chaque outil, ainsi que des informations sur l'endroit et le moment de son déploiement par des acteurs hostiles. Des mesures aidant à la détection de chaque outil et limitant leur efficacité sont également décrites. Le rapport conclut avec des conseils généraux permettant d'améliorer les méthodes de défense des réseaux. Voir *Joint Report on Publicly Available Hacking Tools: Limiting the Effectiveness of Tools Commonly Used by Malicious Actors*, octobre 2018, https://www.ncsc.gov.uk/joint-report.

[5] L'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), par exemple, a développé sa propre taxonomie des menaces, et produit un rapport annuel sur le les menaces. Le modèle ENISA, par exemple, utilise la structure suivante pour décrire les cybermenaces : une courte description de la cybermenace telle qu'elle s'est manifestée durant la période de rapport ; une liste de points intéressants avec des observations particulières pour la cybermenace spécifique ; des tendances et des statistiques de haut niveau incluant des informations géographiques ; un top des incidents dans la catégorie de menaces spécifiques ; des vecteurs d'attaque spécifiques utilisés pour lancer la menace ; des actions d'atténuation spécifiques ;la chaîne cybercriminelle pour la cybermenace spécifique ; et des documents de référence. Voir "ENISA Threat Landscape Report 2019", https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape.

[6] Voir par exemple le cadre Common Attack Pattern Enumeration and Classification (CAPEC) de la MITRE Corporation (https://capec.mitre.org/), Open Threat Taxonomy by Enclave Security (https://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf), A Taxonomy of Operational Cyber Security Risks par Carnegie Mellon University (https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf) et autres.

[7] Pour consulter un exemple d'analyse de tendance récente, voir ENISA, *Threat Landscape Report 2018*, 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[8] ITU, "Definitions of terms related to quality of service", Recommendation ITU-T E.800, 2008, p. 10, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-E&type=items.

[9] Comme évoqué par MITRE, il existe des variantes pour le terme « groupe d'attaquants » comme « groupes de menace, groupes d'activité, acteurs de la menace, ensembles d'intrusion, et campagnes ». Les analystes utilisent différentes méthodologies pour « suivre les grappes d'activités » et attribuer un ou plusieurs de ces termes aux responsables. Parfois, certains groupes se voient attribuer « différents noms associés à des activités similaires car différentes entreprises suivent des activités similaires en utilisant différents noms ». La façon dont une organisation définit un groupe peut conduire à un chevauchement d'appellation partiel avec la désignation d'un groupe par une autre organisation. De plus, il est également possible que des désaccords émergent sur les désignations et les activités spécifiques. Voir la note explicative de Mitre Att&ck sur les 'Groupes', https://attack.mitre.org/groups/.

comme les rançongiciels, le minage de cryptomonnaie clandestin, les Botnets, les Troyens d'administration à distance (RAT), les portes dérobées, etc.

Souvent, les vulnérabilités sécuritaires sont utilisées pour déployer de tels outils. Les vulnérabilités sont des faiblesses dans les systèmes d'exploitation, applications ou matériels informatiques, ou des failles créées délibérément ou sans le savoir par les organisations ou les êtres humains. Un code d'exploitation en revanche, est un élément de programme ou logiciel conçu pour tirer parti d'une vulnérabilité sécuritaire afin de compromettre la confidentialité, l'intégrité et la disponibilité des systèmes ciblés, par l'utilisation de différents outils comme des logiciels malveillants. Ces derniers peuvent avoir des répercussions plus importantes sur les réseaux de TIC ou en matière de surveillance et de contrôle des processus cyber-physiques (par ce que l'on appelle des technologies d'exploitation).[10] Néanmoins, parfois l'objectif d'un code d'exploitation est simplement de démontrer l'existence réelle de la vulnérabilité.

Les principaux acteurs malveillants ayant opéré en 2017-2018 comprennent des groupes criminels (et de plus en plus des groupes criminels organisés), des États, des personnes en interne (qu'elles soient malveillantes, négligentes ou compromises), des terroristes, des hacktivistes, et des attaquants de niveau élémentaire (script kiddies).

Voici un échantillon de certains outils d'attaque, menaces, techniques, codes d'exploitation et vecteurs d'attaque ayant fait les gros titres récemment.

Exploitations de vulnérabilités dites « 0-day » ou « Zero-day »

Une des techniques malveillantes ayant reçu le plus d'attention au cours des dernières années est « le code d'exploitation Zero-day » (généralement appelés « Zero-day »), un terme informel utilisé pour décrire l'exploitation d'une vulnérabilité qui n'est pas encore connue du fournisseur, fabricant ou de l'utilisateur final du logiciel ciblé. La dissimulation des Zero-days est souvent perçue comment l'élément qui présente le plus de risques : s'ils ne sont pas signalés de façon responsable au fournisseur ou au fabricant, ils peuvent être découverts et utilisés par d'autres acteurs (gouvernementaux ou non gouvernementaux).

Certains affirment que le virus Stuxnet utilisé pour attaquer le site nucléaire de Natanz en Iran constituait la première utilisation publiquement documentée d'un code d'exploitation Zero-day par un État pour cibler les avoirs d'un autre État. Les agences gouvernementales ont démontré un grand intérêt pour les vulnérabilités zero-day et investissent des ressources importantes pour les découvrir, les conserver et les exploiter. Néanmoins, jusqu'à récemment, ceci a généralement eu lieu en l'absence d'un processus

[10] GFCE, "Coordinated Vulnerability Disclosure", 2016, https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking.

« permettant d'envisager de façon adéquate les avantages et désavantages ».[11] Les groupes d'attaquants utilisent ces codes d'exploitation pour lancer un large éventail d'opérations, qui entraînent des perturbations de plus en plus importantes ayant des répercussions négatives pour l'économie mondiale et contribuant à accroître les tensions entre les États.[12] Cependant, d'après plusieurs sources, le nombre de Zero-days aurait chuté depuis 2017, prétendument en raison d'une réduction du nombre de vulnérabilités disponibles. En revanche, cela n'a pas globalement mis fin aux activités malveillantes ciblées.[13]

Rançongiciels (et attaques d'effaceurs des données (wiper) déguisés en rançongiciels)

En termes simples, les attaques de rançongiciels utilisent une cryptographie avancée pour verrouiller l'appareil d'un utilisateur et l'empêcher d'accéder à ses données jusqu'à ce qu'une rançon soit payée. En revanche, les attaques d'effaceurs de données ne visent généralement pas à engendrer des retombées financières, mais visent plutôt à effacer définitivement les données présentes sur un appareil sous couvert d'un rançonnage informatique. Les attaques de rançongiciels existent depuis un certain temps même si l'attaque Locky de 2016 a reçu une attention toute particulière car elle a permis d'extraire une rançon de 17 000 USD d'un hôpital aux États-Unis. De plus, les concepteurs du programme malveillant Locky l'ont régulièrement mis à jour pour éviter d'être détectés, et ont inclus des fonctionnalités innovantes comme des capacités de demande de rançon multilingues. L'envergure, l'ampleur et les effets des attaques de rançongiciels ont augmenté en 2017, comme le montrent les attaques très médiatisées Petya et WannaCry.

WannaCry a été particulièrement féroce, ciblant les vulnérabilités des systèmes d'exploitation Microsoft Windows en chiffrant les données et demandant des rançons en Bitcoin, une cryptomonnaie. Ce rançongiciel utilisait deux codes d'exploitation puissants : EternalBlue et DoublePulsar. Le premier, EternalBlue, fait référence à un code d'exploitation créé par l'Agence Nationale de Sécurité des États-Unis (NSA), qui a fuité à la suite d'un détournement de données plus tôt en 2017.[14] Ce code d'exploitation était conçu pour tirer profit d'une vulnérabilité découverte (et non signalée) par la NSA dans

[11] K. Charlet, S. Romanosky and B. Thomson, "It's Time for the International Community to Get Serious about Vulnerability Equities", lawfareblog.com, 15 novembre 2017, https://www.lawfareblog.com/its-time-international-community-get-serious-about-vulnerability-equities; P. Stockton and M. Golabek-Goldman, "Curbing the Market for Cyber Weapons", *Yale Law and Policy Review*, vol. 32, no. 1, 2013.

[12] Par exemple, le Conseil économique américain a chiffré l'impact de la cyberactivité malveillante sur l'économique américaine à entre 57 milliards USD et 107 milliards USD en 2016 ; voir "The Cost of Malicious Cyber Activity to the US Economy", février 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[13] ENISA, *Threat Landscape Report 2018*, 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018; Symantec, "2019 Internet Security Threat Report", https://www.symantec.com/security-center/threat-report.

[14] A. Greenberg, "The Untold Story of NotPetya, The Most Devastating Cyberattack in History', *Wired*, 22 août 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

un protocole spécifique de Windows, le protocole Server Message Block, donnant aux hackers « carte blanche pour exécuter leur propre code à distance sur n'importe quelle machine n'ayant pas fait l'objet d'un correctif ».[15] L'autre outil, Double Pulsar, est un implant de porte dérobée également créé par la NSA qui a été utilisé pour installer et exécuter le code du rançongiciel.

Microsoft avait publié des correctifs pour ces vulnérabilités avant même la propagation des codes d'exploitation, mais un grand nombre des organisations affectées ne les avaient pas encore appliqués ou utilisaient des systèmes Windows piratés ou obsolètes. Dans certains cas, par exemple au sein des sociétés fiduciaires du système national de santé britannique, l'assistance étendue convenue avec Microsoft en 2014 pour les utilisateurs d'XP avait expiré en 2015, laissant de nombreuses machines sans prise en charge.[16] Dans d'autres cas, les « portes dérobées » installées par le code d'exploitation Double Pulsar sapèrent les efforts d'atténuation.

L'attaque NotPetya de 2017 est le meilleur exemple connu d'une attaque d'effaceur de données (wiper). Utilisant une variante du rançongiciel Petya, le logiciel malveillant impliqué dans l'attaque NotPetya fut propagé par deux exploitations de vulnérabilité très puissantes : le même code d'exploitation EternalBlue utilisé dans l'attaque WannaCry, combiné à un code d'exploitation voleur d'identifiants intitulé Mimikatz. Le code d'exploitation Mimikatz avait été créé comme démonstration de faisabilité par un chercheur français en matière de sécurité pour démontrer les failles relatives aux mots de passe des systèmes Windows. Ce dernier pouvait être utilisé pour extraire des mots de passe de la mémoire vive (RAM) des ordinateurs et les utiliser pour pirater d'autres machines, dont des réseaux multiutilisateurs utilisant les mêmes informations d'identification.[17] Cela donnait la possibilité aux attaquants « d'infiltrer une cible, d'exfiltrer une quantité considérable de données, de chiffrer les données d'origine, et de conserver les données volées pour les échanger contre une rançon plus importante ».[18] NotPetya s'est effectivement amélioré par rapport à la capacité du rançongiciel d'origine Petya en ce qui concerne le chiffrage du Master Boot Record en chiffrant également la Master File Table et en supprimant la clé de chiffrement. Dans les faits, cela a transformé le rançongiciel en « effaceur de données », en lui permettant d'écraser puis finalement d'effacer le disque dur du système affecté. En ciblant un logiciel de comptabilité ukrainien légitime comme point d'entrée, exfiltrant les informations d'identification des utilisateurs et du Server Message Block à partir de l'hôte infecté et s'en servant pour se connecter à d'autres systèmes du réseau, le programme malveillant s'est rapidement propagé dans

[15] Ibid.
[16] S. Trendall, "NHS £150m Microsoft deal will banish Windows XP", PublicTechnology.Net, 22 mai 2018, https://www.publictechnology.net/articles/news/nhs-£150m-microsoft-deal-will-banish-windows-xp.
[17] Ibid.
[18] Trend Micro, "Midyear Security Roundup: The Cost of Compromise", 2017, https://documents.trendmicro.com/assets/rpt/rpt-2017-midyear-security-roundup-the-cost-of-compromise.pdf.

les réseaux d'entreprises pour déployer sa charge malveillante, ce qui entraîna des coûts rédhibitoires pour des sociétés du monde entier.[19]

Le nombre d'attaques de rançongiciels a supposément diminué en 2018, laissant place à de nouvelles menaces comme le *cryptojacking* (minage de cryptomonnaie clandestin).[20]

Attaques de chaîne d'approvisionnement

La chaîne d'approvisionnement du marché informatique est complexe, impliquant logiciels et matériels informatiques, mais aussi les personnes et les organisations qui gèrent la conception, la production, la livraison, l'installation et la maintenance des produits et services. La chaîne d'approvisionnement mondiale, longue et complexe, présente un large éventail d'opportunités pour l'insertion de programmes malveillants, et cela devient exponentiellement plus complexe avec les systèmes interconnectés et imbriqués de l'Internet des objets (IdO).[21]

Les attaques de chaîne d'approvisionnement logicielle sont à la hausse, Symantec ayant signalé une augmentation de 78 pourcent pour la seule année 2018.[22] Ces types d'attaques « compromettent les codes des logiciels par l'intermédiaire de cyberattaques, de menaces internes et d'autres activités à accès restreint à n'importe quelle phase de la chaîne d'approvisionnement pour infecter un client peu méfiant ».[23] Dans leur forme la plus simple, leur objectif est de modifier le codebase de confiance du produit pour insérer un programme malveillant au début du cycle avant que le code ne soit compilé ou signé électroniquement,[24] ou de corrompre le site de correctifs d'un fournisseur avec un programme malveillant conçu pour emprunter l'identité des codes de correctifs autorisés (incluant les mises à jour de sécurité), trompant ainsi dans la plupart des cas les programmes antivirus et anti-logiciels malveillants. Une fois inséré, le programme malveillant sert généralement de base pour la mise en place d'autres codes d'exploitation capables de manipuler un grand nombre d'ordinateurs (et leurs processus et produits) avec une seule attaque.[25]

---

[19] Symantec, "2019 Internet Security Threat Report", https://www.symantec.com/security-center/threat-report. Voir également "NotPetya Technical Analysis", LogRythm Labs, juillet 2017, https://logrhythm.com/pdfs/threat-intelligence-reports/notpetya-technical-analysis-threat-intelligence-report.pdf.

[20] ENISA, *Threat Landscape Report 2018*, 2019, voir la p. 115 pour visualiser le contexte des menaces actuelles, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[21] Lloyd's, "Networked World: Risks and Opportunities in the Internet of Things", https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world.

[22] Symantec, "Internet Security Threat Report", 2019, https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf?aid=elq_19296.

[23] NIS CSIRT, "Supply Chain Attacks", https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf.

[24] Ibid.

[25] Ibid.

Les développeurs de logiciel sont une source essentielle d'attaques de chaîne d'approvisionnement, en cela que les attaquants « volent les informations d'identification pour les outils de contrôle de version » ou « compromettent des bibliothèques tierces qui sont intégrées dans des projets logiciels de plus grande envergure ».[26] Ces types d'attaques sont utilisées pour l'extorsion, ou pour exfiltrer, manipuler et détruire des données à des fins stratégiques ou criminelles.

Au-delà des logiciels, les attaquants peuvent aussi cibler l'infrastructure physique des TIC comme les microprocesseurs et routeurs pendant le processus de fabrication, en installant des processeurs clandestins ou des codes d'exploitation qui deviennent difficiles à détecter plus loin dans la chaîne d'approvisionnement parce que le matériel informatique a été signé électroniquement par le fabricant. Des responsables américains ont affirmé pendant plusieurs années que le gouvernement chinois a installé des processeurs de surveillance sur le matériel de TIC vendu par ses principales grandes sociétés ; certains suggèrent que la NSA a probablement fait a probablement fait pareil.[27]

De plus, de récents rapports sur une campagne à grande échelle visant à installer des portes dérobées matérielles sur des serveurs assemblés en Chine et à destination d'une société américaine[28] illustrent une inquiétude croissante à l'échelle mondiale concernant les menaces qui pèsent sur l'intégrité de la chaîne d'approvisionnement. Même si les rapports des médias étaient controversés et démentis officiellement aussi bien par les victimes que les auteurs allégués,[29] ces informations ont tout de même causé de véritables ondes de choc pour les marchés informatiques et eu un impact négatif sur le cours des actions des sociétés de technologie chinoises dû à la peur qu'elles ne perdent leur accès aux marchés américains.[30] Les allégations actuelles affirmant que l'équipement mobile 5G développé par le géant des télécommunications chinois Huawei pourrait être utilisé par le gouvernement chinois à des fins d'espionnage ont intensifié les débats sur la résilience et la sécurité de la chaîne d'approvisionnement.[31]

---

[26] Ibid.

[27] G. Greenwald, "How the NSA Tampers with US-made Internet Routers', *The Guardian*, 12 mai 2014, https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

[28] J. Robertson and M. Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", *Bloomberg*, 4 octobre 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[29] G. Faulconbridge and J. Menn, "UK Cyber Security Agency Backs Apple, Amazon China Hack Denials", *Reuters*, 5 octobre 2018, https://www.reuters.com/article/us-china-cyber-britain/uk-cyber-security-agency-backs-apple-amazon-china-hack-denials-idUSKCN1MF1DN; BBC News,"Amazon and Apple Deny China Hack Claims", 5 octobre 2018, https://www.bbc.com/news/technology-45757531.

[30] The Straits Times,"Chinese Tech Firms' Shares Dive after 'Spy Chip' Report", 6 octobre 2018, https://www.straitstimes.com/business/companies-markets/chinese-tech-firms-shares-dive-after-spy-chip-report.

[31] R. Cellan-Jones, "Huawei and 5G: Decision Time", *BBC News*, 8 février 2019, https://www.bbc.com/news/technology-47160725.

Attaques de routage

Le routage IP (Internet Protocol) sous-tend Internet et joue un rôle central dans son bon fonctionnement. Le routage assure « que les courriels parviennent aux bons destinataires, que les sites d'e-commerce restent opérationnels, que les services gouvernementaux en ligne continuent de servir les citoyens ».[32] Toutefois, malgré le nombre de bonnes pratiques ayant émergé en matière de routage, la sécurité du routage reste un défi majeur. L'étendue et l'ampleur des incidents de routage augmentent chaque année, ce qui cause d'importants préjudices économiques.[33]

Le type d'incident de routage le plus commun implique des attaques contre des services Internet, et plus particulièrement des attaques de détournement de Protocole de passerelle frontière (BGP).[34] Le détournement de BGP permet de fausser le sens du trafic Internet, de le surveiller, de l'intercepter, de le diriger vers un « trou noir » (une adresse qui ne mène nulle part), ou de le diriger vers de faux sites Web dans le cadre d'une attaque de l'homme du milieu[35]. Le détournement de BGP, ou le réseau d'un système autonome qui pratique le détournement de BGP, peut aussi être utilisé pour usurper des adresses IP légitimes à des fins d'hameçonnage pour faire fuiter ou voler des données.

Pour la seule année 2017, l'Internet Society a signalé près de 14 000 attaques ou pannes liées au routage comme des fuites ou des détournements du routage.[36] Certaines de ces attaques ont aussi affecté la technologie chiffrée. Par exemple, le code d'exploitation Enthralled découvert en avril 2018 a détourné un certificat SSL non sécurisé pour rediriger les utilisateurs d'Ethereum vers un serveur qui vidait leur porte-monnaie chiffré.[37] Les attaques de routage peuvent aussi être utilisées à des fins de botnetting où de nombreux appareils connectés à Internet sont détournés et coordonnés pour effectuer une tâche spécifique, incluant des attaques par Déni de Service Distribué. En effet, en 2018, Akamai, le réseau de diffusion de contenu et fournisseur de services cloud, a signalé que la vulnérabilité EternalBlue était désormais utilisée pour compromettre près de 45 000 routeurs. Les attaquants avaient apparemment compromis les routeurs en « ciblant les mises en œuvres vulnérables de Universal Plug and Play (UPnP), un protocole largement utilisé [et largement piraté] qui permet aux appareils de reconnaître automatiquement les

---

[32] The Internet Society, "Routing Security for Policy Makers: An Internet Society White Paper", octobre 2018, https://www.internetsociety.org/wp-content/uploads/2018/10/Routing-Security-for-Policymakers-EN.pdf.

[33] Ibid.

[34] Le BGP régit le routage des communications à travers différents systèmes autonomes (c.-à-d., un large réseau ou groupe de réseaux géré par une seule organisation) en permettant au trafic de voyager d'une adresse réseau à l'autre aussi efficacement que possible.

[35] Les attaques homme-au-milieu sont une forme courante de cyberattaque permettant aux attaquants d'écouter ou de modifier des communications légitimes entre deux hôtes.

[36] A. Robachhevsky, "14,000 Incidents: A 2017 Routing Security Year in Review", Internet Society, 9 janvier 2018,https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/.

[37] Microsoft, "The Cybersecurity Tech Accord Endorses the MANRS Initiative, Joining Efforts to Eliminate the Most Common Threats to the Internet's Routing System", 9 août 2018, https://cybertechaccord.org/cybersecurity-tech-accord-endorses-manrs/.

autres appareils d'un réseau local », infectant ainsi des centaines de milliers d'appareils. L'objectif de l'attaque n'était pas clair, mais les chercheurs redoutaient que les routeurs puissent être utilisés pour des attaques de rançongiciels ou pour obtenir « une implantation persistante dans le réseau » en vue d'une exploitation future.[38]

Les rapports de l'année 2019 mettront probablement en évidence la récente tendance à des attaques de détournement du Système d'adressage par domaines (DNS) à des fins d'espionnage. ICANN (l'organisme international multipartite responsable de la coordination du DNS d'Internet, des adresses IP et des numéros de systèmes autonomes), le gouvernement américain et plusieurs sociétés privées ont émis des avertissements en février 2019 concernant une menace d'espionnage très sérieuse liée aux systèmes DNS. Selon certaines sources, les attaquants avaient détourné des serveurs DNS utilisés par des gouvernements et des sociétés privées, redirigeant un grand nombre de courriels sensibles et de trafic VPN vers une adresse Internet sous leur contrôle. Comme l'a fait remarquer le chercheur Brian Krebs, les détournements de DNS ont aussi permis aux attaquants d'obtenir des certificats de chiffrage SSL pour les domaines ciblés, ce qui leur a ensuite permis de « décrypter les informations d'identification des VPN et courriels interceptés afin de les visualiser sous forme de texte ». Les chercheurs en sécurité ont associé la « Campagne de DNSpionage » a des pirates iraniens. D'après l'ICANN, des efforts d'atténuation de la menace ont été difficiles à mettre en œuvre car l'infrastructure DNS est « rarement surveillée en vue de modifications suspectes » et que les organisations ne suivent presque jamais les bonnes pratiques qui rendraient l'infrastructure DNS ou les domaines ciblés beaucoup plus difficiles à détourner.[39]

Attaques liées à l'IdO

L'Internet des objets fait référence à un vaste ensemble d'appareils connectés à Internet, du simple capteur aux smartphones, appareils ménagers et « prêt-à-porter électronique», collectant des données et utilisant ces données pour fonctionner à travers différents produits et services. [40] Les attaques IdO peuvent être analysées selon différentes perspectives. Par exemple, elles peuvent être liées à des attaques réseaux qui utilisent différents outils pour exploiter les vulnérabilités des appareils en réseau IdO, afin de les mettre hors ligne ou de les réunir en botnets pour attaquer d'autres cibles. Ces types

[38] Akamai, "UPnProxy: EternalSilence", 28 novembre 2018, https://blogs.akamai.com/sitr/2018/11/upnproxy-eternalsilence.html.
[39] "Deep Dive on the Recent Widespread DNS Hijacking Attacks", février 2019, https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/.
[40] M. Burgess, "What is the Internet of Things? Wired Explains", *Wired*, 16 février 2018, https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot; voir aussi Lloyd's, "Networked World: Risks and Opportunities in the Internet of Things", https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world.

d'attaques sont généralement associés à une manipulation ou perturbation du trafic du réseau.

Prenons, par exemple, le programme malveillant Mirai qui infecte les appareils intelligents utilisant certains processeurs. Ce botnet qui s'autopropage est l'un des virus IdO les plus connus et il continue d'affecter des appareils dans le monde entier Le botnet a « asservi » de nombreux types d'appareils IdO piratés (routeurs, caméras de sécurité et enregistreurs vidéo numériques) vulnérables au piratage à cause de mots de passe faibles, par défaut ou fixes.[41] Si l'attaque initiale de 2016 a pu être stoppée, le code source a été diffusé publiquement et certains de ses éléments utilisés lors d'autres attaques de botnet, dont l'attaque massive ayant entraîné l'effondrement du prestataire de services d'enregistrement de domaines, Dyn, seulement quelques mois plus tard. Selon Symantec, les groupes d'attaquants ont depuis lors développé de nombreuses variantes de Mirai et « ajoutent continuellement de nouveaux codes d'exploitation pour augmenter le taux de succès des infections, car les appareils sont encore bien souvent dépourvus de correctif ».[42] La découverte ultérieure d'un programme malveillant VPNFilter en 2018, et de modèles subséquents (p. ex. Ssler) en disent long sur l'ampleur et le caractère changeant des perturbations qui peuvent être générées par des vulnérabilités et menaces liées à l'IdO.[43]

D'autres types d'attaques IdO incluent celles qui ciblent les systèmes utilisant des IdO avec assistance cloud de contrôle et d'acquisition de données (SCADA) ou de contrôle industriel (ICS) de différentes installations, de systèmes de fabrication et d'ingénierie ou d'objets d'infrastructure. Ceux-ci sont de plus en plus connectés à Internet, et de façon prédominante via des solutions basées sur l'IdO. De telles activités dépassent la simple perturbation du réseau et, dans un nombre croissant de situations, convergent vers des attaques cyber-physiques. [44] Indubitablement, la numérisation presque totale des systèmes de contrôle de processus des infrastructures essentielles continuera à être problématique. Fours, systèmes de refroidissement, centrifugeuses, feux de signalisation du contrôle aérien, génératrices électriques et bien d'autres systèmes essentiels fonctionnent désormais à l'aide de systèmes numériques. Avec des TIC numériques interconnectés, efficaces et intelligents, la convergence de menaces cyber-IdO est désormais évidente au niveau du contrôle des processus puisque des cyberattaques

---

41 "KrebsOnSecurity Hit with Record DDoS", 21 septembre 2016, *https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/*.

[42] Symantec, "Internet Security Threat Report", 2019, https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf?aid=elq_19296

[43] D'après Symantec, VPNFilter est la « première menace IdO persistante à s'être largement répandue ». Celle-ci a affecté plus de 500 000 routeurs à travers 54 pays et inclut un certain nombre de « charges puissantes ». Symantec, "Internet Security Threat Report", 2019, p. 20, https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf?aid=elq_19296.

[44] Voir C. Greer et al., "Cyber-Physical Systems and Internet of Things", NIST, 2019, https://www.nist.gov/publications/cyber-physical-systems-and-internet-things; voir aussi Y. Pa et al., "Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems", *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. 3, 2017.

ciblant des appareils IdO peuvent générer des effets physiques réels. , ce qui étend grandement la surface d'attaque, au fur et à mesure que de nouvelles vulnérabilités sont identifiées pour une exploitation potentielle.

Exploitation de défaut de conception

En janvier 2018, des chercheurs universitaires et en sécurité ont découvert deux vulnérabilités, Spectre et Meltdown, permises par des défauts de sécurité sous-tendant la technique d'exécution spéculative utilisée par plusieurs processeurs issus de fabricants de premier ordre comme Intel, AMD et ARM.[45] Meltdown, une vulnérabilité de sécurité qui « fait tout simplement fondre les limites de sécurité normalement appliquées par le matériel informatique », a affecté des ordinateurs de bureau, ordinateurs portables et ordinateurs de cloud.[46] Spectre, quant à lui, « brise la séparation entre différentes applications, permettant à un attaquant de tromper les programmes exempts d'erreur en leur faisant suivre les meilleures pratiques pour faire fuiter leurs secrets ».[47] Il a également affecté des ordinateurs de bureau, ordinateurs portables et ordinateurs de cloud, rendant vulnérables presque tous les processeurs modernes.[48] Ces vulnérabilités permettraient le détournement de tous types de données traitées par ordinateur ou système connexe. De nombreux correctifs logiciels initialement déployés par les fabricants de processeurs donnèrent naissance à des problèmes de performance, affectant à nouveau ordinateurs et systèmes du monde entier.

Ce qui est sans précédent avec ces vulnérabilités est qu'elles ont collecté des données sensibles à partir de dispositifs informatiques « fonctionnant comme prévu », plutôt que par l'exploitation de failles ou vulnérabilités des matériels ou logiciels informatiques.[49] En d'autres termes, c'est la conception même de la technologie d'exploitation qui était défaillante. En effet, les recherches en cours ont révélé des faiblesses sécuritaires de base dans la manière dont les processeurs ont été conçues au cours des deux dernières décennies. Par exemple, début 2019, des chercheurs ont découvert une nouvelle défaillance, Spoiler, qui affectait tous les processeurs Intel. Comme Spectre, la défaillance pouvait potentiellement être utilisée pour abuser de la technique d'exploitation spéculative utilisée par les processeurs Intel, même si Intel a insisté sur le fait que Spoiler

[45] L'exécution spéculative est la pratique qui permet aux processeurs d'effectuer une opération anticipée pouvant se révéler nécessaire ou non en fonction de l'achèvement d'un autre calcul ; L. Hay Newman, "The Elite Intel Team Still Fighting Meltdown and Spectre", *Wired,* 3 janvier 2019, https://www.wired.com/story/intel-meltdown-spectre-storm.
[46] Voir https://meltdownattack.com/.
[47] Ibid.
[48] L. Hay Newman, "The Elite Intel Team Still Fighting Meltdown and Spectre", *Wired,* 3 janvier 2019, https://www.wired.com/story/intel-meltdown-spectre-storm; voir aussi C. Williams, "Kernel-memory-leaking Intel Processor Design Flaw Forces Linux, Windows Redesign," *The Register*, 2 janvier 2018, https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/.
[49] Intel, "Intel Responds to Security Research Findings", 3 janvier 2018, https://newsroom.intel.com/news/intel-responds-to-security-research-findings/#gs.AbK4rdO7.

ne révèle pas de données comme les mots de passe. Cependant, il est inquiétant de constater que Spoiler ouvre apparemment la porte à d'autres techniques d'attaques de type « fuite de mémoire » et, surtout, aux attaques par canal auxiliaire.[50] Ces vulnérabilités ont non seulement déclenché un investissement massif visant la découverte d'autres vulnérabilités, mais également un examen fondamental de la façon dont les processeurs sont conçus.

[50] L. Tung, “Intel Finally Issues Spoiler Attack Alert: Now Non-Spectre Exploit Gets CVE But No Patch”, *ZDnet*, 10 avril 2019, https://www.zdnet.com/article/intel-finally-issues-spoiler-attack-alert-now-non-spectre-exploit-gets-cve-but-no-patch/.

DYNAMIQUES FAVORISANT LA DIFFUSION DE TECHNIQUES ET D'OUTILS DE TIC MALVEILLANTS

L'existence de ces menaces et vulnérabilités et des techniques et outils employés pour les exploiter a été, et reste, très difficile à gérer (voire à prévenir) à cause de dynamiques interdépendantes complexes qui résident au cœur de l'élaboration des politiques publiques.

La dynamique fondamentale est la dépendance toujours croissante de la société vis-à-vis du cyberespace et de l'Internet pour la plupart des aspects de la vie économique, sociale et politique alors que d'importants changements ont lieu dans l'ordre international. En juin 2018, le nombre d'utilisateurs d'Internet s'élevait à 4,2 milliards, soit 55 % de la population mondiale (avec une croissance future concentrée dans les pays où les ressources et la capacité en cybersécurité sont faibles).[51] Le rôle central des TIC/du cyberespace comme support de la vie politique, sociale et économique mondiale a cependant attiré l'intérêt de nombreux acteurs criminels cherchant à profiter de nouvelles opportunités, mais aussi des acteurs étatiques, plus particulièrement parmi les grandes puissances, qui utilisent leurs capacités en TIC pour prendre l'avantage dans la compétition qui les oppose les uns aux autres. Entre les deux, on retrouve les sociétés privées qui développent et bénéficient de l'Internet et des autres marchés informatiques et dont les modèles d'affaires, à quelques exceptions près, ont tendance à renforcer et favoriser l'insécurité, transférant les risques en aval, aux utilisateurs de leurs produits.

Dynamiques criminelles et du marché noir

Les acteurs criminels ont toujours été des pionniers dans l'utilisation des technologies de l'information et ils y excellent toujours.[52] Le marché de la cybercriminalité, qui vit de l'échange de techniques et d'outils malveillants, est apparemment prospère, puisqu'il occupe la troisième place en valeur dollars à l'échelle mondiale, derrière des activités illicites comme la corruption gouvernementale et le trafic de narcotiques.[53] Un rapport de McAfee et du Center for Strategic and International Studies (CSIS) a évalué que le coût annuel de la cybercriminalité a augmenté jusqu'à 600 milliards USD (0,8 %) du GDP mondial en 2017, alors qu'il se trouvait à 500 milliards USD en 2014.[54] En plus, près de 2

[51] Voir https://www.internetworldstats.com/stats.html; voir aussi UN News, "Internet Milestone Reached, As More Than 50 Per Cent Go Online: UN Telecoms Agency", 7 décembre 2018,https://news.un.org/en/story/2018/12/1027991.

[52] C. Kavanagh, "IT and Cyber Capabilities as a Force Multiplier for Transnational Crime", dans V. Comolli (ed.), *Organized Crime and Illicit Trade: Responding to Strategic Challenges in Old and New Domains*,2018.

[53] G. Gross, "The Cost of Cybercrime", Internet Society, 25 février 2018, https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/; voir aussi J.A. Lewis, "Economic Impact of Cybercrime: Not Slowing Down", McAfee et CSIS, 2018.

[54] Ibid.

milliards d'individus ont vu leur informations personnelles subtilisées ou compromises, et un beaucoup plus grand nombre leur vie privée violée.

D'énormes profits, des risques faibles et une publicité gratuite catalysent la professionnalisation et la croissance des services criminels offerts, ainsi que l'expansion de centres de ventes dans diverses régions, pour la plupart connectés aux groupes mafieux et du crime organisé existants.[55] Cet univers illégal en ligne et hors ligne permet aux acteurs d'échanger des informations et des idées sur les cibles potentielles, de développer, d'acheter, de vendre ou de déployer des programmes malveillants, des codes d'exploitation de vulnérabilité ou des outils de contournement et d'assombrissement, de fournir des services allant de tâches spécialisées (conception de faux site web, piratage de mot de passe) à la sous-traitance (recrutement de pirates informatiques, botnet à louer, attaques en déni de service distribué comme service) d'activités de déstabilisation plus complexes, et d'acheter et vendre des ressources numériques, des données personnelles et des informations d'identification.[56] Ces acteurs criminels « échangent des informations et modèles commerciaux, et s'affrontent pour fournir et accéder à des services », ils s'appuient donc de plus en plus sur les lacunes réglementaires qui entourent les technologies blockchain pour monétiser leur activité.[57]

La publicité qui entoure les attaques de grande notoriété et leur valeur ont aussi servi de formidable outil de marketing pour les acteurs criminels. Prenons, par exemple, le marché Zero-day : même si en 2007 les professionnels de la sécurité avaient du mal à trouver des acheteurs pour les Zero-day qu'ils découvraient, en 2012 des rapports médiatiques dressant le portrait de pirates informatiques vendant des Zero-days dans la clandestinité d'Internet amena cette pratique au centre de l'attention.[58] Des rapports ont aussi révélé la grande valeur des Zero-days.

La tendance de prix croissants documentée au fil de la décennie (voir le Tableau 1) a continué d'évoluer. Pour illustrer cela, en janvier 2019, ArsTechnica a signalé « une plus grande demande en ce qui concerne des codes d'exploitation capables de sérieusement compromettre des applications ou des appareils sans que l'utilisateur ciblé ne s'en

---

[55] *UNIDIR,* "*Preventing and Mitigating ICT-Related Conflict: Cyber Stability Conference 2018 Summary Report",* *http://unidir.org/files/publications/pdfs/preventing-and-mitigating-ict-related-conflict-cyber-stability-conference-2018-summary-report-en-724.pdf*

[56] J. Friedmann and M. Bouchard, "The Definitive Guide to Cyber Threat Intelligence: Using Knowledge About Adversaries to Win the War Against Targeted Attacks", ISight Partners, 2015, https://cryptome.org/2015/09/cti-guide.pdf.

[57] UNIDIR, "Preventing and Mitigating ICT-Related Conflict: Cyber Stability Conference 2018 Summary Report"; voir aussi Digital Shadows, "A Tale of Epic Extortions: How Cybercriminals Monetize Our Online Exposure", https://resources.digitalshadows.com/whitepapers-and-reports/a-tale-of-epic-extortions-how-cybercriminals-monetize-our-online-exposure.

[58] C. Miller, "The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales" Workshop on the Economics of Information Security, 2007; A. Greenberg, "Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)", *Forbes*, 21 mars 2012.

aperçoive ».[59] Le leader du courtage en codes d'exploitation, Zerodium, vient tout juste d'offrir 2 millions USD pour des jailbreaks sans intervention de l'utilisateur (zero click) pour iOS d'Apple, 1,5 millions USD pour des jailbreaks en un click pour iOS sans intervention de l'utilisateur et 1 million USD pour des codes d'exploitation qui prennent le contrôle des applications de messagerie WhatsApp et iMessage. Zerodium a également annoncé une augmentation importante des coûts d'un certain nombre d'autres codes d'exploitation, dont certains se trouvent dans la liste ci-dessus.[60]

Tableau 1. Dynamiques du Marché Zero-Day[61]

Service	Prix par vulnérabilité zero-day	Année
Microsoft Excel	> 1 200 $	2007
Mozilla	500 $	2007
Code d'exploitation Vista	50 000 $	2007
Code d'exploitation Windows Metafile	4 000 $	2007
Adobe Reader	5 000 $ - 30 000 $	2012
Android	30 000 $ - 60 000 $	2012
Chrome ou Internet Explorer	80 000 $ - 200 000 $	2012
iOS	100 000 $ - 250 000 $	2012
Microsoft Word	50 000 $ - 100 000 $	2012
Windows	60 000 $ - 120 000 $	2012
WeChat	500 000 $	2018
Facebook Messenger	500 000 $	2018
Apple iPhone	Jusqu'à 1 500 000 $	2018

Le chercheur en sécurité Bruce Schneier, qui s'inquiète de ces évolutions, a prédit que la hausse du marché des zero-days aurait des conséquences négatives pour la sécurité logicielle, en plombant les pratiques émergeantes dans le domaine de la recherche en sécurité.[62] Lorsque des chercheurs indépendants découvraient des vulnérabilités, ils pouvaient s'attendre à être récompensés par une certaine notoriété, ce que l'on appelle une « prime au bogue » (rémunération du chasseur de bogues), ou dans certains cas nu rôle de conseil ou un poste dans la société propriétaire du produit vulnérable. Dans chacun de ces cas, la vulnérabilité elle-même était en fin de compte corrigée et sécurisée. En contrepartie, le marché des zero-days a favorisé une tendance à récompenser la non divulgation: les chercheurs qui trouvaient des vulnérabilités étaient mieux récompensés

[59]D. Goodin, "Zeroday Exploit Prices Are Higher than Ever, Especially for iOS and Messaging Apps", *ArsTechnica*, 8 janvier 2019, https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/.

[60]Le jailbreaking fait référence à l'augmentation de droits d'accès dans le but de retirer toutes les restrictions de logiciel imposées par Apple sur appareils iOS. En ce qui concerne la recrudescence d'exploits zero-day, voir ibid.

[61] Tableau développé par Evgeny Scherbakov. Voir L. Ablon, M. Libicki and A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar", RAND Corporation, 2014; Zerodium, https://zerodium.com; and K. Huang, M. Siegel, and S. Madnick, "Systematically Understanding the Cyber Attack Business: A Survey", Cybersecurity Interdisciplinary Systems Laboratory, Sloan School of Management, MIT, July 2018, http://web.mit.edu/smadnick/www/wp/2018-08.pdf.

[62] B. Schneier, "The Vulnerabilities Market and the Future of Security", *Forbes*, 30 mai 2012.

par les acheteurs (sociétés, gouvernements, ou acteurs du darknet) qui collectionnent souvent les vulnérabilités plutôt que de les divulguer ou de les sécuriser, puisque cela fait évidemment monter leur prix. Cela était apparemment le cas avec la vulnérabilité EternalBlue qui, selon Microsoft, n'a été divulguée par la NSA qu'après qu'elle ait fuité (avec d'autres codes d'exploitation de vulnérabilité de la NSA).[63] Il ne fait aucun doute que d'autres gouvernements utilisent (ou cherchent à utiliser) les zero-days, même si dans certains cas on note une évolution vers une utilisation plus responsable par l'intermédiaire d'une divulgation coordonnée de vulnérabilités ou la mise en place de processus nationaux d'évaluation et de gestion des vulnérabilités.[64] D'autres facteurs catalysant la flambée des prix des zero-days incluent le fait que les cibles deviennent plus difficiles à exploiter car une pression accrue pèse sur les sociétés en ce qui concerne la conception de produits plus sécurisés, et que la demande augmente du côté des agences gouvernementales également.

Dynamiques géopolitiques et des sécurités nationales

Les technologies de l'information ont toujours été perçues comme des composantes essentielles de la défense et de la sécurité des États, pour des communications sécurisées et la coordination des ressources militaires sur le terrain, la surveillance à distance des ressources et des capacités des autres États, et la collecte d'informations sur des adversaires potentiels. Aujourd'hui, les TIC et les infrastructures nationales et mondiales qu'elles soutiennent sont devenues des éléments essentiels de la puissance militaire, économique et politique, et donc des cibles stratégiques dans la compétition entre les États. Pendant près de trois décennies, cette compétition a été le moteur de trois changements majeurs dans la stratégie et la doctrine militaires. Aujourd'hui, il est évident que de nombreux États développent des capacités offensives dans lesquelles les techniques et les outils malveillants jouent un rôle central, et l'infrastructure critique (défense, énergie, finance, santé, informations), les institutions politiques et les processus comme les élections et les plateformes de média deviennent des cibles toujours plus attrayantes.

En ce qui concerne les vulnérabilités matérielles et logicielles évoquées ci-dessus, il devient de plus en plus évident que certains États utilisent des vulnérabilités et failles découvertes pour développer des codes d'exploitation à des fins de renseignement, de défense ou d'offensives plus actives au lieu de signaler immédiatement les vulnérabilités ou failles aux fournisseurs ou acteurs concernés. Les fuites Snowden ont confirmé ce

[63] Des exemples antérieurs de vulnérabilités non divulguées incluent le ver Conficker Microsoft et le code d'exécuà distance Welchia libérées dans la nature en 2008 et 2003, respectivement ; *Wired*,"The Leaked NSA Spy Tool that Hacked the World", 7 mars 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

[64] En ce qui concerne les processus d'évaluation et de gestion des vulnérabilités et la divulgation coordonnée des vulnérabilités, voir la note *supra* 11 et les notes 96 et 98 ci-dessous.

phénomène tout comme la plus récente exfiltration de données de la NSA qui a conduit au fuitage et au déploiement subséquent de ses codes d'exploitation de vulnérabilités.

Dans de nombreux cas, les États s'appuient sur les marchés noirs pour acheter des codes d'exploitation et autres techniques et outils malveillants ou pour engager les services d' intermédiaires criminels afin de les déployer.[65] Les Groupes d'experts gouvernementaux des Nations Unies travaillant sur les TIC et la sécurité internationale ont reconnu l'utilisation d'intermédiaires par les États « pour mettre en œuvre des actions TIC malveillantes », liant cet enjeu au droit international et à la question de la responsabilité des États.[66] Des allégations existent selon lesquelles d'autres États ont directement ou indirectement encouragé l'émergence de groupes spécialisés : des « cyber-mafias » ou des « pirates patriotes »—afin qu'ils fournissent des compétences offensives (p. ex. Russian Business Network), vendent et propagent des codes d'exploitation zero-day (p. ex. les Shadow Brokers), notamment à d'autres États ou acteurs parrainés par l'État, qu'ils servent de leurre ou qu'ils donnent l'impression d'un soutien populaire.

Les cyber-opérations soutenues ou dirigées par les États peuvent affecter l'infrastructure critique ou les services essentiels pour le public et avoir des coûts directs et indirects significatifs pour l'économie mondiale. L'attaque WannaCry qui, à l'époque, fut décrite comme l'une des « plus grandes perturbations cyber que le monde ait connu » a affecté sans discrimination quelques 300 000 ordinateurs à travers 150 pays.[67] Les usines de construction automobiles ont été forcées d'arrêter leur production tandis que les établissements de soins ont dû annuler des milliers de procédures et de rendez-vous médicaux. L'attaque WannaCry aurait couté près de 100 millions GBP au National Health Service britannique, en plus des coûts directs et indirects de 19 000 annulations de rendez-vous.[68] Des industries et services en Chine et en Russie ont aussi été fortement touchés. En tout, Trend Micro estime les pertes mondiales dues à l'attaque, « incluant la réduction de productivité afférente et les coûts de contrôle des dommages », à 4 milliards de dollars américains.[69] Des interrogations subsistent sur la façon dont sont calculés ces différents coûts et certains suggèrent que l'attaque a été plus dérangeante que coûteuse. Qu'elle ait été coûteuse ou simplement gênante, en décembre 2017 le gouvernement britannique a attribué l'attaque au groupe Lazarus soutenu par la République populaire

[65] Le Manuel de Tallin souligne qu'une cyberattaque menée par des acteurs ne relevant pas d'un État pourrait être attribuée à un État si ce dernier est considéré comme exerçant un « contrôle effectif » sur ceux-ci. Voir M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, p. 81.

[66] Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, 2013 (document A/68/98*, juin 2013, pp. 4, 6 and 8) et 2015 (document A/70/174, juillet 2015, p. 13).

[67] A. Greenberg, "The Untold Story of NotPetya, The Most Devastating Cyberattack in History', *Wired*, 22 août 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[68] D. Palmer, "This Is How Much the WannaCry Ransomware Attack Cost the NHS", *ZDnet*, 12 octobre 2018, https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/.

[69] Trend Micro, "2017 Midyear Security Roundup: The Cost of Compromise", https://documents.trendmicro.com/assets/rpt/rpt-2017-Midyear-Security-Roundup-The-Cost-of-Compromise.pdf.

démocratique de Corée (également blâmée pour le piratage de Sony Pictures en 2014).[70] Les États-Unis ont rapidement emboité le pas, suivis par l'Australie, le Canada, le Japon et la Nouvelle-Zélande.[71] Des procureurs américains ont plus tard inculpé un ressortissant de la République populaire démocratique de Corée pour son implication dans la création du logiciel rançonneur WannaCry (ainsi que pour son implication dans l'attaque antérieure de Sony).[72]

De la même manière, NotPetya, le virus effaceur de données évoqué plus haut, a mis hors service environ 10 pourcent du parc d'ordinateurs ukrainien et affecté le travail d'innombrables sociétés internationales, dont FedEx et Durex, ainsi que le géant pharmaceutique américain Merck, et la société de internationale de transport maritime Maersk qui furent apparemment les plus touchés.[73] Le principal défi posé par cette technique malveillante spécifique est sa capacité à chiffrer et effacer les disques durs de dizaines de milliers de systèmes informatiques, induisant des pertes pouvant s'élever à des centaines de millions en frais de réparation et opportunités commerciales perdues. Les sociétés de cybersécurité d'Europe de l'Est ont infirmé l'hypothèse initiale selon laquelle il s'agissait d'une attaque de rançongiciel d'origine criminelle, faisant plutôt le lien avec un groupe connu sous le nom de Sandworm (ou Telebots), qui avait été largement impliqué dans des cyber-opérations contre l'Ukraine.[74] En février 2018, le gouvernement américain a publiquement attribué l'attaque à l'agence du renseignement militaire de la Fédération de Russie, le GRU, indiquant que l'attaque « faisait partie des efforts soutenus du Kremlin visant à déstabiliser l'Ukraine... démontrant encore plus clairement l'implication de la Russie dans le conflit en cours ». L'attaque a eu des répercussions « en Europe, en Asie et aux Amériques, avec des dégâts à hauteur de plusieurs milliards de dollars ».[75] La Russie a nié toute responsabilité dans cette attaque.

Il est peu probable que ces tendances se dissipent. Selon certains rapports, en 2016, 30 États développaient des capacités cyber offensives, dans lesquelles les codes d'exploitation de vulnérabilité et autres techniques et outils malveillants jouent un rôle central. L'Australie, la France, l'Allemagne, le Royaume-Uni et les États-Unis ont depuis lors divulgué publiquement le développement de cybercapacités offensives à des fins de

[70] UK Government, "Foreign Office Minister Condemns North Korean Actor for WannaCry attacks", 19 décembre 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.
[71] White House, "Press Briefing on the Attribution of the Wannacry Malware Attack to North Korea", 19 décembre 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.
[72] Voir https://www.justice.gov/usao-cdca/press-release/file/1091951/download.
[73] *The Register*, "Nothing Could Protect Durex Peddler from NotPetya Ransomware", 6 juillet 2017, https://www.theregister.co.uk/2017/07/06/notpetya_reckitt_benckiser/.
[74] A. Greenberg, "The White House Blames Russia for NotPetya, The 'Most Costly Cyberattack in History'", *Wired*,15 février 2018, https://www.wired.com/story/white-house-russia-notpetya-attribution/.
[75] White House, "Statement from the Press Secretary", 15 février 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

défense nationale. Il est bien entendu présumé que toutes les puissances majeures et de nombreuses puissances intermédiaires travaillent dans la même direction.[76]

En réponse à l'activité malveillante persistante qui affecte leurs institutions et infrastructures nationales, les États-Unis sont passés à la vitesse supérieure, affirmant dans la cyberstratégie 2018 du Département de la Défense qu'ils « se défendraient en attaquant (« defend forward ») pour perturber ou interrompre les activités malveillantes à leur source, incluant les activités sont sous le seuil du conflit armé ».[77] Ils se sont aussi engagés (avec le Danemark, l'Estonie, les Pays-Bas et le Royaume-Uni) à utiliser leurs capacités cyber pour la défense collective de l'OTAN. Pour certains, ces développements doctrinaux favorisant l'attaque plutôt que la défense et la résilience sont providentiels et appropriés puisque les efforts existants pour promouvoir un comportement responsable et une plus grande retenue n'ont pas porté leurs fruits. Pour d'autres, cependant, ceux-ci posent les bases d'un « environnement conflictuel en ligne » plus déstabilisant, et peuvent rendre inefficaces les activités de mise en confiance diplomatiques et para-diplomatiques en cours.[78] De plus, un tel environnement requerra, en toute logique, un arsenal constant de techniques et d'outils malveillants, ce qui irait possiblement à l'encontre de l'engagement des États d'endiguer leur propagation, et saperait aussi le travail des sociétés, chercheurs et ingénieurs qui tendent à développer des services et des produits plus sécurisés.

Dynamiques du marché des technologies de l'information

Enfin, un certain nombre de dynamiques du marché des technologies de l'information sapent également la sécurité et la capacité à gérer (voire d'empêcher) la propagation de techniques et d'outils malveillants. Les experts ont décrit les ordinateurs et systèmes afférents comme « fondamentalement non sécurisés » de par leur conception même, particulièrement lorsqu'ils sont connectés en réseau. Ce problème est lié au fait que les sociétés et développeurs de technologie n'adhèrent pas aux principes scientifiques reconnus en matière de sécurité informatique datant des années 70, et à l'absence de moyens (en termes de politiques publiques) pour garantir leur adhésion. Des logiciels et matériels informatiques (actuels et obsolètes) hautement vulnérables, ainsi que des défauts fondamentaux de conception dans des composantes principales comme les processeurs, un faible niveau de sensibilisation de la part des fournisseurs de logiciels et des utilisateurs finaux des produits informatiques causent des problèmes exponentiels

[76] T. Uren, B. Hogeveen and F. Hanson, "Defining Offensive Cyber Capabilities", Australian Strategic Policy Institute, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities/.
[77] "Domain Trends", *The Military Balance*, vol. 119, no. 1; US Department of Defense, "Summary. Department of Defense Cyber Strategy 2018", https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[78] Ibid.; voir aussi UNIDIR,"Preventing and Mitigating ICT-Related Conflict: Cyber Stability Conference 2018 Summary Report", http://unidir.org/files/publications/pdfs/preventing-and-mitigating-ict-related-conflict-cyber-stability-conference-2018-summary-report-en-724.pdf; et J. Mallery, à venir en 2019.

lorsque ces technologies deviennent de plus en plus intégrées à de vastes systèmes interconnectés. Ces moteurs de vulnérabilité « se répandent à travers le secteur des biens d'équipement jusque dans les infrastructures critiques et les systèmes informatiques des entreprises et du gouvernement ».[79] La plupart du temps, les retombées de l'exploitation de leurs vulnérabilités affectent largement les tierces parties plutôt que ceux qui les commercialisent.

Ces défis sont exacerbés par la diversité et la complexité extrêmes des chaînes d'approvisionnement de logiciels et matériels informatiques. La structure du marché informatique actuel mondialisé, transnational et extrêmement compétitif signifie que l'intégration verticale complète des chaînes d'approvisionnement de systèmes informatiques est devenue impossible pour les fournisseurs ou les opérateurs. Une plus grande complexité des chaînes d'approvisionnement implique de plus grandes chances que des vulnérabilités existent dans le code des produits informatiques et rend l'audit complet des vulnérabilités plus difficile et chronophage.

Qu'est-ce qui pousse les entreprises de technologie à précipiter les produits sur le marché avant même qu'ils ne soient sécurisés de façon adéquate ? Ce phénomène s'explique par un certain nombre de facteurs. Le premier touche les enjeux de conception sécuritaire et s'explique aussi par la nature des systèmes d'exploitation et des langages de programmation utilisés. Selon un expert, si les entreprises concevaient des systèmes d'exploitation compétents (p. ex. une séparation de kernel et des langages de programmation à sûreté du typage), un grand nombre de problèmes persistants seraient éliminés dès la conception.[80] Néanmoins, le secteur « reste fidèle à des technologies fondamentales désuètes intrinsèquement non sécurisées ».[81] La rétrocompatibilité aux anciens codes base contribue à cette situation, ainsi qu'une main d'œuvre peu formée en matière de programmation sécurisée.

Les dynamiques de marchés des entreprises dominantes concourent à expliquer pourquoi les entreprises commerciales ont tendance à précipiter des produits non sécurisés sur le marché.[82] Ross Anderson et Tyler Moore ont identifié plusieurs caractéristiques des marchés de services et produits numériques qui favorisent le temps de mise sur marché au détriment de la sécurité.[83] Il y a tout d'abord les *effets de réseau*, selon lesquels la valeur d'un service est proportionnelle au nombre de ses utilisateurs, l'une des

[79] J. Mallery, à venir en 2019. Voir aussi la conférence de J. Mallery, "Cyber arms control: risk reduction under linked regional insecurity dilemmas", IISS, 10 septembre 2018, https://www.iiss.org/events/2018/09/cyber-arms-control
[80] Ibid.
[81] Ibid.
[82] L'OCDE définit une « entreprise dominante » comme une entreprise qui « occupe une part importante d'un marché donné et possède une part de marché bien plus grande que son rival le plus proche. Les entreprises dominantes sont généralement considérées comme ayant des parts de marché s'élevant à 40 % ou plus. » OCED Glossary of Statistical Terms, https://stats.oecd.org/glossary/detail.asp?ID=3199.
[83] R. Anderson and T. Moore, "Information Security Economics – and Beyond", dans A. Menzes (ed.), *Advances in Cryptology*, 2007, https://link.springer.com/chapter/10.1007/978-3-540-74143-5_5.

motivations principales qu'ont les entreprises de souhaiter revendiquer leur part du marché rapidement. Bien avant l'émergence d'Internet, les effets de réseau étaient centraux dans les stratégies d'entreprises comme celles de l'American Telephone and Telegraph company (AT&T), puisqu'ils ont permis d'étendre sa portée à travers les États-Unis.[84] Pendant l'ère d'Internet, les effets de réseau ont été adaptés et popularisés à travers la loi de Metcalfe, qui indique que l'effet d'un réseau de télécommunications est proportionnel au carré du nombre d'utilisateurs connectés au système.[85] Un réseau téléphonique devient plus précieux avec chaque personne supplémentaire qui s'y connecte, de la même manière que la valeur fonctionnelle de Facebook ou Twitter augmente avec chacun de ses nouveaux utilisateurs.

Un deuxième élément, étroitement lié aux effets de réseau, est le coût élevé d'un *changement* entre des services de réseau virtuel souvent mutuellement exclusifs.[86] Les systèmes d'exploitation Windows et Apple, par exemple, adhèrent à deux architectures numériques distinctes et incompatibles. Passer de l'une à l'autre au niveau commercial impliquerait des procédures lourdes et coûteuses telles qu'une requalification du personnel et une réingénierie des protocoles concernés. Pour les consommateurs, certains produits, comme les navigateurs Internet, ne sont pas forcément incompatibles mais redondants.

Suite à ce qui a été évoqué précédemment se pose la question de *l'interopérabilité entre d'autres plateformes, services et applications* lors des étapes initiales de l'existence d'un produit, ainsi qu'une *approche laxiste des composantes open source*. Les entreprises cherchent à ménager les applications externes en laissant une certaine marge de manœuvre dans leur code. En effet, les jeunes entreprises feront probablement tout ce qui est en leur pouvoir pour courtiser les fournisseurs de premier ordre afin d'accumuler les bénéfices de la plus grande visibilité qu'ils octroient.[87] Certaines entreprises ont mis en place des mesures pour empêcher ces comportements laxistes. En ce qui concerne les composantes open source, en 2017 un sondage Open Source à 360° a déploré l'utilisation accrue dans l'industrie des technologies des composantes open source pour renforcer ses propres systèmes et logiciels. Le problème n'était pas les composantes open source en soi, car celles-ci peuvent aider à réduire les coûts, faciliter l'accès, éviter les systèmes exclusifs onéreux des fournisseurs, personnaliser le code, corriger directement les failles et vulnérabilités, et améliorer l'innovation des entreprises. Mais plutôt le fait qu'aucune norme efficace de gestion des risques et de sécurité n'ait été mise en place au moment de leur incorporation. Environ 80-90 % des applications modernes utilisent des

[84] Voir, par exemple, "1908: Annual Report of The Directors of the American Telephone & Telegraph Company to the Stockholders for Year Ending December 31, 1908", Boston, 1909, https://beatriceco.com/bti/porticus/bell/pdf/1908ATTar_Complete.pdf.
[85] B. Metcalfe, "There Oughta Be a Law", *New York Times,* 15 juillet 1996.
[86] C. Shapiro et H. Varian, "Information Rules: A Strategic Guide to the Network Economy", Harvard Business School, 1999, p. 11.
[87] T. Moore et R. Anderson, "Internet Security", in M. Peitz et J. Waldfogel (eds), *The Oxford Handbook of the Digital Economy,* 2012.

composantes de logiciels open source pour répondre aux demandes de sociétés de plus en plus dépendantes à la technologie, ce qui augmente grandement les risques.[88]

Enfin, il subsiste une question épineuse et complexe, celle de la *réglementation*. L'industrie des technologies est peu réglementée et les réglementations qui existent se conforment largement à ce qui a été décrit, puisqu'étant de type *ex ante*.[89] Celles-ci prennent généralement la forme d'une conformité imposée plutôt que de l'imposition de prescriptions techniques externes, à cause d'inquiétudes légitimes quant à l'impact qu'aurait un régime de réglementations de sécurité strict sur, par exemple, l'innovation logicielle dans la phase de développement et la difficulté de maintenir des réglementations prescriptives dans un secteur évolution constante. Bien que les réglementations *ex ante* soient la norme, le taux élevé et ininterrompu d'attaques réussies suggère néanmoins que les réglementations ne parviennent pas à fournir efficacement une plus grande sécurité. Cela est dû à un certain nombre d'externalités au marché informatique, dont le fait que les coûts encourus par l'exploitation des vulnérabilités ne sont pas subis par les fournisseurs responsables de la vulnérabilité, mais par les utilisateurs. Ceci est également dû à « la prévalence de la décharge ou le transfert de responsabilité entre différents acteurs dans les chaînes d'approvisionnement ».[90]

Pour certain, la législation ou la réglementation en matière de responsabilité *ex post* présente aussi des difficultés. Elle peut ralentir le rythme de l'innovation tandis que les entreprises étirent les périodes de développement pour se concentrer sur la sécurité, sans assurance d'une augmentation importante de la sécurité étant donné les failles ou vulnérabilités inévitables qui existent même dans les logiciels les mieux codés. Une responsabilité pour les risques de chaîne d'approvisionnement pourrait être plus plausible, avec des normes de diligence raisonnable basées sur les bonnes pratiques d'une industrie en pleine évolution. Par exemple, Moore suggère une approche réglementaire qui mélange les deux formes de contrôle : il doit être demandé aux fabricants de logiciels de fournir des preuves que des tests de sécurité rigoureux ont été effectués pendant le développement du logiciel tout en endossant une responsabilité juridique plus importante en cas de non-conformité à ces normes de vérification.[91] Pour l'instant, un certain nombre d'initiatives stratégiques prometteuses qui ne sont pas des réglementations contraignantes, sont à l'essai. Elles incluent des lignes directrices, de l'étiquetage et des systèmes de certification. De telles initiatives sont de plus en plus

[88] Un logiciel open source peut être adopté pour faire des économies, avoir un accès facile, disposer de la capacité à personnaliser le code et corriger directement les bogues, et qu'il n'y a pas de système de verrouillage fournisseur. D'après certaines sources, cela favorise aussi l'innovation commerciale.

[89] R. Anderson and T. Moore, "Information Security Economics – and Beyond", dans A. Menzes (ed.), *Advances in Cryptology*, 2007, https://link.springer.com/chapter/10.1007/978-3-540-74143-5_5.

[90] ENISA, "Economics of Vulnerability Disclosure", décembre 2018, https://www.enisa.europa.eu/news/enisa-news/the-economics-of-vulnerability-disclosure/.

[91] R. Anderson and T. Moore, "Information Security Economics – and Beyond", dans A. Menzes (ed.), *Advances in Cryptology*, 2007, https://link.springer.com/chapter/10.1007/978-3-540-74143-5_5.

nombreuses, propulsées en grande partie par les défis et risques émergeants liés aux IdO. Le cadre de certification de cybersécurité de l'UE et le code de bonnes pratiques pour la conception sécuritaire du Royaume-Uni sont des exemples de ces initiatives gouvernementales.[92] Cependant, ces initiatives n'en sont toujours qu'à leurs débuts, évoluent principalement dans une seule région ou doivent rivaliser (et souvent s'opposer) avec des approches réglementaires qui émergent ailleurs.

[92] La proposition de l'UE pour un cadre européen d'étiquetage et de certification en matière de sécurité des TIC vise à favoriser une plus grande confiance et sécurité dans les services et produits de TIC à travers un ensemble complet de procédures, normes, exigences techniques et règles (non contraignantes). Le cadre de certification n'est qu'une composante de l'acte législatif sur la cybersécurité de l'UE, qui complète les instruments existants par de nouvelles initiatives visant à améliorer davantage la réponse et la résilience cyber de l'UE ; voir https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework/; voir aussi, Gouvernement britannique, "Code of Practice for Consumer IoT Security", 2018, https://www.gov.uk/government/collections/secure-by-design/.

RÉPONSES DU SECTEUR PRIVÉ POUR ENDIGUER LA PROPAGATION DE TECHNIQUES ET D'OUTILS TIC MALVEILLANTS

Les cinq dernières années ont fait l'objet d'un changement significatif au niveau du rôle des différents acteurs en ce qui concerne le traitement des différentes dynamiques décrites ci-dessus, propices à la propagation des menaces, vulnérabilités, techniques et outils TIC malveillants évoqués ici. Ces actions peuvent être décrites comme un mélange de mesures *réactives* et *productives*.[93] Les mesures réactives sont manifestes, par exemple, dans la réponse et la réparation des incidents, ou la coopération de l'industrie avec les autorités policières pour combattre la cybercriminalité. Les mesures productives, celles à caractère plus normatif, ont généralement pour objectif de protéger les intérêts commerciaux en repoussant ou exerçant des pressions contre certaines réglementations ou législations, ou en favorisant certaines positions pour protéger des parts de marché. Dernièrement, des mesures productives ont pris la forme d'un certain nombre d'initiatives normatives issues de sociétés et d'experts en technologie dans le but de limiter les comportements des acteurs malveillants étatiques et non-étatiques. Bien que ce ne soit pas le sujet de ce rapport, des mesures productives pourraient aussi être évidentes dans les décisions récentes des compagnies d'assurance pour rejeter les réclamations liées à des incidents majeurs de cybersécurité qui ont été attribués à des États, entraînant des pressions supplémentaires pour le développement de normes et standards.[94]

Divulgation des vulnérabilités

Les vulnérabilités génèrent des coûts importants qui ne sont pas nécessairement assumés par les fournisseurs et les fabricants. Néanmoins, plusieurs entreprises technologiques ont travaillé sur la réparation et la réponses aux incidents pendant de nombreuses années, comme le montrent les stratégies et pratiques de certaines entreprise en ce qui concerne les failles et vulnérabilités affectant leurs propres produits et services (p. ex., le programme STROM d'Intel et son Security First pledge,[95] le Security Vulnerability Research Programme de Microsoft, et le Project Zero de Google et son Vulnerability Disclosure Program).[96] Certains ont mis en place des programmes de chasse aux bogues (p. ex., Les programmes Bug Bounty de Facebook et Vulnerability Reward de Google) qui ont, à leur tour, donné lieu à l'émergence d'une industrie de chasse aux bogues. D'autres se concentrent sur le long terme, préconisant une plus grandes responsabilités des

[93] P. Cornish and C. Kavanagh, "Geneva Dialogue on Responsible Behaviour in Cyberspace", Swiss Federal Department of Foreign Affairs, à venir en 2019. L'auteure est aussi reconnaissante pour les discussions avec Dennis Broeders dans le cadre du travail du Dialogue de Genève.

[94] J.S. Nye Jr., "Normative Restraints on Cyber Conflict", Belfer Center for Science and International Affairs, 2018.

[95] Intel, "Security-first Pledge", 2018, https://newsroom.intel.com/news-releases/security-first-pledge/; pour une discussion sur la mise en oeuvre du groupe STORM d'Intel group, voir L. Hay Newman, "The Elite Intel Team Still Fighting Meltdown and Spectre", *Wired,* 3 janvier 2019, https://www.wired.com/story/intel-meltdown-spectre-storm.

[96] Pour le Security Vulnerability Research Program de Microsoft, voir: https://www.microsoft.com/en-us/msrc/msvr ; pour le Vulnerability Disclosure Program de Google, voir : https://hackerone.com/google/.

chercheurs en sécurité, entreprises technologiques et autres acteurs concernant la découverte et la divulgation publique des vulnérabilités et une meilleure coordination entre eux (p. ex. des lignes directrices et principes communs sur la divulgation coordonnée des vulnérabilités), ainsi que des efforts pour favoriser une plus grande transparence et réduire les risques associés aux pratiques et stratégies de gestion et d'évaluation des vulnérabilités es gouvernements.[97] Ces mesures complètent le travail tout aussi important des chercheurs et des organes techniques comme les équipes d'intervention en cas d'urgence informatique (CERT) qui, pendant de nombreuses années, ont contribué au développement de lignes directrices et de recommandations sur les processus de gestion et d'évaluation des vulnérabilités et les mécanismes de vulnérabilité coordonnés aux niveaux national et international, même si d'importants défis demeurent.[98] Néanmoins, parfois, certaines sociétés ont des approches conflictuelles sur les vulnérabilités. La rivalité en cours Microsoft-Google sur la correction de vulnérabilités et l'éthique de divulgation en est un bon exemple.[99] De plus, certaines réponses, comme les chasses aux bogues, peuvent souvent conduire à de nouvelles difficultés et rivalités.[100]

Au-delà de la divulgation des vulnérabilités

Au-delà de la divulgation des vulnérabilités, les sociétés et les communautés technologiques s'engagent efficacement dans des *initiatives intersectorielles* ou *à l'échelle de l'industrie* pour réduire les menaces communes, renforcer la sécurité des produits et des services, et mettre en place des normes et protocoles de base pour protéger l'architecture TIC mondiale, les chaînes d'approvisionnement mondiales et les utilisateurs. Tous ces éléments jouent un rôle dans l'enrayement de la propagation de techniques et d'outils malveillants.

Les premiers exemples incluent les Mutually Agreed Norms for Routing Security (MANRS) impliquant des opérateurs réseaux du monde entier. L'initiative est gérée par l'Internet Society, et son objectif prioritaire est de « fournir des correctifs cruciaux afin de réduire les menaces de routage les plus communes », dont un grand nombre a été évoqué précédemment dans ce rapport.[101] Une autre initiative en cours est la Domain-Based

[97] Voir K. Charlet *et al*, supra note 11.
[98] Voir par exemple le Software Engineering Institute, "The CERT Guide to Coordinated Vulnerability Disclosure", Carnegie Mellon University", août 2017, https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf/.
[99] C. Betz, "A Call for Better Coordinated Vulnerability Disclosure", Microsoft, 11 janvier 2015, https://blogs.technet.microsoft.com/msrc/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/; voir aussi R. Brandom, "Google Just Disclosed a Major Windows Bug — And Microsoft Isn't Happy", *The Verge*, 31 octobre 2016, https://www.theverge.com/2016/10/31/13481502/windows-vulnerability-sandbox-google-microsoft-disclosure; et plus récemment T. Warren, "Google Discloses Microsoft Edge Security Flaw Before a Patch Is Ready", *The Verge*, 19 février 2018, https://www.theverge.com/2018/2/19/17027138/google-microsoft-edge-security-flaw-disclosure
[100] B. Schneier, "The Vulnerabilities Market and the Future of Security", Forbes, 30 mai 2012 ; voir aussi, "The Bug Bounty Problem: How Mishandled Bounties Hurt the Industry", 16 octobre 2016, https://cybellum.com/bug-bounty-problem-mishandled-bounties-hurt-industry/.
[101] Mutually Agreed Norms for Routing Security (MANRS), https://www.manrs.org/.

Message Authentication, Reporting and Conformance (DMARC), une stratégie d'authentification et un protocole de communication par courriel mis en œuvre par les sociétés « réceptrices, expéditrices, intermédiaires et de développement » dans le but « d'aider à empêcher les attaques d'usurpation d'identité par courriel ».[102] Certaines initiatives plus récentes devraient être interprétées comme cherchant à renforcer la confiance dans les services et produits TIC, mais aussi à induire des changements de comportement. Celle-ci comprennent la Charter of Trust et le Cybersecurity Tech Accord, la première étant piloté par Siemens, la seconde par Microsoft.[103] La Charter of Trust a pour objectif de mettre en œuvre des normes et principes à l'échelle de l'industrie, tandis que le Cybersecurity Tech Accord approuve et fait la promotion des pratiques, normes et initiatives existantes et met un accent particulier sur le façonnement du comportement des États. Un troisième effort, la Global Cyber Alliance, est une initiative intersectorielle impliquant de nombreuses sociétés et entités, et focalisée sur « l'éradication du cyber-risque ».[104]La société de cybersécurité Kaspersky Lab, a également cherché à renforcer la confiance en ses services et produits, notamment grâce à sa Transparency Initiative. Celle-ci a impliqué la délocalisation du traitement et du stockage des données, ainsi que de son infrastructure d'assemblage de logiciels en Suisse, où la société a également ouvert un Transparency Centre.[105]

Certains de ces efforts servent aussi à catalyser ou à rassembler davantage d'appuis envers d'autres initiatives afin de façonner des comportements productifs plutôt que réactifs. Par exemple, le Cybersecurity Tech Accord a récemment souscrit à l'initiative MANRS et, a également souscrit à l'initiative DMARC en partenariat avec la Global Cyber Alliance. Le Tech Accord a aussi émis des propositions au Groupe de haut niveau sur la coopération numérique du secrétaire général de l'ONU en ce qui concerne les principes et les éléments d'action visant à protéger les utilisateurs et clients des menaces numériques, s'opposer aux cyberattaques sur les civils et les entreprises, responsabiliser les utilisateurs et clients afin qu'ils se protègent mieux par eux-mêmes, et favoriser la coopération en matière de cybersécurité.[106] Enfin, les signataires du Tech Accord ont récemment publié une synthèse de leurs positions sur les mesures de renforcement de la confiance en matière de cybersécurité, présentes « une série de recommandations qui tireraient profit des propositions faites par les organisations faisant autorité comme les [Nations Unies] et l'OCDE » et pourraient « aider à combler les lacunes existantes dans les approches des

[102] Domain-based Message Authentication, Reporting and Conformance (DMARC), https://dmarc.org/about/history/.
[103] Voir Siemens, "Time for Action: Building a Consensus for Cybersecurity", https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html; Cybersecurity Tech Accord, https://cybertechaccord.org/about/.
[104] The Global Cyber Alliance (GCA), https://www.globalcyberalliance.org/who-we-are/#mission-purpose.
[105] 'Kaspersky Lab relocates data processing to Switzerland'. Disponible sur : https://www.kaspersky.com/transparency-center
[106] Voir Cybersecurity Tech Accord submission to the United Nations High Level Panel on Digital Cooperation, février 2019, https://digitalcooperation.org/wp-content/uploads/2019/02/Tech-Accord-HLP-Response.pdf/.

États vis-à-vis de la cybersécurité », avec un accent particulier sur l'Organisation des États américains comme destinataire potentiel des idées proposées.[107]

Certaines sociétés ont aussi joué un rôle important dans le financement et la participation à des initiatives multipartites ciblant la promotion de comportements plus productifs de la part d'acteurs ou non-étatiques. Microsoft, par exemple, a constamment soutenu les efforts faits par la Commission mondiale sur la stabilité du cyberespace afin de promouvoir une série de normes (parfois peut-être mieux décrites comme des bonnes pratiques) qui, en cas de mise en œuvre, pourraient contribuer de plusieurs façons importantes à atténuer les cybermenaces et protéger les chaînes d'approvisionnement mondiales des TIC.[108]

Efforts du secteur privé pour façonner le comportement des États

De nombreuses entreprises se mobilisent en faveur d'efforts normatifs entrepris par les gouvernements avec pour objectif d'atténuer les effets négatifs potentiels sur le long terme des règles proposées, afin de mettre la pression sur les gouvernements pour qu'ils respectent les règles ou engagements existants concernant leur utilisation des TIC, ou qu'ils en adoptent de nouveaux. De telles actions du secteur privé peuvent à la fois être perçues comme des réactions à une menace immédiate (les menaces pour ses intérêts commerciaux évidemment, mais aussi les menaces pour la cybersécurité et plus largement sur la stabilité et la sécurité internationales), tout en contribuant à des changements dans le paysage normatif et dans les comportements des autres acteurs.[109] Une fois de plus, celles-ci complètent les efforts entrepris par d'autres acteurs comme les ingénieurs, les chercheurs en sécurité et les membres de la société civile.

Par exemple, un certain nombre de sociétés et d'associations collaborent avec l'Union européenne pour orienter le développement de la directive sur la sécurité des réseaux et de l'information, mais aussi de l'acte législatif sur la cybersécurité, des révisions de réglementation de l'ENISA, du cadre européen de certification de sécurité et d'étiquetage.[110] L'intention n'était pas seulement d'empêcher une réglementation stricte

[107] Voir Tech Accord, "Promoting International Peace and Stability by Building Trust between States in Cyberspace: The Importance of Effective Confidence-Building Measures", avril 2019, https://cybertechaccord.org/uploads/prod/2019/04/FINALOASWP.pdf/.

[108] Voir la Commission mondiale sur la stabilité du cyberespace (GCSC), https://cyberstability.org; plus spécifiquement, voir https://cyberstability.org/research/global-commission-proposes-definition-of-the-public-core-of-the-internet/ et https://cyberstability.org/research/singapore_norm_package/.

[109] Une étude plus complète des rôles et responsabilités du secteur privé pourrait prendre le temps de se pencher sur les pratiques de lobbying complexes et très coûteuses des entreprises de technologie du monde entier.

[110] Le cadre de l'UE pour la certification de cybersécurité pour les services en ligne et les appareils grand public est « la première loi de marché interne dirigée vers l'amélioration de la sécurité des produits connectés, des appareils de l'Internet des objets (IdO) et de l'infrastructure critique » ; voir T. Reeve, "EU Shakes up Cyber-Security with New Agency and Certification Framework", *SC Media*, 11 décembre 2018, https://www.scmagazineuk.com/eu-shakes-cyber-security-new-agency-certification-framework/article/1520888/.

mais de contribuer à améliorer les propositions et leurs effets nationaux et internationaux à long terme.[111]

Un grand nombre de ces mêmes sociétés s'engagent également dans des efforts visant à influencer les positions de négociation de leurs gouvernements lorsque les politiques liées aux TIC deviennent partie intégrante des négociations sur le contrôle des exportations ou le commerce, souvent encore pour protéger leurs intérêts commerciaux, mais aussi dans l'optique de se préserver contre les risques potentiels et d'influencer le paysage normatif. Dans ce contexte, des acteurs de l'industrie ont participé aux discussions suscités par des membres de l'Arrangement de Wassenaar sur la proposition de restreindre les explorations de certains outils d'intrusion numérique afin d'empêcher que des codes d'exploitation de vulnérabilités et des programmes malveillants ne tombent entre les mains de régimes répressifs. Cela aurait nécessité des restrictions sur les exportations de technologies, logiciels et systèmes qui développent ou utilisent des logiciels d'intrusion, ce qui inclut certaines techniques et certains outils utilisés par des entreprises et chercheurs en sécurité impliqués dans des activités légitimes comme les tests d'intrusion, la divulgation des vulnérabilités et la réponse aux incidents. Perçue comme une forme de « réglementation sur les technologies de piratage », la réglementation risquait de mettre en péril le travail des chercheurs légitimes en cybersécurité avec potentiellement des « répercussions considérables et catastrophiques pour l'industrie de la sécurité informatique dans son ensemble ».[112]

Aux États-Unis, les démarches initiales entreprises par le Département du Commerce pour intégrer la réglementation proposée au sein de l'Arrangement de Wassenaar dans la législation nationale ont suscité l'opposition d'un certain nombre d'entreprises de cybersécurité qui se sont ralliées pour mettre sur pied la Coalition for Responsible Cybersecurity dans le but d'empêcher les « règlementations sur le contrôle des exportations nuisibles pour les services et produits de cybersécurité »[113] À la suite d' efforts soutenus de l'industrie (incluant la Coalition et ses membres), de la communauté académique et des chercheurs, le Département du Commerce a révisé ses propositions réglementaires sur le contrôle des exportations concernant les outils de cybersécurité et a sollicité les perspectives de ces acteurs pour élaborer sa position de négociation visant des changements à dans la proposition initiale formulée au sein de l'Arrangement de Wassenaar. Ces changements furent acceptés lors de la session plénière annuelle de l'Arrangement de Wassenaar de décembre 2017.[114]

---

[111] Commission européenne, "Review of ENISA Regulation and Laying Down a EU ICT Security Certification and Labelling", https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3436811/feedback_en?p_id=34664/.

[112] The Coalition for Responsible Cybersecurity, http://www.responsiblecybersecurity.org/latest/.

[113] Ibid.

[114] Voir "Wassenaar Arrangement List of Dual-Use Goods and Technology and Munitions List", décembre 2017, https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf; voir aussi S. Waterman "The Wassenaar Arrangement's Latest Language is Making Security

La forte pression émanant de Microsoft en faveur d'une Convention de Genève sur le numérique, sa plus récente l'Initiative pour la paix numérique et ses actions pour mettre en place un Institut pour la paix numérique constituent un autre exemple important de l'action de l'industrie vis à vis des efforts normatifs entrepris par les gouvernements afin de réagir à des menaces existantes (comportement des États, plus particulièrement concernant le préjudice potentiel pour les citoyens) et d'essayer, sur le long terme, d'empêcher la récidive de tels comportements. Ces efforts sont maintenant devenus un objectif central de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, une initiative multipartite soutenue par le gouvernement français qui gagne en intensité au niveau international.[115]

Researchers Very Happy", cyberscoop.com, 20 décembre 2017, https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

[115] Voir " Appel de Paris pour la confiance et la sécurité dans le cyberespace", 12 novembre 2018, https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf

OBSERVATIONS DE CONCLUSION

Les initiatives évoquées ci-dessus sont toutes importantes. Elles démontrent que les entreprises de technologie jouent un rôle de plus en plus important dans les problèmes de gouvernance nationale et mondiale, tout en signalant que certaines compagnies assument peu à peu des rôles et des responsabilités qui découlent d'une influence et d'un pouvoir accrus. Ces rôles et responsabilités sont complémentaires aux responsabilités des États, de la communauté des technologies et des autres acteurs. Ils ne les remplacent pas.[116]

La question est de savoir si ces initiatives (cumulées aux efforts des États et des autres acteurs) sont suffisantes pour relever les défis en cours. Évidemment, les initiatives évoquées ci-dessus sont loin d'être exhaustives. Toutefois, ces initiatives et les multiples autres qui existent ne semblent pas être en mesure de produire des systèmes et des produits plus sécurisés, ni d'endiguer le flux de techniques et d'outils malveillants, même si les remèdes immédiats sont parfois efficaces et les objectifs normatifs ambitieux. En l'état, les entreprises font face à une perspective imminente de réglementation. Cela est mis en évidence, par exemple, dans l'ensemble de mesures adoptées par l'Union européenne dans son acte législatif sur la cybersécurité. En évoquant les pratiques de divulgation des vulnérabilités, le récent rapport de l'ENISA « Economics of Vulnerability Disclosure » suggère également que des leviers structurels supplémentaires sont peut-être nécessaires « pour aider à compenser certaines conséquences négatives des caractéristiques économiques du marché de la sécurité des technologies de l'information ».[117]

En se tournant vers l'avenir, il sera important de d'élargir et d'encadrer un grand nombre d'approches existantes pour traiter les vulnérabilités et la propagation des techniques et outils malveillants par des cadres de politiques cohérents afin de permettre leur mise en œuvre dans différents pays et régions et de s'assurer que leurs effets puissent être propagés de façon internationale. En effet, jusqu'à présent, celles –ci ont essentiellement avancées par des acteurs du secteur privé et des gouvernements d'Amérique du Nord et d'Europe, principalement car la plupart des sociétés informatiques étaient basées sur ces continents. Ce n'est plus le cas, et comme pour d'autres avancées majeures du domaine technologique qui complexifient les problèmes de gouvernance, un effort devra être fait pour éviter l'émergence de régions aux réglementations conflictuelles, qu'il s'agisse d'autoréglementation de la part des acteurs de l'industrie, ou de réglementations introduites par les gouvernements, ou d'un mélange des deux.[118]Il est donc important de

[116] Voir P. Cornish et C. Kavanagh, "Geneva Dialogue on Responsible Behaviour in Cyberspace", Swiss Federal Department of Foreign Affairs, à venir en 2019.
[117] ENISA, "Economics of Vulnerability Disclosure", décembre 2018, pp. 5–6, https://www.enisa.europa.eu/news/enisa-news/the-economics-of-vulnerability-disclosure/.
[118] C. Kavanagh, *New Tech, New Threats*, Carnegie Endowment for International Peace, à venir.

s'accorder sur les leviers structurels privés et publics complémentaires. Mais à quoi ressembleraient ces leviers et comment une telle approche pourrait-elle être calibrée afin de s'assurer qu'elle ne soit ni trop stricte, freinant l'innovation et décourageant les investissements, ni trop souple, sacrifiant l'intérêt général à la poursuite d'intérêts privés et nationaux ? Il sera sans aucun doute difficile de répondre à ces questions, étant donné la complexité des technologies elles-mêmes, mais aussi l'état actuel des relations internationales, toutefois ce sont précisément ces types de réponses qui sont les plus urgemment requises

Ensuite, un plus grand investissement (politique, financier et technique) doit être réalisé pour assurer une meilleure prise en compte de la sécurité lors de la conception, du développement et de l'application des produits et services. C'est un vieux problème qui n'a pas encore produit d'effets à plus long terme. Certaines solutions alternatives ont été suggérées. Par exemple, la Commission mondiale sur la stabilité du cyberespace a recommandé un « niveau raisonnable de diligence... donnant priorité à la sécurité... et réduisant la probabilité, la fréquence, l'exploitabilité et la sévérité des vulnérabilités ».[119] La façon dont « raisonnable » est défini, mis en œuvre et évalué dans cet environnement complexe reste une question ouverte, notamment alors que les problèmes de cybersécurité se répandront ou convergeront avec l'IdO et d'autres avancées technologiques dans les années à venir.

Enfin, il est difficile de vérifier quels sont les résultats tangibles des différentes initiatives soutenues par l'industrie, puisque celles-ci ont tendance à ne publier que leurs objectifs et de l'information sur les partenariats ou activités passées ou à venir. Une plus grande transparence à cet égard pourrait contribuer à développer la confiance, à convaincre les utilisateurs, les gouvernements et les autres parties affectées de la valeur des initiatives et à identifier les failles émergentes et existantes dans les pratiques et stratégies actuelles. En retour, cela pourrait aider à déterminer si une législation ou une réglementation stricte est effectivement nécessaire. Des mesures de transparence pourraient inclure des rapports et un engagement plus rigoureux sur la façon dont les initiatives atteignent leurs objectifs, sur quels critères elles sont évaluées et par qui, leurs sources de financement et les défis persistants relatifs à leur mise en œuvre. L'Appel de Paris, le Global Forum on Cyber Expertise, le G7 et le G20 constitueraient des plateformes importantes pour présenter ces résultats. Le Groupe de travail à composition non limitée de l'ONU sur le comportement responsable des États dans le cyberespace [120] (OEWG) et le sixième Groupe d'experts gouvernementaux de l'ONU chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité

[119] Voir Commission globale sur la stabilité du cyberespace, 'Norm to Reduce and Mitigate Significant Vulnerabilities', dans "Singapore Norm Package", novembre 2018, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

[120] Voir la Résolution des Nations Unies A/RES/73/27 du 11 décembre 2018.

internationale, [121] qui commenceront leur travail aux Nations Unies plus tard cette année le seront aussi. La résolution qui a créé le Groupe de travail à composition non-limitée mentionne explicitement la possibilité de consultations intersessionnelles avec le secteur privé pour nourrir ses efforts. En effet, les efforts de l'industrie qui démontrent être en mesure de contribuer à la mise en œuvre des normes pertinentes, incluant celles en rapport avec les vulnérabilités et la propagation des techniques et outils malveillants, seront probablement intéressants pour les deux groupes et représenteront une contribution importante à leur travail.

[121] Voir la Résolution des Nations Unies A/RES/73/266 du 2 janvier 2019.

PROGRAMME DE SÉCURITÉ ET DE TECHNOLOGIE

Limiter l'utilisation à des fins malveillantes des menaces et vulnérabilités dans les TIC

Un aperçu des tendances actuelles, des dynamiques de propagation et des réponses du secteur privé

Tandis que les sociétés deviennent de plus en plus dépendantes aux technologies numériques, les entreprises de technologie privées ont à endosser de nouveaux rôles et responsabilités pour façonner et mettre en œuvre une stratégie de sécurité internationale, particulièrement concernant la limitation de la propagation des menaces et vulnérabilités liées aux TIC. Ce rapport stratégique explore les tendances récentes en matière de menaces et de vulnérabilités, examine les dynamiques qui favorisent leur diffusion, et propose des mesures à adopter par le secteur privé pour les endiguer.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH