Droit international et prolifération des cyberarmes

Aude Géry

Dans Politique étrangère 2018/2 Été , pages 43 à 54
Éditions Institut français des relations internationales

ISSN 0032-342X
ISBN 9782365678155
DOI 10.3917/pe.182.0043
Date de mise en ligne : 08/06/2018

Droit international et prolifération des cyberarmes

Par **Aude Gery**

Aude Géry est doctorante en droit international et chercheur associé à la chaire Castex de cyberstratégie.

Les attaques informatiques sont de plus en plus fréquentes et sophistiquées. Des cyberarmes telles que des virus ou des vers sont produites et diffusées par des acteurs publics et privés. Dans ce contexte, certains États cherchent à empêcher la prolifération des outils informatiques malveillants. La régulation des cyberarmes se révèle toutefois particulièrement difficile et les instruments juridiques adoptés jusqu'à présent ne permettent pas à eux seuls de garantir la stabilité du cyberespace.

politique étrangère

Les piratages de Sony Pictures et de Yahoo !, la contamination de centaines de milliers d'ordinateurs par les logiciels malveillants *WannaCry* et *NotPetya*, ou encore les attaques menées contre le secteur de l'énergie ou d'autres infrastructures critiques aux États-Unis, constituent autant d'exemples récents de cyberattaques impliquant une multitude d'acteurs, aux relations ambiguës et aux motivations floues. Ces événements récents illustrent la prolifération des techniques et outils informatiques malveillants utilisés pour mener des cyberopérations. Afin de maintenir la sécurité et la stabilité de l'environnement informatique mondial, les États ont adopté plusieurs instruments pour lutter contre la diffusion incontrôlée de ces outils.

Le contexte de la prolifération des outils informatiques offensifs

Lutter contre la prolifération des outils informatiques offensifs nécessite préalablement de s'intéresser à la spécificité de ces outils et de l'écosystème dans lequel ils sont développés, vendus et utilisés.

Le concept de cyberarme

Il n'existe pas de définition officielle, faisant consensus entre États, de la notion de cyberarme. Cette notion n'apparaît dans aucun instrument

international. Le rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (GEG) au sein des Nations unies lui préfère ainsi l'expression – non définie – de « techniques et outils informatiques malveillants[1] ». L'Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage se concentre, quant à lui, sur les « logiciels d'intrusion[2] ».

Il n'existe pas non plus de consensus sur le terme à employer au sein des États, et rares sont ceux qui définissent le concept retenu. En 2011, l'US Air Force employait la notion de cybercapacités et en proposait la définition suivante : « Toute charge utile d'un dispositif ou d'un logiciel conçue pour perturber, refuser l'accès, dégrader, remettre en cause, altérer ou détruire les systèmes informatiques, données, activités ou capacités adverses. Les cybercapacités n'incluent pas les dispositifs ou logiciels conçus exclusivement pour permettre d'accéder à un système informatique adverse à des fins d'exploitation de données[3]. » La France, dans la *Revue stratégique de cyberdéfense* de février 2018, a retenu les expressions d'arme numérique et de cyberarme, et proposé plusieurs éléments de définition. Ainsi l'expression « arme numérique » renvoie-t-elle d'une part à des « logiciels intrusifs ou destructifs[4] » et d'autre part à des logiciels qui « ne sont pas uniquement conçus pour s'introduire ponctuellement dans un système mais pour y perdurer ou endommager leur cible[5] ». La *Revue* définit également deux catégories d'armes informatiques : les « armes informatiques ciblées » et les « armes informatiques massives ». Des chercheurs[6] ont également tenté de définir ce concept, en se référant, alternativement ou cumulativement,

1. Assemblée générale des Nations unies, « Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale », document des Nations unies A/70/174, 2015, p. 10.
2. Arrangement de Wassenaar, *List of Dual-Use Goods and Technologies and Munition List*, décembre 2017, Annexe « Definition of the terms used in these lists », p. 217-218.
3. U.S. Air Force, *Legal Reviews of Weapons and Cyber Capabilities*, 27 juillet 2011, p. 5, disponible sur : <https://nsarchive2.gwu.edu>. Traduction de l'auteur.
4. Secrétariat général de la défense et de la sécurité nationale, *Revue stratégique de cyberdéfense*, février 2018, p. 87, disponible sur : <www.sgdsn.gouv.fr>.
5. *Ibid*., p. 105.
6. P. Lorents et R. Ottis, « Knowledge Based Framework for Cyber Weapons and Conflict », *Proceedings of the 2nd International Conference on Cyber Conflict*, Tallinn, 2010, p. 129-142 ; B. Boyer, *Cyberstratégie. L'art de la guerre numérique*, Paris, Éditions Nuvis, 2012 ; M. Schmitt (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013 ; E. M. Roche et M. J. Blaine, « Convention internationale sur l'utilisation pacifique du cyberespace », *Netcom*, vol. 27, n° 3-4, 2013, p. 309-330 ; S. Mele, « Legal Considerations on Cyber-Weapons and Their Definition », *Journal of Law & Cyber Warfare*, 2014, vol. 3, n° 1, p. 52-69 ; P. McBurney, T. Rid, « Cyber-Weapons », *The RUSI Journal*, 2012, vol. 157, n° 1, p. 6-13 ; T. Herr et P. Rosenzweig, « Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model », *Journal of National Security Law & Policy*, vol. 8, 2016, p. 301-319.

à la structure du bien (vecteur, perforateur, charge utile), au contexte d'emploi, à l'intention, ou encore aux effets de ces outils, ne prenant que rarement en compte l'usage final des cyberarmes.

Le terme de cyberarme recouvre ainsi une très grande palette d'outils informatiques (vers, virus, *ransomware*[7], etc.), aux effets variés : intrusion, extraction de données, neutralisation ou encore destruction d'un système ou de données. Il s'agit de biens dont la complexité varie grandement : certains outils sont relativement simples tandis que d'autres nécessitent des moyens extrêmement importants. À titre d'exemple, le ver Stuxnet – qui a endommagé le programme nucléaire iranien en 2010 – a nécessité près de trois ans de travail (programmation, renseignement, construction de répliques des centrifugeuses utilisées en Iran afin de tester le ver) avant être déployé[8].

Constitués de lignes de code, ces outils peuvent aisément être copiés, réutilisés, détournés et échangés. De plus, ils peuvent être utilisés à des fins extrêmement diverses, tels la recherche de profit pécuniaire, la défense d'une idéologie, l'espionnage, ou la recherche d'un avantage stratégique. Enfin, ils se caractérisent par une double dualité. Ils peuvent en effet être utilisés à des fins civiles ou militaires, et à des fins pacifiques ou malveillantes. En effet, certains outils pouvant être utilisés à des fins malveillantes sont également utiles pour renforcer la sécurité informatique[9]. Cette double dualité sera au cœur des enjeux de régulation.

L'environnement des cyberarmes

Au-delà des caractéristiques mêmes des cyberarmes, l'environnement dans lequel elles sont développées, vendues et utilisées constitue une donnée complexe pour l'exercice de la régulation.

Une grande variété d'acteurs développe ces outils. Les États ont les capacités les plus avancées. S'il n'existe pas de donnée précise sur le nombre de pays développant des capacités offensives, de plus en plus d'États affirment aujourd'hui en détenir, en les développant eux-mêmes ou en les achetant à des acteurs privés. Des entreprises, des groupes de hackers ou encore de simples individus sont également susceptibles de développer, vendre et utiliser de tels outils. Les acteurs susceptibles

7. Un *ransomware* est un programme malveillant conçu pour chiffrer les données d'un ordinateur et forcer les victimes à payer une rançon afin que les fichiers soient déchiffrés.
8. D. Sanger, *Obama. Guerres et secrets*, Paris, Belin, 2012.
9. Voir par exemple J. O'Gorman, D. Kennedy, D. Kearns et M. Aharoni, *Metasploit: The Penetration Tester's Guide*, San Francisco, No Starch Press, 2011, disponible sur : <https://repo.zenk-security.com>.

de développer, vendre et utiliser des cyberarmes sont donc plus divers et nombreux que ceux impliqués dans la prolifération des armes classiques ou de destruction massive.

Les relations entre ces acteurs sont, par ailleurs, complexes. D'une part, de nombreux rapports et études font état de relations commerciales entre eux, tant sur les marchés noirs que dans des cadres plus officiels[10]. D'autre part, la difficulté à tracer les attaques informatiques, et l'anonymat que procure l'architecture des réseaux, ont encouragé certains États à recourir à des *proxies* pour mener des cyberopérations. Le profil, les motivations, et le contrôle des États sur ces acteurs varient grandement[11]. L'action des États en matière de régulation de ces outils devra donc prendre en compte ces différents paramètres.

L'état de la régulation internationale des outils informatiques offensifs

Le système de sécurité collective est fondé sur la régulation de la force et non des moyens utilisés. Il n'existe par ailleurs pas d'interdiction générale de posséder des armes. Le droit international régule cependant la possession, le transfert ou l'utilisation de certaines armes par les États et les acteurs privés. Pour prévenir les conflits dans le cyberespace, ils ont adopté un certain nombre de dispositions relatives aux outils informatiques malveillants. Ces dispositions visent d'une part les acteurs non étatiques, d'autre part les États, et sont articulées autour de mesures relevant de la lutte contre la cybercriminalité, du contrôle des exportations, et de l'adoption de comportements responsables en matière de lutte contre la prolifération des techniques et outils informatiques malveillants.

La lutte contre la cybercriminalité et la prolifération des cyberarmes

La plupart des instruments internationaux relatifs à la lutte contre la cybercriminalité contiennent des dispositions relatives au développement et au transfert de certains outils informatiques offensifs[12].

Établie dans le cadre du Conseil de l'Europe et ouverte à la signature le 23 novembre 2001, la Convention de Budapest sur la cybercriminalité est le premier instrument international visant à lutter contre la criminalité

10. Voir par exemple R. M. Harrison et T. Herr (dir.), *Cyber Insecurity. Navigating the Perils of the Next Information Age*, Lanham, Rowman & Littlefield, 2016.
11. T. Maurer, *Cyber Mercenaries. The State, Hackers and Power*, Cambridge, Cambridge University Press, 2018, p. 20-21.
12. Office des Nations unies contre la drogue et le crime, Étude détaillée sur la cybercriminalité. Ébauche, Nations unies, New York, février 2013, disponible sur : <www.unodc.org>.

en ligne. Elle ne relève pas du droit du désarmement. Son but est de mettre en place une politique pénale commune aux États signataires afin de lutter contre la cybercriminalité. Elle participe cependant à la lutte contre la prolifération des outils informatiques malveillants en érigeant en infraction la détention et le transfert de certains codes malveillants. Notons que ce type de mesure fonctionnelle n'est pas inconnu du droit du désarmement, notamment en matière nucléaire[13] et d'armes légères et de petit calibre[14].

L'article 6 de la Convention de Budapest couvre un large éventail d'actes informatiques malveillants et une grande diversité d'outils, puisqu'il porte sur les logiciels et dispositifs, entendus comme les matériels informatiques, et les mots de passe et codes permettant d'avoir accès aux données et systèmes informatiques. Cependant, la simple production, vente, obtention pour utilisation, importation, diffusion et possession d'outils informatiques malveillants ne sont pas érigées en infractions. En limitant le champ matériel de l'infraction par un double élément intentionnel, cet article vise à éviter la sur-incrimination de la possession et du transfert d'outils informatiques offensifs. L'élément intentionnel est en effet particulièrement important, dans la mesure où un individu peut détenir sur son système ou transférer des outils informatiques malveillants sans en avoir connaissance. L'article 6 prend également en compte l'usage, non seulement avec l'élément intentionnel, mais également en spécifiant explicitement que ces actes sont licites dès lors qu'ils ont pour finalité des « essais autorisés ou de protection d'un système informatique ». La double dualité précédemment expliquée est donc pleinement prise en compte.

La Convention de Budapest présente toutefois deux limites importantes. La première est géographique, seuls 49 États ayant ratifié ce texte. La seconde tient à la réalité de la prolifération et à l'existence de marchés sur le *deep web* et le *dark web* où sont notamment commercialisés des outils informatiques malveillants et des services associés. Compte tenu des caractéristiques de ces forums, la répression de l'abus de dispositifs s'avère particulièrement difficile. Il n'en reste pas moins que l'incrimination de ces actes constitue un pilier fondamental de la lutte contre la prolifération des cyberarmes.

13. Organisation des Nations unies, « Traité d'interdiction complète des essais nucléaires », New York, 10 septembre 1996, article 3 ; Organisation des Nations unies, « Traité d'interdiction des armes nucléaires », New York, 7 juillet 2017, article 5(2).
14. Organisation des Nations unies, « Protocole contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la Convention des Nations unies sur la criminalité transnationale organisée », New York, articles 5 et 9.

Contrôles des exportations et cyberarmes

Le contrôle des exportations constitue un élément important de la lutte contre la prolifération des outils informatiques offensifs. S'il est parfois perçu comme visant à empêcher certains États de développer leurs capacités, il permet de limiter le risque d'une diffusion incontrôlée de ces outils et de prévenir des usages portant atteinte à la sécurité et à la stabilité de l'environnement informatique mondial.

Les années 2011 à 2013 ont été marquées par des révélations concernant l'implication d'entreprises européennes dans la vente – notamment à la Syrie[15] et la Libye[16] – de systèmes permettant aux gouvernements de ces États de surveiller et d'intercepter les communications électroniques de leurs citoyens. En réaction à ces affaires, la France et le Royaume-Uni ont proposé l'inscription, sur la *Liste des biens et technologies à double usage* de l'Arrangement de Wassenaar, des logiciels d'intrusion et systèmes de surveillance IP. L'Arrangement de Wassenaar est un régime de contrôle des biens considérés comme sensibles. Son but est de « contribuer à la sécurité et la stabilité régionale et internationale en promouvant la transparence ainsi qu'une plus grande responsabilité dans les transferts d'armes conventionnelles et de biens et technologies à double usage, pour, au final, en prévenir les accumulations excessives[17] ». Ce régime de contrôle est non contraignant et s'analyse comme un accord informel aux termes duquel les États participants s'engagent à contrôler l'exportation des biens inscrits sur la *Liste des biens et technologies à double usage* et la *Liste des munitions*. Pour être effectif, les États doivent transposer les listes dans leur droit national. La transposition en droit interne ne constitue cependant pas une obligation internationale et son absence ne permet pas d'engager la responsabilité internationale de l'État.

Le contrôle non contraignant de Wassenaar

Dans l'Arrangement de Wassenaar, l'organisation du contrôle des logiciels d'intrusion s'articule autour de deux séries de dispositions. Les logiciels d'intrusion sont définis dans l'annexe *Définitions*, tandis que le champ matériel du contrôle est déterminé par la Catégorie 4 de la *Liste des biens et technologies à double usage*. Les logiciels d'intrusion sont définis par leurs effets auxquels sont adjoints plusieurs exceptions recouvrant principalement des outils de d'analyse du code, d'évaluation de la sécurité d'un

15. B. Elgin et V. Silver, « Syria Crackdown Gets Italy Firm's Aide With U.S.-Europe Spy Gear », Bloomberg, 4 novembre 2011, disponible sur : <www.bloomberg.com>.
16. P. Sonne et M. Coker, « Firms Aided Libyan Spies », *The Wall Street Journal*, 30 août 2011, disponible sur : <www.fidh.org>.
17. Arrangement de Wassenaar, *Public Documents*, vol. 1, Founding Documents, février 2017, p. 4.

système et de gestion des droits. L'Arrangement n'impose toutefois pas de contrôles aux exportations sur les logiciels d'intrusion eux-mêmes, mais sur leurs vecteurs. Sont ainsi contrôlés les systèmes, équipements et composants spécialement créés ou modifiés pour la génération, le commandement et le contrôle ou l'injection de logiciels d'intrusion (disposition 4.A.5), les logiciels créés ou modifiés pour la génération, le commandement et le contrôle ou l'injection de logiciels d'intrusion (disposition 4.D.4) et les technologies, définies comme les informations spécifiques nécessaires pour le développement, la production ou l'utilisation d'un produit, pour le développement des logiciels d'intrusion (disposition 4.E.1.c). Selon la technologie entourant le logiciel d'intrusion, le périmètre du contrôle ne sera donc pas le même.

En décembre 2017, les États participants à l'Arrangement ont adopté de nouvelles exceptions au contrôle du *software* et de la technologie. Désormais, les logiciels spécialement conçus et limités à la fourniture de mises à jour ou de mises à niveau logicielles ne sont pas soumis à contrôle, dès lors que la mise à jour ou la mise à niveau s'exécute avec l'autorisation du propriétaire ou de l'administrateur du système et que la mise à jour ou la mise à niveau ne constitue pas un logiciel créé ou modifié pour la génération, le commandement et le contrôle ou l'injection de logiciels d'intrusion ou un logiciel d'injection.

De plus, la technologie pour le développement des logiciels d'intrusion et la technologie pour le développement, la production ou l'utilisation d'un équipement ou logiciel visé aux catégories 4.A ou 4.D, n'est pas soumise à contrôle, dès lors qu'elle vise la divulgation de vulnérabilités ou la réponse à incidents. Cela implique donc que les informations échangées dans le cadre de la notification de vulnérabilités, ou lors de la réponse à un incident, ne nécessiteront pas d'autorisation d'exportation. Ces finalités sont définies par l'Arrangement qui dispose néanmoins qu'elles ne sauraient diminuer le droit des autorités nationales à vérifier la conformité des informations échangées dans le cadre des dispositions relatives à la technologie des logiciels d'intrusion.

Ces modifications répondent à plusieurs critiques formulées à l'encontre des dispositions portant sur les vecteurs des logiciels d'intrusion[18]. En effet,

18. T. Dullien, V. Iozzo et M. Tam, *Surveillance, Software, Security, and Export Controls. Reflections and Recommandations for the Wassenaar Arrangement*, 2015 ; S. Bratus, D. J. Capelis, M. Locasto et A. Shubina, *Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk- And How To Fix It*, 2014 ; T. Herr, « Malware Counter-Proliferation and the Wassenaar Arrangement », *Proceedings of the 8th International Conference on Cyber Conflict*, Tallinn, 2016, p. 175-190.

de nombreux experts considéraient que les dispositions en vigueur jusqu'en décembre 2017 dégradaient le niveau mondial de cybersécurité en imposant des contrôles sur des outils nécessaires à la recherche en cybersécurité et au renforcement de la sécurité des systèmes informatiques. En introduisant les exceptions citées précédemment, les États participants ont donc pris en compte la finalité de l'usage des vecteurs des logiciels d'intrusion et leur double dualité. La prise en compte de l'usage constitue une exception dans la méthodologie de l'Arrangement. En effet, ses dispositions sont traditionnellement articulées autour de briques technologiques, et non des effets ou de l'usage. Elle représentait cependant une nécessité compte tenu de la spécificité des outils informatiques. Ces nouvelles dispositions, qui assouplissent le régime de contrôle, faciliteront donc l'échange d'informations relatives aux menaces, aidant à renforcer la sécurité informatique[19].

La problématique du contrôle des exportations des logiciels d'intrusion devrait continuer à alimenter les discussions autour de la lutte contre la prolifération des outils informatiques malveillants et du maintien d'un haut niveau de cybersécurité. En effet, au-delà de la question de la transposition des nouvelles dispositions dans les droits internes, la France a annoncé souhaiter créer une nouvelle catégorie dans la *Liste des munitions*, pour contrôler l'exportation des armes numériques[20]. De plus, au sein de l'Union européenne, le projet de réforme des contrôles des exportations des biens à double usage, proposé par la Commission européenne en septembre 2016[21], devrait être adopté dans les prochains mois. Ce projet crée notamment une nouvelle catégorie de biens dénommée « technologies de cyber-surveillance », étend le champ matériel de la *catch-all clause*[22], élargit le champ matériel du contrôle à l'assistance technique, et établit une obligation de diligence pour les exportateurs.

Des projets européens spécifiques

Pour fonctionner et atteindre ses objectifs en dépit des limites liées aux facilités de détournement, à l'impossibilité technique de contrôler la finalité des outils, ou encore à l'existence de marchés parallèles, un des enjeux

19. K. Moussouris, « Serious Progress Made on the Wassenaar Arrangement for Global Cybersecurity », *The Hill*, 17 décembre 2017, disponible sur : <http://thehill.com>.
20. Secrétariat général de la défense et de la sécurité nationale, *Revue stratégique de cyberdéfense*, *op. cit*., p. 105.
21. Commission européenne, Proposition de règlement du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte), 28 septembre 2016.
22. La *catch-all clause* est une disposition permettant aux autorités de contrôler des biens qui ne sont pas sur les listes de contrôle dont l'exportation peut contrevenir aux objectifs de non-prolifération ou permettre des violations des droits de l'homme.

est aujourd'hui celui de l'universalisation des contrôles. L'Arrangement de Wassenaar ne regroupe en effet que 42 États, dont de nombreux États européens soumis au régime européen de contrôle aux exportations des biens à double usage[23].

Une obligation non contraignante de prévenir la prolifération des techniques et outils informatiques malveillants, et de notifier les vulnérabilités

Aux côtés des dispositions sur la lutte contre la cybercriminalité et le contrôle des exportations, les États ont adopté de nouvelles obligations non contraignantes visant à prévenir la prolifération des techniques et outils informatiques malveillants et à encourager la notification de vulnérabilités.

La problématique des technologies de l'information et de la communication dans le contexte de la sécurité internationale a été inscrite à l'ordre du jour de l'Assemblée générale des Nations unies dès 1998. Cependant, la question de la prolifération n'a été abordée pour la première fois qu'en 2011, lorsque les États membres de l'Organisation de coopération de Shanghai ont proposé un code de conduite pour la sécurité de l'information – non adopté –, dans lequel ils appelaient à lutter contre les armes informationnelles[24]. L'Assemblée générale a par ailleurs demandé à cinq reprises au Secrétaire général de réunir un GEG pour examiner les questions informatiques dans le contexte de la sécurité internationale. Trois rapports, en 2010[25], 2013[26] et 2015[27], ont été produits.

Le rapport adopté par consensus par les États membres du GEG en juin 2015 propose plusieurs normes de comportement responsable et mesures de confiance. Ces normes, facultatives et non contraignantes, ont pour objectif

23. Règlement délégué (UE) n°1382/2014 de la Commission du 22 octobre 2014 modifiant le règlement (CE) n°428/2009 du Conseil instituant un régime communautaire de contrôle des exportations, des transferts et du courtage et du transit de biens à double usage.
24. ONU, Lettre datée du 12 septembre 2011, adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, de l'Ouzbékistan et du Tadjikistan, 14 septembre 2011, document des Nations unies A/66/359, para. b.
25. Assemblée générale des Nations unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, document des Nations Unies A/65/201, 2010.
26. Assemblée générale des Nations unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, document des Nations Unies A/68/98, 2013.
27. Assemblée générale des Nations unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, document des Nations Unies A/70/174, 2015.

« d'aboutir à une vision commune afin de renforcer la stabilité et la sécurité de l'environnement informatique mondial. […] Elles ne cherchent pas à limiter ou à interdire des actes qui respectent le droit international : elles traduisent les attentes de la communauté internationale, fixent des règles de comportement responsable des États, et permettent à la communauté internationale d'étudier les activités menées par les États et d'apprécier leurs intentions[28] ». Certaines d'entre elles portent sur la prolifération.

La première norme relative à la prolifération dispose que « [l]es États devraient prendre des mesures raisonnables pour garantir l'intégrité de la chaîne logistique, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits informatiques, et devraient s'attacher à prévenir la prolifération des techniques et des outils informatiques malveillants et l'utilisation de fonctionnalités cachées malveillantes[29] ». La notion d'intégrité de la chaîne logistique renvoie au fait de ne pas créer volontairement de vulnérabilité dans les logiciels, notamment des *backdoors*, mais également au fait de ne pas intégrer des systèmes afin de les exploiter. La seconde partie de la phrase pose une obligation non contraignante de prévention de la prolifération. Il s'agit simplement d'un engagement des États à lutter contre la diffusion incontrôlée de ces outils dont il ne saurait être déduit un principe d'interdiction de développement, de possession, ou d'usage de ces biens.

Le rapport de 2015 ne détaille pas cette obligation générale. La France avait proposé, lors des négociations du cinquième GEG (2016-2017) de préciser cette norme, par une disposition selon laquelle les États s'engageraient à mettre en place des contrôles aux exportations sur les techniques et outils informatiques malveillants[30]. Le GEG n'ayant pu aboutir à un consensus, celle-ci n'a pas été adoptée. Cette proposition est cependant toujours défendue par la France, qui souhaite une universalisation des contrôles aux exportations sur ces outils[31]. D'autres pistes de régulation sont également envisageables. Il s'agirait de prévenir certains usages de ces outils par des acteurs privés, en leur interdisant de conduire des activités offensives ou d'exploiter des fonctionnalités cachées malveillantes, mesures également portées par la France qui souhaite réguler les activités

28. *Ibid*., para. 10, p. 8.
29. *Ibid*., para. 14, p. 9.
30. Secrétariat général de la défense et de la sécurité nationale, *Revue stratégique de cyberdéfense*, *op. cit*., p. 85.
31. Discours de M. Jean-Yves Le Drian, ministre de l'Europe et des Affaires étrangères, 72e Assemblée générale des Nations unies, New York, 18 septembre 2017 ; Secrétariat général de la défense et de la sécurité nationale, *Revue stratégique de cyberdéfense*, *op. cit*., p. 104.

offensives du secteur privé[32]. Une norme portant sur des exigences qualitatives pour les outils informatiques offensifs pourrait également être envisagée. Les exigences qualitatives en matière d'armement sont des mesures visant à assurer ou à empêcher que des armes déterminées disposent de certains attributs. Ce mécanisme, principalement utilisé dans les traités de maîtrise des armements, pourrait être transposé aux outils informatiques malveillants, en exigeant des critères de précision, de non réutilisation possible, ou encore d'autodestruction.

La seconde norme portant sur la prolifération dispose que « [l]es États devraient encourager le signalement responsable des failles informatiques et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies de l'information et des communications et pour les infrastructures qui en dépendent[33] ». Cette disposition concerne la notification des failles informatiques afin qu'un correctif puisse être apporté et la vulnérabilité corrigée. Renforcée par une mesure de confiance sur la notification de vulnérabilité et les échanges d'informations sur les menaces pesant sur les technologies de l'information et de la communication, elle participe à la la lutte contre la prolifération des outils informatiques malveillants en visant à rendre inopérant le recours à ces outils pour exploiter les vulnérabilités. Cet échange d'informations devrait impliquer tant les acteurs non étatiques que les États, et pourrait être renforcé par d'autres mesures : la mise en place de structures pour gérer au niveau national la notification de vulnérabilités ; la mise en place de programmes type *bug bounty* dont l'objectif est la découverte de failles ; ou la mise en place de procédures et mécanismes de coordination pour l'échange d'informations sur les incidents informatiques.

La notification des failles informatiques

***

Les instruments juridiques adoptés par les États pour tenter de réguler les cyberarmes présentent quatre grandes caractéristiques : ils sont majoritairement non contraignants, leur portée n'est pas universelle, leur précision est variable et il n'existe pas d'articulation entre eux. En outre, les mesures existantes portent principalement sur la prolifération du fait des acteurs non étatiques.

32. *Ibid*., p. 88-89.
33. Assemblée générale des Nations unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, op. cit*., para. 13(j), p. 10.

Si les cyberopérations récentes ont montré l'implication de certains États, l'adoption d'un instrument visant à limiter les capacités de ces derniers n'est pas à l'ordre du jour. Au-delà de l'état de la perception des menaces et des intérêts attachés à l'utilisation de ces outils, de nombreuses difficultés, à l'instar de la définition des cyberarmes, ou de la vérification attachée au respect des dispositions adoptées, devront être surmontées pour parvenir à un consensus. L'adoption de mesures complémentaires pour lutter contre la prolifération des outils informatiques offensifs constituera donc, sans aucun doute, un exercice complexe.

L'objectif de lutte contre leur prolifération ne pourra cependant être atteint que si le niveau mondial de cybersécurité est également renforcé afin d'élever le coût des attaques informatiques. Le renforcement des capacités et l'adoption de comportements responsables en termes d'usage des produits et services informatiques, tant par les acteurs étatiques que non étatiques, sont donc deux enjeux majeurs pour lutter contre la prolifération des outils informatiques malveillants. Le maintien d'un internet ouvert, sûr et pacifique ainsi que de la sécurité et de la stabilité de l'environnement informatique mondial dépendra donc de la capacité des États à adopter une politique cohérente, prenant en compte tous les aspects de la sécurité.

PE

Mots clés
Internet
Cyberespace
Cyberarmes
Droit international