Présentation du Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto) au Comité parlementaire sur la sécurité nationale et le renseignement (CPSNR)

30 juin 2023

Pour toute question relative à cette présentation, veuillez communiquer avec :

Ronald J. Deibert, directeur, The Citizen Lab, Munk School of Global Affairs
Professeur de sciences politiques, Université de Toronto
r.deibert@utoronto.ca

Ont contribué à ce rapport (par ordre alphabétique) :

Siena Anstis (conseillère juridique principale, The Citizen Lab)
Ronald J. Deibert, directeur, The Citizen Lab, Munk School of Global Affairs
Camila Franco (juriste externe, The Citizen Lab)
Zoe Panday (assistante de recherche, The Citizen Lab)

Remerciements :

Merci à Michelle Akim (stagiaire en droit, The Citizen Lab) et Snigdha Basu (spécialiste en communications, The Citizen Lab) pour la mise en forme et la révision.

TABLE DES MATIÈRES

Introduction

Le Citizen Lab est un laboratoire interdisciplinaire de la Munk School of Global Affairs & Public Policy de l'Université de Toronto. Ce laboratoire se consacre à la recherche, au développement et à la mobilisation stratégique et juridique de haut niveau, à la jonction entre les technologies de l'information et de la communication, les droits de la personne et la sécurité internationale.

Le Citizen Lab adopte une approche mixte pour ses recherches, laquelle intègre des méthodes issues de l'informatique, du droit, des sciences politiques et des études territoriales. Les domaines de recherche comprennent l'étude de l'espionnage numérique à l'encontre de la société civile, la documentation sur les logiciels de filtrage d'Internet et d'autres technologies et pratiques ayant une incidence sur la liberté d'expression en ligne, l'analyse des contrôles de publications populaires en matière de confidentialité, de sécurité et d'information, ainsi que l'examen des mécanismes de transparence et de responsabilité qui s'appliquent aux relations entre les organismes gouvernementaux et les entreprises concernant les données personnelles et les activités de surveillance.

Les recherches menées par le Citizen Lab sur l'utilisation des logiciels espions par les acteurs étatiques montrent que cette technologie est utilisée à mauvais escient par certains gouvernements, entraînant des violations des droits de la personne et des risques graves pour la sécurité nationale, la démocratie et l'état de droit. L'utilisation abusive des logiciels espions n'est pas l'apanage des régimes autoritaires, elle est également pratiquée par des États démocratiques et quasi démocratiques à l'encontre de journalistes, de membres des oppositions politiques, de défenseurs des droits de la personne, d'avocats et de membres de la société civile.

Le Citizen Lab se réjouit de l'occasion qui lui est donnée de présenter au Comité parlementaire sur la sécurité nationale et le renseignement (CPSNR) un rapport sur la menace croissante que représentent les logiciels espions mercenaires, une question qui, jusqu'à ce jour, n'a suscité qu'un intérêt limité de la part des décideurs politiques canadiens. Le champ d'application du présent document se divise en trois volets :

1. Fournir un aperçu des principaux acteurs du marché et des caractéristiques techniques des logiciels espions mercenaires, et mettre en évidence les sources pertinentes. Cette partie exposera les principales préoccupations relatives aux logiciels espions mercenaires et les défis liés à la réglementation en vigueur dans le secteur.
2. Examiner les abus liés aux logiciels espions à l'échelle internationale, notamment leur utilisation contre les défenseurs des droits de la personne (DDP), la société civile, les journalistes et des membres des oppositions politiques. Nous analyserons les risques liés à la prolifération des logiciels espions, en mettant l'accent sur les préoccupations relatives aux droits de la personne, à la démocratie, à l'état de droit et à la sécurité nationale. Nous examinerons les initiatives législatives ou politiques existantes et proposées (au 15 mai 2023) visant à lutter contre la prolifération des logiciels espions dans l'Union européenne (UE) et aux États-Unis.
3. Résumer les risques pour les droits de la personne, la démocratie et l'état de droit au Canada qui découlent de l'utilisation de logiciels espions par les institutions et les organismes gouvernementaux canadiens, ainsi que les risques pour la sécurité nationale avec lesquels le

gouvernement fédéral doit désormais composer, compte tenu de la prolifération mondiale incontrôlée des logiciels espions mercenaires.

Logiciels espions mercenaires

Fonctions et capacités techniques

Les logiciels espions sont une forme de maliciels (c'est-à-dire des logiciels malveillants) qui permettent à un opérateur, tel qu'un organisme de renseignement gouvernemental, d'accéder à un appareil électronique et d'extraire, de modifier ou de diffuser son contenu[1]. Au Canada, les « outils d'enquête embarqués » (OEE) de la Gendarmerie royale du Canada (GRC) ont des capacités analogues à celles des logiciels espions mercenaires[2].

L'utilisation du terme « mercenaire », en association avec les logiciels espions, souligne la volonté des entreprises présentes sur ce marché de commercialiser leurs produits en faisant abstraction des risques d'abus engendrés par ces technologies, comme la violation des droits de la personne. Elle témoigne également du rôle du secteur privé dans le développement et la fourniture de logiciels espions aux organismes gouvernementaux et du soutien à l'utilisation de cette technologie au moyen de la configuration de systèmes, de la formation, de la maintenance, de l'assistance et des mises à niveau, à l'instar des sociétés de sécurité privées[3].

Les logiciels espions fonctionnent en exploitant les failles du code logiciel (les « exploits ») qui rendent les applications et les systèmes d'exploitation populaires vulnérables aux attaques de tiers (p. ex. WhatsApp et iOS[4]). Les logiciels espions sophistiqués comportent généralement des exploits « de jour zéro », c'est-à-dire que ceux-ci n'ont pas encore été découverts par le fabricant du logiciel et peuvent ainsi être exploités subrepticement. Des logiciels espions, comme Pegasus, du NSO Group, dont il sera question plus loin, sont ainsi installés sur un appareil ciblé, après qu'une ou plusieurs failles aient été exploitées pour obtenir un accès non autorisé au système d'exploitation. Le NSO Group est connu pour avoir recours à ses ressources internes afin de trouver des exploits qui ne sont vraisemblablement pas disponibles sur le marché public. Le caractère « exclusif » de ceux-ci contribue au coût élevé associé à la technologie des logiciels espions mercenaires.

---

[1] Anstis, Siena, Ronald J. Deibert, et Angela Yang (2022), « Mémoire présenté au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11921005/br-external/CitizenLab-10662114_001-f.pdf https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11921005/br-external/CitizenLab-10662114_001-f.pdf>.

[2] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », la *Chambre des communes* <<https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf>>, pp. 20-22.

[3] Voir p. ex. : « Exhibit 1 through 11: *WhatsApp Inc. v. NSO Group Technologies Limited* » (Filed 10/29/2019) <https://www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/>, pièce 10.

[4] The Citizen Lab (2019), « NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>; Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, et Ronald J. Deibert (2021), « FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.

Les appareils électroniques peuvent être infiltrés par différents vecteurs d'infection : 1) les liens malveillants pour le piratage psychologique qui incitent une cible à interagir avec un lien, déclenchant ainsi le téléchargement d'un logiciel espion sur l'appareil (p. ex. en cliquant sur une URL dans un message WhatsApp); 2) l'exploitation zéro-clic, qui ne requiert aucune interaction de la part de l'utilisateur ciblé et permet ainsi l'infection silencieuse de l'appareil; 3) l'installation manuelle, où le logiciel espion est installé après la saisie physique de l'appareil de l'utilisateur ciblé[5]. En plus de fournir des logiciels espions et les exploits associés, les entreprises spécialisées dans ce domaine peuvent également proposer des services supplémentaires aux opérateurs gouvernementaux, comme une assistance à l'installation de matériel, de la formation sur les systèmes, la maintenance et du soutien technique[6].

Les logiciels espions mercenaires permettent aux organismes gouvernementaux d'accéder aux données d'un appareil ciblé et de les manipuler[7]. Cela comprend l'accès aux mots de passe des comptes, aux justificatifs d'identité dans le nuage (p. ex. comptes Apple), aux fichiers, aux listes de contacts, aux courriels, aux événements du calendrier, aux messages textes (y compris les messages chiffrés qui sont déchiffrés sur l'appareil) et aux photos[8]. Certains logiciels espions peuvent permettre à l'opérateur d'injecter des données dans un appareil ciblé, permettant ainsi à un acteur étatique d'y introduire à distance des contenus incriminants ou diffamatoires et de s'en servir ultérieurement comme preuve contre une cible innocente[9]. Cette technologie intrusive a également la capacité d'activer silencieusement le microphone et la caméra d'un appareil et d'envoyer des informations en direct sur la localisation de l'utilisateur[10]. De telles fonctionnalités transforment efficacement tout appareil mobile infecté en un outil

[5] Marczak, Bill, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, et Ronald J. Deibert (2020), « The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2020/12/great-ipwn-journalists-hacked-suspected-nso-group-imsg-zero-click-exploit/>, p. 2; Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, et Jon Penney (2022), « Submission of the Citizen Lab (Munk School of Global Affairs, Université de Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of- Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>, pp. 3–4; Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, et Ronald J. Deibert (2018), « Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2018/09/hide-seek-tracking-nso-groups-pegasus-spyware-to-operations-45-countries/>, p.7.

[6] Voir p. ex. : « Exhibit 1 through 11: *WhatsApp Inc. v. NSO Group Technologies Limited* », (déposée le 29/10/2019) <https://www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/>, pièce 10.

[7] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, et Jon Penney (2022), « Submission of the Citizen Lab (Munk School of Global Affairs, Université de Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of- Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>, p. 4; Anstis, Siena, Ronald J. Deibert, et Angela Yang (2022), « Mémoire présenté au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11921005/br-external/CitizenLab-10662114_001-f.pdf ation-Privacy-and-Ethics.pdf> ation-Privacy-and-Ethics.pdf>, p.3.

[8] Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, et Ronald J. Deibert (2018), « Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2018/09/hide-seek-tracking-nso-groups-pegasus-spyware-to-operations-45-countries/>, p 7.

[9] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>, p. 5; Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, et Ronald J. Deibert (2022), « CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, p. 25 (p. ex., une affaire récente en Inde concernait l'introduction présumée de preuves incriminantes dans l'appareil d'un activiste indien accusé de terrorisme).

[10] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, et Jon Penney (2022), « Submission of the Citizen Lab (Munk School of Global Affairs, Université de Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances », *Citizen Lab (Munk School of Global*

de surveillance portable, capable de transmettre les conversations qui ont lieu à proximité de la cible, ainsi que d'autres informations confidentielles et personnelles concernant le propriétaire de l'appareil ou les personnes qui communiquent avec lui[11].

Caractéristiques du marché

Le marché des logiciels espions mercenaires fonctionne dans un cadre interentreprises où des sociétés privées vendent des produits à des clients gouvernementaux, tels que les services de renseignement, les forces de l'ordre et les agences de sécurité[12]. Le secteur a connu une croissance significative au cours de la dernière décennie, l'évolution vers une société de plus en plus connectée numériquement s'accompagnant d'un intérêt croissant (et d'un financement accru) de la part des organismes gouvernementaux pour l'acquisition et l'utilisation de technologies de surveillance à des fins de lutte contre le terrorisme[13]. En 2016, plus « plus de 500 entreprises concevant des technologies de surveillance vendaient leurs produits [de surveillance numérique] à des États[14] ». La valeur estimée de ce secteur s'élevait à 12 milliards de dollars américains en 2022[15].

Malgré cette prolifération, presque tous les aspects du secteur des logiciels espions mercenaires sont entourés de secret : des acheteurs de produits de surveillance[16] aux expositions commerciales secrètes où ils sont promus[17], en passant par les noms des entreprises de logiciels espions et la nature de leurs

Affairs & Public Policy, Université de Toronto) <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of- Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>, pp. 4–5.

[11] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, et Jon Penney (2022), « Submission of the Citizen Lab (Munk School of Global Affairs, Université de Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of- Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>, pp. 4–5.

[12] Anstis, Siena, Ronald J. Deibert, et Jon Penney (2019), « Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, Université de Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protecti on-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf>, p. 11.

[13] Ronald J. Deibert (2022), « Protecting Society From Surveillance Spyware », *Issues in Science and Technology* 2(38) <https://issues.org/surveillance-spyware-uso-group-pegasus-citizen-lab/>; Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (2023), « Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach », *Procédures spéciales du Conseil des droits de l'homme* <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulat ion-ct-spyware-technology-trade.pdf>, p. 17.

[14] Conseil des droits de l'homme des Nations unies (2019), « Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », 41e sess., Doc ONU A/HRC/41/35 <https://docs.un.org/fr/a/hrc/41/35>, par. 6.

[15] Ronan Farrow (2022), « How Democracies Spy on Their Citizens », *The New Yorker* (18 avril 2022) <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.

[16] Voir p. ex. : Merlin Delcid (2022), « El Salvador Denies Responsibility for Hacking Journalists After Report Finds Pegasus Spyware on their Phones », *CNN* (13 janvier 2022) <https://www.cnn.com/2022/01/13/americas/el-salvador-pegasus-spyware-intl/index.html>; Justin Spike (2021), « Hungarian Official: Government Bought, Used Pegasus Spyware », *AP News* (4 novembre 2021) <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>; Vanessa Gera (2022), « Polish Leader Admits Country Bought Powerful Israeli Spyware », *AP News* (7 janvier 2022) <https://apnews.com/article/technology-business-software-spyware-jaroslaw-kaczynski-0c41a504e8fbdbb6b9b06f6869848a4>; Panu Wongcha-um (2022), « Thailand Admits to Using Phone Spyware, Cites National Security », *Reuters* (20 juillet 2022) <https://www.reuters.com/world/asia-pacific/thailand-admits-using-phone-spyware-cites-national-security-2022-07-20/>; Joseph Wilson (2022), « Catalan: Spain Spy Chief Admits Legally Hacking Some Phones », *AP News* (5 mai 2022) <https://apnews.com/article/technology-europe-barcelona-spain-hacking-38dcf5392b273f8e8447b0a9f62ed2f5>.

[17] Voir p. ex. : Ilya Lozovsky (2021), « Where NSO Group Came From—And Why It's Just the Tip of the Iceberg », *Organized Crime and Corruption Reporting Project* <https://www.occrp.org/en/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg>.

activités[18]. Les structures commerciales complexes, notamment les entités juridiques multiples qui exercent leurs activités dans différents pays, compliquent la vérification de la conformité d'une entreprise à la législation en vigueur, comme les exigences en matière de licence d'exportation[19]. Ce secret s'étend aux politiques et aux normes des entreprises[20]. Même pour les entreprises connues du grand public, il existe généralement peu d'informations substantielles sur leur conformité aux *Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme*, sur la manière dont elles traitent les répercussions des logiciels espions qu'elles conçoivent et commercialisent sur les droits de la personne, sur l'existence d'un système de diligence raisonnable en cette matière qui donne des résultats vérifiables ou la mise en place d'un système de règlement des griefs, par exemple[21].

Le manque de transparence sur le marché des logiciels espions est favorisé par l'absence de réglementation de la part des États, ce qui permet à ce secteur d'activité de fonctionner sans véritable contrôle public ou gouvernemental[22]. Le lien étroit entre les entreprises qui produisent des logiciels espions et les organismes gouvernementaux qui les achètent laisse supposer que ce manque de transparence est perçu comme avantageux pour les deux parties, ce qui contribue à perpétuer l'absence de réglementation[23]. Enfin, la pression externe en faveur de la transparence est moins forte dans le contexte des transactions commerciales dont le principal client est le gouvernement, le public ayant une connaissance limitée de ce qui se passe[24].

---

[18] Voir p. ex. : Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>, p. 2.

[19] Amnesty International, Privacy International et le Centre de recherche sur les entreprises multinationales (2021), « Operating from the Shadows: Inside NSO Group's Corporate Structure », *Amnesty International* <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>; Ronald J. Deibert (2022), « Subversion Inc: The Age of Private Espionage », *Journal of Democracy* 2(33), p. 34.

[20] Anstis, Siena, Ronald J. Deibert, et Jon Penney (2019), « Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, Université de Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protecti on-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf>, p. 11.

[21] Anstis, Siena, Ronald J. Deibert, et Jon Penney (2019), « Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, Université de Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protecti on-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf>, p. 17.

[22] Anstis, Siena, Ronald J. Deibert, et Angela Yang (2022), « Mémoire présenté au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11921005/br-external/CitizenLab-10662114_001-f.pdf ation-Privacy-and-Ethics.pdf>, p. 7.

[23] Voir Hagar Shezaf et Jonathan Jacobson (2018), « Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays », *Haaretz* (20 octobre 2018) <https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hun t-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000> (Examen de la relation étroite qui existe entre les entreprises privées fabriquant des technologies de surveillance avec l'armée et la défense nationales en Israël.)

[24] Anstis, Siena, Ronald J. Deibert, et Jon Penney (2019), « Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, Université de Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protecti on-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf>, p. 18.

Entreprises sélectionnées

Un nombre croissant d'entreprises mettent au point et commercialisent des logiciels espions mercenaires[25]. Cette partie porte sur quatre entités au sujet desquelles le Citizen Lab a récemment publié : NSO Group, Candiru, Cytrox et QuaDream. Toutefois, d'autres entreprises ont également été impliquées dans la vente de logiciels espions à des organismes gouvernementaux et ont fait l'objet de rapports techniques de la part du Citizen Lab, notamment Gamma Group[26], FinFisher GmbH[27], Cyberbit[28], Amesys[29] (aujourd'hui « Nexa Technologies »), Qosmos, DarkMatter, WiSpear et Hacking Team (aujourd'hui « Memento Labs[30] »).

[25] Voir p. ex. : Conseil des droits de l'homme des Nations Unies (2023) « Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism », 52e sess., Doc ONU A/HRC/52/39 <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx>, par. 47.

[26] Siena Anstis (2018), « Litigation and other Formal Complaints Related to Mercenary Spyware », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#GammaGroup> (Le Gamma Group est un fabricant international de systèmes de surveillance dont le siège social se trouve au Royaume-Uni et qui prétend fournir des services de conseil aux organismes chargés de l'application de la loi. Il a créé une gamme de logiciels espions appelée « FinFisher/FinSpy », qu'il aurait cessé de vendre après 2012).

[27] Siena Anstis (2018), « Litigation and other Formal Complaints Related to Mercenary Spyware », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#FinFisher> (FinFisher GmbH est une société établie en Allemagne qui commercialise FinFisher/FinSpy depuis 2013.) Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, et Sarah McKune (2015), « Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/> (Le logiciel espion FinFisher a été impliqué dans de nombreux abus en matière de surveillance. Le Citizen Lab a identifié 33 utilisateurs gouvernementaux possibles dans 32 pays. Par exemple, le gouvernement de Bahreïn a utilisé FinFisher entre 2010 et 2012 pour surveiller des cabinets d'avocats, des journalistes, des militants et des opposants politiques. Des dissidents éthiopiens en exil au Royaume-Uni et aux États-Unis ont également été infectés par le logiciel espion FinFisher.) Voir aussi à ce sujet : Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, et John Scott-Railton (2013), « You Only Click Twice: FinFisher's Global Proliferation », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/>.

[28] Marczak, Bill, Geoffrey Alexander, Sarah McKune, John Scott-Railton, et Ronald J. Deibert (2017), « Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/> (Créée en 2015, Cyberbit est une société israélienne qui commercialise ses produits auprès des agences de renseignement et des forces de l'ordre. Son logiciel, PC Surveillance System, a été utilisé pour cibler des dissidents éthiopiens dans plusieurs pays, dont les États-Unis et le Royaume-Uni.)

[29] Paul Sonne et Margaret Coker (2011), « Firms Aided Libyan Spies », *Wall Street Journal* (30 août 2011). <http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html> (Nexa Technologies, anciennement « Amesys », est une entreprise française qui a fourni des logiciels espions aux gouvernements libyen et égyptien afin de surveiller des militants, de les suivre, de les torturer et de les faire disparaître de force sous les régimes de Kadhafi et d'Al-Sissi, respectivement); Fédération internationale pour les droits de la personne (2022), « France : La Cour d'appel confirme la mise en examen d'Amesys et de ses dirigeants pour complicité de torture en Libye », *Business & Human Rights Resource Centre* <https://www.business-humanrights.org/en/latest-news/france-court-of-appeal-confirms-indictment-of-amesys-its-executives- over-allegations-of-complicity-of-torture-in-lybia/> (Les dirigeants de Nexa et d'Amesys ont été mis en examen par la Cour d'appel de Paris pour leur complicité dans la fourniture de technologies utilisées dans le cadre de ces crimes.)

[30] Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, et John Scott-Railton (2014), « Mapping Hacking Team's "Untraceable" Spyware », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>; Anstis, Siena, Ronald J. Deibert, et Jon Penney (2019), « Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, Université de Toronto) to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the Surveillance Industry and Human Rights », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protecti on-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf>, p. 11 (Memento Labs est une société établie en Italie qui fournit des « technologies offensives » aux forces de l'ordre et aux services de renseignement du monde entier. Selon des rapports du Citizen Lab, publiés en 2014 et 2015, son logiciel espion, Remote Control System [RCS], a tenté de cibler les employés de l'Ethiopian Satellite Television, un média indépendant géré par des membres de la diaspora éthiopienne. Le Citizen Lab a cartographié l'utilisation présumée du RCS par les gouvernements d'Azerbaïdjan, de Colombie, d'Égypte, d'Éthiopie, de Hongrie, d'Italie, du Kazakhstan, de Corée, de Malaisie, du Mexique, du Maroc, du Nigeria, d'Oman, du Panama, de Pologne, d'Arabie saoudite, du Soudan, de Thaïlande, de Turquie, des Émirats arabes unis et d'Ouzbékistan, entre autres.)

NSO Group

Le NSO Group est une société de logiciels espions fondée en Israël en 2010 et ayant des liens avec les services de renseignement militaire israéliens[31]. Pegasus, le logiciel espion du NSO Group, dispose de fonctionnalités « un clic » et « zéro clic » qui transforment les appareils ciblés en outils sophistiqués de suivi et de surveillance[32]. Le Citizen Lab a publié de nombreux rapports faisant état du déploiement du logiciel espion Pegasus par le gouvernement israélien, ciblant un large éventail de personnes, notamment des défenseurs des droits de la personne, des acteurs de la société civile, des journalistes, des scientifiques, des avocats et des politiciens, ce qui ne serait probablement pas justifié au regard du droit international en matière de droits de la personne[33]. En 2018, le Citizen Lab a recensé 45 pays où les opérateurs de Pegasus pouvaient mener des opérations de surveillance[34]. Cela comprend le Canada, où le Citizen Lab a découvert qu'un dissident saoudien résidant en permanence au Canada, Omar Abdulaziz, avait été ciblé par le logiciel espion Pegasus, probablement par un opérateur saoudien[35]. En juin 2022, des représentants du NSO Group ont déclaré devant le Parlement européen que Pegasus avait été utilisé par certains États pour cibler entre 12 000 et 13 000 personnes par an[36].

Candiru (Saito Tech)

Fondée en Israël en 2014, Candiru commercialise des logiciels espions « non traçables » exclusivement destinés à des clients gouvernementaux[37]. Candiru semble être actuellement enregistré sous le nom de

---

[31] Ronen Bergman et Mark Mazzetti (2022), « The Battle for the World's Most Powerful Cyberweapon », *The New York Times* (28 janvier 2022) <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>; Al Jazeera (2022), « Pegasus: What You Need to Know About Israeli Spyware », *Al Jazeera* (8 février 2022) <https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus>.

[32] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, et Jon Penney (2022), « Submission of the Citizen Lab (Munk School of Global Affairs, Université de Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances, » *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of- Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>, pp. 3–4

[33] Siena Anstis (2018), « Litigation and other Formal Complaints Related to Mercenary Spyware », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/> (Pour plus d'informations sur le NSO Group, y compris une liste non exhaustive de ressources sur les entreprises de logiciels espions compilée par le Citizen Lab et une liste de rapports sur les cibles suivantes : le défenseur des droits de la personne émirati, Ahmed Mansoor, les dissidents saoudiens, Omar Abdulaziz et Ghanem Al-Masarir, ainsi qu'un autre activiste saoudien, des journalistes salvadoriens d'*El Faro*, des défenseurs des droits de l'homme, des avocats et des journalistes jordaniens, des membres de la société civile en Palestine, des manifestants prodémocratie en Thaïlande, des journalistes, des politiciens et des représentants de la société civile mexicains, des membres de la société civile catalane, et un journaliste du *New York Times*).

[34] Anstis, Siena, Ronald J. Deibert, Émilie LaFlèche, et Jon Penney (2022), « Submission of the Citizen Lab (Munk School of Global Affairs, Université de Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of- Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>, p. 6.

[35] Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, et Ronald J. Deibert (2018), « The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>.

[36] Parlement européen : Centre du multimédia (2022), « Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware », *Parlement européen* <https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA>; Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste des Nations Unies (2023), « Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach », Procédures spéciales du Conseil des droits de l'homme des Nations Unies <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulat ion-ct-spyware-technology-trade.pdf>, p. 21.

[37] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>, p. 14.

« Saito Tech Ltd[38] ». Ses produits permettent aux clients d'exfiltrer des fichiers, d'extraire des messages d'applications chiffrées et de voler des témoins de programmes et des mots de passe[39]. Le logiciel espion donne aux clients la possibilité d'envoyer des messages directement, à partir d'un appareil infecté, en accédant aux comptes de messagerie électronique ou aux réseaux sociaux connectés, ce qui donne l'impression que les messages ont été envoyés par la cible du logiciel espion[40]. Le Citizen Lab a recensé des centaines de sites Web liés à Candiru qui utilisent de faux domaines pour se faire passer pour des organisations de défense et des cibles de piratage[41]. De nombreux abus ont été recensés, notamment des attaques ciblant des journalistes au Moyen-Orient[42] et des représentants de la société civile en Espagne[43].

Cytrox

Cytrox est une entreprise macédonienne présente en Hongrie et en Israël qui prétend fournir aux gouvernements des « systèmes de cyberenseignement conçus pour assurer leur sécurité[44] ». Or, le logiciel espion de Cytrox, Predator, a été utilisé pour pirater les comptes de politiciens égyptiens qui critiquaient le régime de Sissi[45], et dans le cadre du scandale actuel de surveillance interne en Grèce[46]. En 2012, Meta a supprimé environ 300 comptes sur Facebook et Instagram qui étaient liés à Cytrox et signalé que de nombreux utilisateurs de Meta dans le monde avaient été ciblés par le logiciel, y compris des politiciens et des journalistes[47].

---

[38] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>, p. 2; consulter également Sam Levin (2021), « Israeli Spyware Firm Linked to Fake Black Lives Matter and Amnesty Websites », *The Guardian* (15 juillet 2021). <https://www.theguardian.com/technology/2021/jul/15/spyware-company-impersonates-activist-groups-black-lives-matter>.

[39] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>, p. 7.

[40] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus », *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>, p. 7.

[41] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>, p. 10.

[42] Emma McGowan (2022), « New Candiru Attack Targets Journalists in the Middle East », *Avast* (28 juillet 2022) https://blog.avast.com/candiru-targeting-journalists-middle-east.

[43] Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, et Ronald J. Deibert (2022), « CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.

[44] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, et Ronald J. Deibert (2021), « Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2021/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-spyware/> (Cytrox fait partie du consortium international « Intellexa Alliance », une étiquette marketing regroupant plusieurs fournisseurs de logiciels de surveillance mercenaires, apparue en 2019. Ce consortium comprend plusieurs entreprises, dont Nexa Technologies, qui cherchent à concurrencer des acteurs majeurs du marché, comme le NSO Group.)

[45] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, et Ronald J. Deibert (2021), « Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2021/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-spyware/>

[46] Georgios Samaras (2022), « Greece's 'Watergate' Explained: Why the European Parliament is Investigating Over a Wiretapping Scandal », *The Conversation* (8 novembre 2022) <http://theconversation.com/greeces-watergate-explained-why-the-european-parliament-is-investigating-over-a-wiretapping-sc andal-192537>.

[47] Dvilyanski, Mike, David Agranovich, et Nathaniel Gleicher (2021), « Threat Report on the Surveillance-for-Hire Industry », *Meta* <https://about.fb.com/wp-content/uploads/2021/12/nThreat-Report-on-the-Surveillance-for-Hire-Industry.pdf>.

QuaDream

QuaDream est une entreprise israélienne qui commercialise des technologies numériques offensives pour ses clients gouvernementaux[48]. Son logiciel espion, **Reign**, utilise des exploits zéro-clic pour infecter les appareils des personnes ciblées[49]. Un rapport d'enquête réalisé en 2023 par le Citizen Lab a identifié des opérateurs de QuaDream en Bulgarie, en République tchèque, en Hongrie, au Ghana, en Israël, au Mexique, en Roumanie, à Singapour, dans les Émirats arabes unis et en Ouzbékistan[50]. L'enquête a révélé que les logiciels espions ont été déployés contre différentes cibles, notamment des journalistes, des opposants politiques et du personnel d'ONG[51]. Des rapports récents suggèrent que QuaDream a mis fin à ses activités en avril 2023, après des mois de difficultés financières et la publication du rapport du Citizen Lab[52].

Les logiciels espions mercenaires suscitent des inquiétudes

Sécurité nationale

Les logiciels espions représentent un risque important pour la sécurité nationale. Ils sont, du fait de leur nature, très intrusifs, en constante évolution et difficiles à détecter. Cette situation engendre des risques difficiles à gérer et à atténuer pour les gouvernements, d'autant plus que la connaissance du marché dans son ensemble est limitée et que l'origine des logiciels espions et l'identité des utilisateurs finaux manquent de transparence[53].

Ces risques sont aggravés par la prolifération de cette technologie, qui donne à tout pays prêt à payer des capacités de surveillance sans précédent.

L'industrie des logiciels espions mercenaires introduit un nouveau type d'acteurs dans ce domaine. L'existence de ce marché non réglementé a permis à un nombre croissant de gouvernements, y compris ceux de pays hostiles au Canada ou ayant des antécédents en matière de violations des droits de la

[48] Gur Megiddo (2021), « Secretive Israeli Cyber Firm Selling Spy-tech to Saudi Arabia », *Haaretz* (8 juin 2021) <https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tec h-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000>.
[49] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, et Ronald J. Deibert (2023), « Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/>.
[50] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, et Ronald J. Deibert (2023), « Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/>.
[51] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, et Ronald J. Deibert (2023), « Sweet QuaDreams A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/>.
[52] Omer Benjakob (2023), « Israeli Spyware Maker QuaDream Closes, Fires All Employees », *Haaretz* (16 avril 2023). <https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadrea m-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000>; Howard Solomon (2023), « Commercial Spyware-maker QuaDream to Close, Say Reports », *IT World Canada* (17 avril 2023) <https://www.itworldcanada.com/article/commercial-spyware-maker-quadream-to-close-say-reports/536543> (indiquant que QuaDream a licencié tous ses employés sauf deux la semaine suivant la publication du Citizen Lab en 2023).
[53] Marczak, Bill, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, et Ronald J. Deibert (2020), « The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2020/12/great-ipwn-journalists-hacked-suspected-nso-group-imsg-zero-click-exploit/>; Duncan B. Hollis (2011), « An e-SOS for Cyberspace », *Harvard International Law Journal* 2(52) <https://harvardilj.org/wp-content/uploads/sites/15/2011/07/HILJ_52-2_Hollis1.pdf>.

personne, d'accéder à des technologies de surveillance très intrusives. La disponibilité des logiciels espions donne aux gouvernements les moyens de se livrer à des activités de cyberespionnage transfrontalier, que ce soit à l'encontre d'autres États, de membres de la diaspora ou de leurs propres résidents dissidents.

Les États dotés de capacités avancées en matière de logiciels espions sont en mesure d'utiliser cette technologie pour façonner de manière stratégique le pouvoir politique, militaire, économique et idéologique mondial[54]. Plusieurs cas avérés d'utilisation de logiciels espions à l'encontre de fonctionnaires gouvernementaux ont été signalés, ce qui représente un risque pour la sécurité nationale. Parmi les exemples, mentionnons notamment l'infection de réseaux gouvernementaux britanniques par des logiciels espions (en particulier le bureau du premier ministre et les bureaux des Affaires étrangères, du Commonwealth et du Développement[55]), celle des appareils du premier ministre espagnol, Pedro Sánchez, de la ministre de la Défense, Margarita Robles[56], et d'au moins 50 fonctionnaires américains dans 10 pays différents[57].

Le projet Pegasus, une enquête internationale sur le cyberespionnage gouvernemental menée par un consortium de 17 organisations médiatiques, a révélé que les numéros de téléphone de 14 chefs d'État ainsi que ceux de diplomates, de chefs militaires et de hauts responsables politiques de 34 pays figuraient dans une base de données ayant fait l'objet d'une fuite, laquelle répertoriait des cibles potentielles pour des logiciels espions[58]. Les appareils infectés de défenseurs des droits de la personne, de journalistes ou de militants peuvent également être utilisés pour surveiller les réunions avec des fonctionnaires. Par exemple, Carine Kanimba, une militante américano-belge, a rencontré des fonctionnaires des États-Unis, de Belgique, du Royaume-Uni et du Parlement européen alors que son téléphone était infecté par Pegasus[59].

Droits de la personne

Les gouvernements et les organisations internationales reconnaissent de plus en plus l'incompatibilité des logiciels espions mercenaires avec les droits fondamentaux[60]. Comme l'ont observé le Contrôleur

[54] Agence de l'Union européenne pour la cybersécurité (2021), « ENISA Threat Landscape 2021 », *Agence de l'Union européenne pour la cybersécurité* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, p. 21.
[55] Ronald J. Deibert (2022), « UK Government Officials Infected with Pegasus », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/>.
[56] Vincent Manancourt (2022), « Hack of Spanish PM's Phone Deepens Europe's Spyware Crisis », *POLITICO* (2 mai 2022) <https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles- digital-espionage-crisis/>.
[57] Ellen Nakashima, Tim Starks (2023), « At Least 50 U.S. Government Employees Targeted with Phone Spyware Overseas », *The Washington Post* (27 mars 2023) <https://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus/>; Peter Guest (2023), « Spyware Finally Got Scary Enough to Freak Lawmakers Out—After It Spied on Them », *Bloomberg* (24 janvier 2023) <https://www.bloomberg.com/news/features/2023-01-24/nso-group-s-pegasus-spyware-focus-of-us-eu-investigations>; Katie Benner, David E. Sanger, et Julian E. Barnes (2021), « Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa » *The New York Times* (3 décembre 2021) <https://www.nytimes.com/2021/12/03/us/politics/phone-hack-nso-group-israel-uganda.html>.
[58] Angelique Chrisafis, Dan Sabbagh, Stephanie Kirchgaessner, et Michael Safi (2021), « Emmanuel Macron Identified in Leaked Pegasus Project Data », *The Guardian* (20 juillet 2021) <https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data>.
[59] Stephanie Kirchgaessner (2021), « Hotel Rwanda Activist's Daughter Placed under Pegasus Surveillance », *The Guardian* (19 juillet 2021) <https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>.
[60] Contrôleur européen de la protection des données (2022), « Preliminary Remarks on Modern Spyware », *Contrôleur européen de la protection des données* <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf>, p. 8 (Le Contrôleur européen de la protection des données conclut que les logiciels espions sont probablement incompatibles avec la *Charte des droits fondamentaux de l'Union européenne*, car « [traduction] le niveau d'ingérence dans le droit à la vie privée est tel que la personne en est en fait

européen de la protection des données (CEPD) et les rapporteurs spéciaux actuels et anciens des Nations unies (ONU), en facilitant l'accès intégral au contenu d'un appareil, les logiciels espions portent atteinte aux droits de la personne, notamment aux droits relatifs à la liberté d'expression, à l'association et au rassemblement, à la vie privée, à la vie, à la liberté et à la sécurité des personnes, à la protection des données et à d'autres droits individuels, et constituent une menace constante pour les institutions de la société civile[61].

Bien que les droits de la personne puissent parfois être enfreints par des acteurs gouvernementaux dans le cadre des lois internationales relatives à ceux-ci, ces infractions doivent être prévues dans la législation, servir un objectif légitime et être nécessaires et proportionnées[62]. Il existe de nombreuses preuves que les logiciels espions sont utilisés d'une manière qui entraîne des violations injustifiées des droits de la personne. Ils ont ainsi servi à surveiller des journalistes et des DDP qui jouent un rôle essentiel dans les institutions de la société civile et dans le maintien des normes démocratiques et respectueuses des droits. Cibler ces acteurs entrave leur capacité à défendre les droits de la personne ou à pratiquer un journalisme d'investigation et porte atteinte à des droits fondamentaux, comme la liberté d'expression et d'opinion et le droit à la vie privée[63]. Comme l'a récemment souligné la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (la « Rapporteuse spéciale sur les droits de l'homme et la lutte antiterroriste »), dans son rapport sur les logiciels espions :

> « La surveillance a une incidence considérable sur de multiples droits de l'homme. La Rapporteuse spéciale souligne que le droit à la vie privée contribue à la protection et à l'exercice de nombreux autres droits et libertés, et que sa protection est intimement liée à l'existence et à la promotion d'une société démocratique. Par conséquent, elle considère que l'augmentation rapide du recours à la surveillance secrète et à la collecte d'informations de contenu et de métadonnées au nom de la lutte contre le terrorisme, conjuguée au développement débridé de nouvelles technologies sous réglementées, est une importante menace pour les sociétés démocratiques[64]. »

privée » et que l'utilisation de cette technologie « [traduction] ne peut être considérée comme étant proportionnée, indépendamment du fait que la mesure peut être jugée nécessaire pour atteindre les objectifs légitimes d'un État démocratique », car elle affecte « l'essence même » du droit à la vie privée).

[61] Contrôleur européen de la protection des données (2022), « Preliminary Remarks on Modern Spyware », *Contrôleur européen de la protection des données* <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf>, p. 2; Conseil des droits de l'homme des Nations unies (2013), « Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », 23e sess., Doc ONU A/HRC/23/40 <https://docs.un.org/fr/A/HRC/23/40>, par. 24 (« [l]e droit au respect de la vie privée est souvent perçu comme un préalable essentiel à la réalisation du droit à la liberté d'expression. Une atteinte indue à la vie privée des personnes peut directement et indirectement limiter la liberté de développement et d'échange des idées »); Conseil des droits de l'homme des Nations unies (2015), « Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », 29e sess., Doc ONU A/HRC/29/32 <https://documents.un.org/doc/undoc/gen/g15/095/86/pdf/g1509586.pdf>, par. 6–10 (examen de la relation entre la vie privée et la liberté d'opinion et d'expression dans le contexte du débat sur le chiffrement et l'anonymat).

[62] Dunja Mijatović (2023), « Des logiciels espions très intrusifs menacent l'essence des droits de la personne », *Commissaire aux droits de l'homme* <https://www.coe.int/fr/web/commissioner/-/des-logiciels-espions-tr%C3%A8s-intrusifs-menacent-l-essence-des-droits-humains>.

[63] Conseil des droits de l'homme des Nations unies (2013), « Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », 23e sess., UN Doc A/HRC/23/40 <https://docs.un.org/fr/A/HRC/23/40>, par. 24–26.

[64] Voir p. ex. : Conseil des droits de l'homme des Nations unies (2023), « Effets sur les droits de l'homme de la mise au point, de l'utilisation et du transfert de nouvelles technologies dans le cadre de la lutte antiterroriste et de la prévention et de la répression de l'extrémisme violent », 52e sess., Doc ONU A/HRC/52/39 <https://docs.un.org/fr/A/HRC/52/39>, par. 45.

Outre les États qui exploitent et utilisent des logiciels espions en violation des lois internationales relatives aux droits de la personne, des entreprises mercenaires spécialisées dans les logiciels espions – prêtes à vendre leur technologie à des pays ayant un bilan médiocre en matière de respect des droits de la personne –, opèrent dans un environnement non transparent[65] et contreviennent aux normes énoncées dans les *Principes directeurs des Nations Unies*[66]. La nature non réglementée de ce secteur facilite la capacité des gouvernements à se procurer des logiciels espions et à les utiliser largement contre des cibles, en violation des lois internationales relatives aux droits de la personne[67].

Démocratie et état de droit

Les logiciels espions constituent une menace importante pour la démocratie et l'état de droit[68]. Ils ont été utilisés par des régimes répressifs pour limiter ou contrôler la dissidence politique, les médias, les tribunaux et d'autres institutions de la société civile[69]. Les gouvernements ont eu recours à ces logiciels pour favoriser la coercition, la manipulation et les campagnes de diffamation. Des personnalités de la sphère publique, notamment des journalistes, des politiciens de l'opposition et des militants, ont été la cible de logiciels espions. Les violations de ces logiciels ne se produisent pas seulement au sein de régimes autoritaires, mais aussi dans les démocraties[70]. Des logiciels espions ont ainsi été employés pour perturber le processus électoral, au moyen de manipulations et de campagnes de dénigrement visant des membres

[65] Direction générale des politiques externes de l'Union, Département thématique, Parlement européen (2015), « Surveillance and Censorship: The Impact of Technologies on Human Rights », *Parlement européen* <https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf>, p. 29; Cindy Cohn, Trevor Timm, et Jillian C. York (2012), « Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes », *Electronic Frontier Foundation* <https://www.eff.org/document/human-rights-and-technology-sales>, pp. 4–5.

[66] Commission des droits de l'homme des Nations Unies (2011), « Principes directeurs relatifs aux entreprises et aux droits de l'homme », *Commission des droits de l'homme des Nations Unies*, Doc ONU HR/PUB/11/04 <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_fr.pdf>.

[67] Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (2023), « Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach », *Procédures spéciales du Conseil des droits de l'homme des Nations Unies* <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulat ion-ct-spyware-technology-trade.pdf>, pp. 22–23 (Sur les diverses violations du droit international relatif aux droits de l'homme, notamment : les violations du droit à la vie et l'exposition indue à des risques physiques; l'ingérence disproportionnée dans la vie privée; l'ingérence disproportionnée dans la liberté d'expression, la liberté de réunion pacifique, d'association et de religion; les préjudices envers les femmes et les personnes LGBTQI+; les répercussions sur le droit à un procès équitable et à une procédure régulière, le droit à un recours efficace.)

[68] Contrôleur européen de la protection des données (2022), « Preliminary Remarks on Modern Spyware », *Contrôleur européen de la protection des données* <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf>, p. 9.

[69] Ronald J. Deibert (2022), « The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy », *Foreign Affairs* 1(102).

[70] Voir p. ex. : Agence de l'Union européenne pour la cybersécurité (2021), « ENISA Threat Landscape 2021 », *Agence de l'Union européenne pour la cybersécurité* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, p. 16 (L'Agence de l'Union européenne pour la cybersécurité a désigné le cyberespionnage d'État comme un risque majeur dans ce rapport.)

de l'opposition politique, dans des pays aussi divers que l'Arabie saoudite[71], l'Inde[72], la Pologne[73], la Hongrie[74], la Grèce et l'Espagne[75].

Les logiciels espions compromettent la qualité de la participation démocratique à la politique en empêchant les citoyens de se mobiliser à l'égard de certaines questions politiques, d'exprimer leurs opinions véritables et de former des réseaux politiques et professionnels[76]. Ainsi, ils ont servi à réprimer les détracteurs du gouvernement et les manifestants en faveur de la démocratie aux Émirats arabes unis[77], en Thaïlande[78], en Arabie saoudite[79], et en Hongrie[80]. Les logiciels qui ont été utilisés contre des fonctionnaires judiciaires et des organisations de la société civile cherchant à responsabiliser les gouvernements espions compromettent également l'état de droit. L'Argentine[81], le Mexique[82], l'Espagne[83], et la Pologne[84], où des avocats ont été pris pour cible, en sont des exemples.

Les journalistes ont été une cible privilégiée des logiciels espions, ce qui constitue une grave atteinte aux fondements de la démocratie, à l'état de droit et à la liberté de la presse[85]. Ces logiciels compromettent la confidentialité des sources journalistiques ainsi que le fonctionnement et la crédibilité du libre accès à

---

[71] Stephanie Kirchgaessner (2021), « Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests », *The Guardian* (18 juillet 2021) <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.

[72] Human Rights Watch (2021), « India: Spyware Use Violates Supreme Court Privacy Ruling », *Human Rights Watch* <https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling>.

[73] Agence France-Presse (2021), « Claims Polish Government Used Spyware is 'Crisis for Democracy', Says Opposition », *The Guardian* (28 décembre 2021) <https://www.theguardian.com/world/2021/dec/28/poland-pegasus-spyware-donald-tusk>.

[74] Shaun Walker (2021), « Viktor Orbán Using NSO Spyware in Assault on Media, Data Suggests », *The Guardian* (18 juillet 2021) <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>.

[75] Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, et Ronald J. Deibert (2022), « CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.

[76] Sartor, Giovanni, et Loreggia Andrea (2022), « L'incidence de Pegasus sur les droits fondamentaux et les processus démocratiques », *commission du Parlement européen chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (PEGA)* https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU (2022)740514_FR.pdf, p. 29.

[77] Marczak, Bill, et John Scott-Railton (2016), « The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/96976/1/Report%2378--Million-Dollar-Dissident.pdf>, p. 8.

[78] Scott-Railton, John, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert, et Ronald J. Deibert (2022), « GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/>.

[79] Stephanie Kirchgaessner (2021), « Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests », *The Guardian* (18 juillet 2021) <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.

[80] Justin Spike (2021), « Hungarian Official: Government Bought, Used Pegasus Spyware », *AP News* (4 novembre 2021) <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>.

[81] Scott-Railton, John, Morgan Marquis-Boire, Claudio Guarnieri, et Marion Marschalek (2015), « Packrat: Seven Years of a South American Threat Actor », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* https://citizenlab.ca/2015/12/packrat-report/, pp. 9–10.

[82] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, et Ronald J. Deibert (2017), « Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>.

[83] Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, et Ronald J. Deibert (2022), « CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.

[84] Agence France-Presse (2021), « Claims Polish Government Used Spyware is 'Crisis for Democracy', Says Opposition ». *The Guardian* (28 décembre 2021) <https://www.theguardian.com/world/2021/dec/28/poland-pegasus-spyware-donald-tusk>.

[85] Saskia Bricmont, Claudia Rothe, et Georg McCutcheon (2022), « In the Name of National Security: How Spyware Threatens the EU's Democratic Foundations », *Heinrich Böll Stiftung The Green Political Foundation* <https://www.boell.de/en/2022/12/14/name-national-security-how-spyware-threatens-eus-democratic-foundations>.

l'information, de la liberté des médias et de leur pluralisme. Cette situation est d'autant plus préoccupante que les médias indépendants constituent l'un des piliers des sociétés démocratiques[86]. Parmi les exemples récents, citons notamment les attaques visant des journalistes couvrant l'actualité en Grèce[87], en Hongrie[88], au Mexique[89], au Salvador[90], en République dominicaine[91], et en Arabie Saoudite[92]. Un exemple marquant est le fait d'avoir pris pour cible diverses personnes proches du dissident et journaliste saoudien Jamal Khashoggi, qui a été brutalement assassiné par le régime saoudien en Turquie[93].

Réponses des États-Unis et de l'UE aux logiciels espions mercenaires

États-Unis

Les États-Unis ont adopté diverses mesures réglementaires pour répondre aux menaces posées par les logiciels espions[94]. Les législateurs américains sont de plus en plus nombreux à réclamer des enquêtes sur l'utilisation de ces logiciels et des mesures de protection contre les risques pour la sécurité nationale et les droits de la personne qu'ils soulèvent[95]. Jim Himes, membre du Congrès américain, ainsi que 14 de ses collègues, a souligné la nécessité d'une action concertée pour protéger les citoyens et les résidents américains et éviter qu'ils ne deviennent la cible de logiciels espions[96]. Adam Schiff, membre du Congrès américain et ancien président de la commission permanente sur le renseignement de la Chambre des représentants, a demandé au directeur de la Drug Enforcement Administration (DEA) de fournir des détails sur le déploiement du logiciel espion Graphite, soulignant les « [traduction] implications potentielles pour la sécurité nationale des États-Unis » et suggérant que son utilisation pourrait « [traduction] aller à l'encontre des efforts visant à dissuader la prolifération généralisée de puissantes capacités de surveillance

[86] Dunja Mijatović (2023), « Highly Intrusive Spyware Threatens the Essence of Human Rights », *Commissaire des droits de l'homme* (27 janvier 2023) <https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights>.
[87] George Georgiopoulos (2022), « Greek Intelligence Service Admits Spying on Journalist », *Reuters* (3 août 2022) <https://www.reuters.com/world/europe/greek-intelligence-service-admits-spying-journalist-sources-2022-08-03/>.
[88] Shaun Walker (2021), « Viktor Orbán Using NSO Spyware in Assault on Media, Data Suggests », *The Guardian* (18 juillet 2021) <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>.
[89] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, et Ronald J. Deibert (2017), « Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>.
[90] Scott-Railton, John, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, et Ronald J. Deibert (2022), « Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://tspace.library.utoronto.ca/bitstream/1807/123609/1/Report%23148--project-torogoz.pdf>, pp. 5–9.
[91] Amnesty International (2023), « Dominican Republic: Pegasus Spyware Discovered on Prominent Journalist's Phone, » *Amnesty International* <https://www.amnesty.org/en/latest/news/2023/05/dominican-republic-pegasus-spyware-journalists-phone/>.
[92] Marczak, Bill, John Scott-Railton, Siena Anstis, Bahr Abdul Razzak, et Ronald J. Deibert (2021), « Breaking the News: New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts », *Citizen Lab (Munk School of Global Affairs, Université de Toronto)* <https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/>.
[93] Stephanie Kirchgaessner (2021), « Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests », *The Guardian* (18 juillet 2021) <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.
[94] Ronald J. Deibert (2022), « The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy », *Foreign Affairs* 1(102).
[95] Mark Mazzetti et Ronen Bergman (2022), « Lawmakers Signal Inquiries Into U.S. Government's Use of Foreign Spyware », *The New York Times* (28 décembre 2022) <https://www.nytimes.com/2022/12/28/us/politics/spyware-israel-dea-fbi.html>.
[96] Mémoire du représentant James A. Himes et coll. aux secrétaires Antony Blinken et Gina M. Raimondo, 29 septembre 2022, <https://himes.house.gov/_cache/files/f/1/f1a6daf0-9ee6-4936-9cb4-25de81cd7d74/D34AB1A35CAEAA423C986A74FDD68A9 7.letter-concerning-the-unethical-uses-of-foreign-commercial-spyware-29sept-.pdf>.

auprès des régimes autocratiques et d'autres acteurs susceptibles d'en faire un usage abusif[97]. » Le Comité du renseignement de la Chambre des représentants des États-Unis a également tenu une audience sur la lutte contre les menaces pour la sécurité nationale américaine liées à la prolifération des logiciels espions commerciaux étrangers, en juillet 2022[98]. Ces appels à l'action ont donné lieu à divers changements législatifs, réglementaires et politiques de la part du gouvernement fédéral.

L'administration Biden a récemment pris plusieurs mesures pour lutter contre la prolifération des logiciels espions commerciaux et leur utilisation abusive[99], notamment l'organisation d'un événement sur les progrès de la technologie au service de la démocratie, dans le cadre du Sommet pour la démocratie de 2023. Au cours de cet événement, les États-Unis ont adopté, avec dix autres pays, dont le Canada, une déclaration commune sur les efforts visant à lutter contre la prolifération et l'utilisation abusive des logiciels espions commerciaux, afin de promouvoir la coopération internationale en matière de réglementation concernant ce type de logiciels[100].

Cette démarche a été renforcée par la mise en place de mesures nationales, dans le cadre d'un décret (le « Décret ») signé par le président Biden, le 27 mars 2023. Celui-ci interdit au gouvernement américain d'utiliser des logiciels espions commerciaux qui « [traduction] présentent des risques importants en matière de contre-espionnage et de sécurité pour le gouvernement américain ou sont susceptibles d'être utilisés de manière abusive par un gouvernement ou un ressortissant étranger, notamment pour cibler des citoyens américains ou perpétrer des violations des droits de la personne[101] ». L'interdiction s'applique à diverses institutions et à certains organismes fédéraux, dont les services chargés de l'application de la loi, la défense et les services de renseignement[102]. Elle répond également à une pression croissante exercée pour lutter contre les menaces graves que représentent les logiciels espions, en établissant des facteurs clés en matière de contre-espionnage, de sécurité et d'utilisation abusive comme indicateurs de risque justifiant le recours à l'interdiction[103]. Le Décret a été signé à la suite de révélations selon lesquelles

---

[97] Mémoire du représentant Adam B. Schiff à l'honorable Anne Milgram, 22 décembre 2022, <https://int.nyt.com/data/documenttools/schiff-letter-on-israeli-spyware-companies/a514c9b78dd75959/full.pdf>.

[98] Comité du renseignement de la Chambre des représentants des États-Unis, « House Hearing on Foreign Spyware », 2022, C-SPAN <https://www.c-span.org/video/?522013-1/house-hearing-foreign-spyware>; Tim Starks (2022), « Congress Joins the Fight over Foreign Spyware », *Washington Post* (25 juillet 2022) <https://www.washingtonpost.com/politics/2022/07/25/congress-joins-fight-over-foreign-spyware/>; Comité du renseignement de la Chambre des représentants des États-Unis, « Full Committee Hearing on Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware, Before the Permanent Select Committee on Intelligence », 117e congrès (2022) <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115048>.

[99] La Maison-Blanche (2023), « FACT SHEET: Advancing Technology for Democracy », *salle de presse de la Maison-Blanche* <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/>.

[100] La Maison-Blanche (2023), « Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware », *salle de presse de la Maison-Blanche* <*https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/*>.

[101] La Maison-Blanche (2023), « FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security », *salle de presse de la Maison-Blanche* <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-orde r-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/>.

[102] La Maison-Blanche (2023), « FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security », *salle de presse de la Maison-Blanche* <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-orde r-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/>; voir également Tim Starks (2023), « Biden's Spyware Executive Order Gets Mostly Good Reviews », *The Washington Post* (28 mars 2023) <https://www.washingtonpost.com/politics/2023/03/28/bidens-spyware-executive-order-gets-mostly-good-reviews/>.

[103] Comité des transports et des infrastructures de la Chambre des représentants des États-Unis, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117e congrès (2022) <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>.

au moins 50 fonctionnaires du gouvernement américain à l'étranger avaient été la cible de logiciels espions[104].

Le Décret s'appuie sur les dispositions de la *National Defence Authorization Act* (NDAA) de 2023 et s'inscrit dans leur prolongement[105]. La NDAA, qui a été promulgué le 23 décembre 2022, a introduit des mesures visant à atténuer les menaces de contre-espionnage liées à la prolifération et à l'utilisation de logiciels espions commerciaux étrangers[106]. L'énoncé de politique figurant dans les nouvelles dispositions souligne l'engagement du gouvernement à agir de manière décisive contre les menaces de contre-espionnage posées par les logiciels espions commerciaux et les personnes qui participent à ce marché[107]. La NDAA confie à la communauté du renseignement américaine le mandat de présenter au Congrès une évaluation des menaces de contre-espionnage et des autres risques que la prolifération de logiciels espions commerciaux étrangers fait peser sur la sécurité nationale des États-Unis[108]. Elle autorise également le directeur du renseignement national à interdire à tout membre de la communauté du renseignement « [traduction] d'acheter, de louer ou d'acquérir de quelque manière que ce soit sur le marché commercial, ou de prolonger ou de renouveler un contrat visant à acheter, à louer ou à acquérir de quelque manière que ce soit, des logiciels espions commerciaux étrangers[109] ».

Les États-Unis ont également pris des mesures pour lutter contre la menace que représentent pour la sécurité nationale les anciens fonctionnaires des services de renseignement qui travaillent avec des sociétés mercenaires spécialisées dans les logiciels espions. Par exemple, après avoir appris que d'anciens agents des services de renseignement américains travaillaient pour des entreprises liées aux Émirats arabes unis[110], les États-Unis ont mis en place des restrictions concernant les anciens employés qui souhaitaient travailler pour des entreprises ou des gouvernements étrangers, notamment des entités spécialisées dans les logiciels espions commerciaux[111]. La NDAA a ainsi apporté des modifications supplémentaires aux restrictions en matière d'emploi, au paragraphe 6301. Mises en œuvre au moyen d'une récente directive à l'intention de la communauté du renseignement, celles-ci imposent une

[104] Tim Starks et Ellen Nakashima (2023), « At Least 50 U.S. Government Employees Targeted with Phone Spyware Overseas », *The Washington Post* (27 mars 2023) <https://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus/>.
[105] Bureau exécutif du président des États-Unis, « Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security », décret 14093 du 27 mars 2023 <https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to>; Comité des services armés de la Chambre des représentants des États-Unis, *National Defense Authorization Act for Fiscal Year 2023*, H.R.7900, 117e congrès <https://www.congress.gov/bill/117th-congress/house-bill/7900>.
[106] Access Now (2022), « U.S. Congress Takes Additional Steps to Combat Spyware », *Access Now* <https://www.accessnow.org/spyware-ndaa-2023/>; Comité des services armés de la Chambre des représentants des États-Unis, *National Defense Authorization Act for Fiscal Year 2023*, H.R.7900, 117e congrès <https://www.congress.gov/bill/117th-congress/house-bill/7900>.
[107] Comité des transports et des infrastructures de la Chambre des représentants des États-Unis, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117e congrès <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>, par. 6318(b)(1).
[108] Comité des transports et des infrastructures de la Chambre des représentants des États-Unis, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117e congrès <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>, par. 6318(c)(b).
[109] Comité des transports et des infrastructures de la Chambre des représentants des États-Unis, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117e congrès <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>, par. 6318.
[110] Christopher Bing and Joel Schectman (2019), « Inside the UAE's Secret Hacking Team of American Mercenaries », *Reuters* (30 janvier 2019) <https://www.reuters.com/investigates/special-report/usa-spying-raven/>.
[111] Comité des transports et des infrastructures de la Chambre des représentants des États-Unis, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117e congrès <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>, par. 6301; Mémoire du représentant James A. Himes et coll. aux secrétaires Antony Blinken et Gina M. Raimondo, 29 septembre 2022, <https://himes.house.gov/_cache/letter-concerning-the-unethical-uses-of-foreign-commercial-spyware-29sept-.pdf>.

interdiction permanente concernant l'exercice de fonctions postérieures au service dans certains pays étrangers désignés[112].

L'exportation et le commerce ont été des domaines prioritaires de la réglementation sur les logiciels espions, soulignant l'intérêt du gouvernement américain à traiter ces derniers à la fois comme une question de sécurité nationale et une menace pour les droits de la personne[113]. La secrétaire américaine au Commerce, Gina M. Raimondo, a expliqué que les États-Unis s'engageaient à « [traduction] utiliser de manière proactive les contrôles à l'exportation afin de responsabiliser les entreprises qui conçoivent, commercialisent ou utilisent des technologies pour mener des activités malveillantes qui menacent la cybersécurité de membres de la société civile, de dissidents, de représentants du gouvernement et d'organisations ici et à l'étranger[114] ».

En novembre 2021, le Bureau de l'industrie et de la sécurité (BIS) du Département américain du Commerce a publié un règlement définitif ajoutant plusieurs entreprises technologiques, dont Candiru et NSO Group, à la « liste des entités » visées par la réglementation sur l'administration des exportations, laquelle restreint l'accès des entreprises désignées aux produits ou technologies d'origine américaine[115]. En mai 2022, le BIS a publié un règlement définitif imposant de nouvelles restrictions sur les articles de cybersécurité pouvant être utilisés à des fins malveillantes[116]. Dans le cadre du Conseil du commerce et des technologies UE-États-Unis, ces derniers ont également souligné leur engagement à « [traduction] lutter contre la prolifération des logiciels espions commerciaux étrangers et des outils de piratage utilisés par des acteurs qui en font un usage abusif pour cibler les DDP et d'autres personnes, et à faire en sorte que les entreprises complices de violations des droits de la personne soient tenues responsables[117] ».

---

[112] Comité des transports et des infrastructures de la Chambre des représentants des États-Unis, *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, H.R.7776, 117e congrès <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>, par. 6301; Bureau du directeur du renseignement national des États-Unis, *Requirements for Certain Employment Activities by Former Intelligence Community Employees*, directive à l'intention de la communauté du renseignement no 712 (23 mars 2023) <https://www.dni.gov/files/documents/ICD/ICD_712.pdf>; Baumohl, Chris, John Davisson, Jake Wiener, et Ben Winters (2023), « Privacy, Surveillance, and AI in the FY'23 National Defense Authorization Act (NDAA) » *Electronic Privacy Information Center* <https://epic.org/privacy-surveillance-and-ai-in-the-fy23-national-defense-authorization-act-ndaa/>.

[113] Département du Commerce des États-Unis, Bureau de l'industrie et de la sécurité, *Export Administration Regulations (EAR)* 15 C.F.R., 16 mars 2021 https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear, par. 730,3; Bureau des affaires publiques (2021), « Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities », *Département du Commerce des États-Unis* <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>.

[114] Bureau des affaires publiques (2021), « Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities », *Département du Commerce des États-Unis* <*https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list*>.

[115] Département du Commerce des États-Unis, Bureau de l'industrie et de la sécurité, *Addition of Certain Entities to the Entity List,* 86(211), FR Doc 2021-24123, Règlement définitif, 4 novembre 2021 <https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2021/file>, par. 60 759; Capito, Charles, Brandon L. Van Grack, et Logan Wren (2021), « Recent Additions to Entity List Part of Broader U.S. Effort Targeting Spyware », *Lawfare* <https://www.lawfareblog.com/recent-additions-entity-list-part-broader-us-effort-targeting-spyware>.

[116] Soliman, Tamer A., Rajesh De, David A. Simon, et Anjani D. Nadadur (2021), « BIS Announces New Export Controls on Cybersecurity Items Used for Malicious Cyber Activity », *Mayer Brown* <https://www.mayerbrown.com/en/perspectives-events/publications/2021/10/bis-announces-new-rule-to-limit-exports-of-cert ain-cybersecurity-products>; Bureau de l'industrie et de la sécurité*, Information Security Controls: Cybersecurity Items*, 87 FR 31948, Règlement définitif, 26 mai 2022 <https://www.federalregister.gov/documents/2022/05/26/2022-11282/information-security-controls-cybersecurity-items>.

[117] Bureau du porte-parole (2022), « Joint Statement on Protecting Human Rights Defenders Online », *Département d'État des États-Unis* <https://www.state.gov/joint-statement-on-protecting-human-rights-defenders-online/>.

Union européenne et États membres

L'UE et ses États membres ont également commencé à reconnaître les risques posés par les logiciels espions. Par exemple, dans son rapport de 2021 sur la situation en matière de menaces, l'Agence de l'Union européenne pour la cybersécurité (ENISA) a qualifié le cyberespionnage d'État de « risque majeur[118] ». Le gouvernement catalan a mis en place un moratoire sur l'utilisation du logiciel espion Pegasus en 2023, devenant ainsi le premier pays européen à adopter une telle mesure[119].

Une grande partie du débat récent sur les logiciels espions dans l'UE s'est concentrée sur la manière de réglementer leur utilisation illégale par les États à l'encontre des résidents et des citoyens de l'UE. En 2022, le Parlement européen a créé une commission d'enquête chargée d'examiner l'utilisation du logiciel espion Pegasus et d'autres logiciels de surveillance équivalents (la « commission PEGA »). Celle-ci a entrepris une enquête approfondie sur l'utilisation de Pegasus, entre autres logiciels espions, par les gouvernements de la Pologne, de la Hongrie, de l'Espagne et de la Grèce[120]. Elle a concentré ses efforts sur les menaces qui pèsent sur les droits fondamentaux, la démocratie et l'état de droit, ainsi que sur la sécurité et la protection des données. Le rapport provisoire de la commission PEGA, publié en novembre 2022, formule plusieurs recommandations, notamment l'imposition d'un moratoire immédiat sur la vente, l'acquisition, le transfert et l'utilisation de logiciels espions, la nécessité pour l'UE de s'entendre sur une définition de la notion de « sécurité nationale » dans le cadre de la justification de l'utilisation de logiciels espions, la création d'un cadre normatif et juridique pour l'utilisation de tels logiciels, ainsi que l'amélioration des mécanismes d'application de la législation en vigueur[121]. En mai 2023, les membres de la commission PEGA ont adopté le rapport définitif non contraignant et les recommandations, à raison de 30 voix pour, 3 contre et 4 abstentions pour le rapport, et de 30 voix pour, 5 contre et 2 abstentions pour les recommandations[122]. Lors de la prochaine session plénière, en juin 2023, les recommandations de la commission PEGA seront soumises au vote de l'ensemble des membres du Parlement européen[123]. Il convient de souligner que les recommandations définitives ne reprennent pas l'appel lancé dans le rapport provisoire en faveur de la mise en place immédiate d'un moratoire sur les logiciels espions. Elles

[118] Agence de l'Union européenne pour la cybersécurité (2021), « ENISA Threat Landscape 2021 », *Agence de l'Union européenne pour la cybersécurité* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, p. 16.
[119] Catalan News (2023), « Catalonia First After US to Restrict Pegasus Spyware Use », *Catalan News* (4 avril 2023) <https://www.catalannews.com/politics/item/catalonia-first-after-us-to-restrict-pegasus-spyware-use>. Il convient de souligner que le Costa Rica a été le premier pays à imposer un moratoire sur les logiciels espions. Consulter Access Now (2022), « Stop Pegasus: Costa Rica is the First Country to Call for a Moratorium on Spyware Technology », *Access Now* <https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/>.
[120] Parlement européen — Communiqué de presse (2022), « EP Inquiry Committee for Pegasus and Other Spyware Launched », *European Parliament* <https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched>.
[121] Sophie in't Veld (2022), « Draft Report: Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware », *Commission d'enquête (PEGA) du Parlement européen chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents* <https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf> at 148–151.
[122] Parlement européen — Communiqué de presse (2023), « Logiciel espions : face à la menace pesant sur la démocratie, le Parlement demande des réformes », *Parlement européen* <https://www.europarl.europa.eu/news/fr/press-room/20230505IPR84901/les-logiciels-espions-menacent-la-democratie-les-deputes-veulent-des-reformescy-and-demand-reforms>.
[123] Parlement européen — Communiqué de presse (2023), « Logiciel espions : face à la menace pesant sur la démocratie, le Parlement demande des réformes », *Parlement européen* <https://www.europarl.europa.eu/news/fr/press-room/20230505IPR84901/les-logiciels-espions-menacent-la-democratie-les-deputes-veulent-des-reformescy-and-demand-reforms>.

demandent plutôt aux États membres de l'UE de se conformer à certains critères d'ici la fin de l'année afin de pouvoir continuer à les utiliser[124].

La fragmentation de la réglementation est une source de préoccupation constante pour l'UE. Les entreprises de logiciels espions mercenaires ont réussi à contourner les contrôles à l'exportation en établissant des bureaux dans des États membres où ceux-ci sont moins rigoureux[125]. Par exemple, NSO Group et Intellexa ont établi des filiales en Bulgarie, à Chypre, en Grèce et à Malte pour faciliter la vente de leurs produits[126]. La question de la « [traduction] mise en œuvre nationale délibérément laxiste », relevée dans le rapport provisoire de la commission PEGA, persistera tant que la cohérence entre la mise en œuvre et l'application ne sera pas mieux assurée[127].

L'UE a également souligné la nécessité de protéger les journalistes contre les logiciels espions. La *législation européenne sur la liberté des médias* qui est proposée vise à protéger l'indépendance des médias, à sauvegarder leur pluralisme et à accroître la transparence en matière de propriété des médias[128]. La législation propose des garanties contre l'utilisation de logiciels espions sur les fournisseurs de services de médias ou les journalistes, bien que des rapports récents suggèrent une tentative inquiétante de la part de certains gouvernements de l'UE d'affaiblir ces protections[129].

Par ailleurs, la réglementation européenne en matière de logiciels espions se concentre également sur la protection des données et la cybersécurité. Le CEPD a publié une déclaration selon laquelle les versions actuelles des logiciels espions sont incompatibles avec les droits de la personne et les dispositions relatives à la protection des données[130]. L'UE a récemment adopté la directive NIS 2, qui remplace la *sécurité des réseaux et des systèmes d'information (NIS 1)* de 2016 et fixe des normes plus strictes en matière de cybersécurité au sein de l'UE[131]. Il existe également le projet de loi sur la cyberrésilience, qui définit les

[124] Parlement européen — Communiqué de presse (2023), « Logiciel espions : face à la menace pesant sur la démocratie, le Parlement demande des réformes », *Parlement européen* <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democra cy-and-demand-reforms. Voir également : Amnesty International — Nouvelles (2023), « Union européenne. Après la proposition du Parlement européen de réglementer les logiciels espions, des "mesures plus fortes" sont nécessaires pour protéger les droits de la personne », *Amnesty International* <https://www.amnesty.org/en/latest/news/2023/05/eu-greater-steps-needed-to-protect-rights-after-eu-parliament-suggests-re.

[125] Feldstein, Steven, et Brian (Chun Hey) Kot (2023), « Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses », *Carnegie Endowment for International Peace* <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-r esponses-pub-89229>, p. 14.

[126] Feldstein, Steven, et Brian (Chun Hey) Kot (2023), « Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses », *Carnegie Endowment for International Peace* <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-r esponses-pub-89229>, p. 14.

[127] Sophie in 't Veld (2022), « Draft Report: Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware », *Commission d'enquête (PEGA) du Parlement européen chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents* <https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf>, p. 95.

[128] Commission européenne (2022), « Législation européenne sur la liberté des médias : La Commission propose des règles pour protéger le pluralisme et l'indépendance des médias dans l'UE », *Commission européenne* <https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_5504>.

[129] Julie Fuchs (2023), « Is the EU Protecting People from Pegasus Spyware? », *Access Now* <https://www.accessnow.org/eu-pegasus-spyware/>; Harald Schumann and Alexander Fanta (2023), « EU governments plan 'blank cheque' to spy on journalists », *Investigate Europe* <https://www.investigate-europe.eu/en/2023/eu-media-freedom-act-governments-exemption-spy-surveillance-journalists/>.

[130] Dunja Mijatović (2023), « Highly Intrusive Spyware Threatens the Essence of Human Rights », *Commissaire des droits de l'homme* <https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights>.

[131] Cyber Risk GmbH (2022), « Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) », *Cyber Risk GmbH* <https://www.nis-2-directive.com/>.

exigences en matière de cybersécurité auxquelles doivent se conformer les fabricants de produits numériques afin de garantir une plus grande sécurité des matériels et des logiciels[132].

La menace des logiciels espions mercenaires pour la sécurité nationale du Canada

Les risques posés au Canada par la prolifération des logiciels espions mercenaires sont doubles. Premièrement, l'adoption de logiciels espions par le gouvernement canadien dans le contexte de l'application de la loi risque d'enfreindre les lois sur les droits de la personne et les protections constitutionnelles et de corroder la démocratie canadienne. Les fractures de la démocratie peuvent devenir un terreau fertile pour la méfiance ou le mécontentement du public et favoriser la propagation d'activités qui menacent la sécurité nationale. Deuxièmement, l'inaction législative concernant l'industrie croissante des logiciels espions mercenaires permet à des acteurs étatiques hostiles de cibler de manière généralisée et clandestine des fonctionnaires, des résidents et des entreprises au Canada, contre lesquels le pays n'est pas à l'abri. Le fait que des organismes ou des fonctionnaires canadiens puissent être visés représente en soi un risque grave pour la sécurité nationale.

Menaces liées à l'utilisation de logiciels espions par les gouvernements

En l'absence de garanties adéquates, l'achat et l'utilisation de logiciels espions par les organismes canadiens risquent de reproduire les violations des droits de la personne constatées dans d'autres États et d'avoir un effet délétère sur la démocratie canadienne. De plus, la nature secrète, non réglementée et facilement exploitable de cette technologie invasive entrave et fausse les écosystèmes d'information dont les citoyens ont besoin pour participer aux processus démocratiques et exiger la responsabilisation des gouvernements. Le principe de « [traduction] responsabilité s'applique lorsqu'il existe une relation dans le cadre de laquelle une personne ou une institution, et l'exécution de ses tâches ou fonctions, sont soumises à la supervision, à la direction ou à la demande d'une autre personne ou institution de fournir des informations ou des justifications concernant ses tâches ou fonctions[133] ». Dans les États démocratiques, la responsabilité peut être divisée en mécanismes horizontaux et verticaux, qui prévoient des outils liés à l'obligation de rendre compte et à l'application de la loi[134]. Le secret caractéristique qui entoure l'industrie des logiciels espions et leur utilisation par le gouvernement représente un obstacle important à toute obligation réelle de rendre compte au Canada.

[132] Commission européenne (2022), « Cyber Resilience Act », *Commission européenne* <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>; Martinet, Charles, et Romain Bosc (2022), « Europe Uses Spyware on its Own Citizens », *Center for European Policy Analysis (CEPA)* <https://cepa.org/article/europe-uses-spyware-on-its-own-citizens/>.

[133] Riccardo Pelizzo et Frederick Stapenhurst (2013), *Government Accountability and Legislative Oversight* (Routledge: 2013), p. 2.

[134] Parsons, Christopher et Adam Molnar (2018), « Government Surveillance Accountability: The Failures of Contemporary Canadian Interceptions Reports », *Canadian Journal of Law and Technology* 1(16), pp. 148–149 (La responsabilité verticale désigne les mécanismes officiels qui obligent certains représentants du gouvernement à rendre compte à une instance, comme un organisme gouvernemental ou un ministère, qui a le pouvoir de les sanctionner s'ils manquent à leurs obligations. Les mesures de responsabilité horizontale prévoient des mécanismes non officiels et indirects, dans lesquels les acteurs concernés divulguent volontairement des informations qui permettent aux intervenants extérieurs au gouvernement de fournir des commentaires, de soulever des préoccupations et de soutenir les processus de responsabilité verticale en place.)

Par exemple, en juin 2022, la GRC a révélé qu'elle utilisait des OEE depuis au moins 2012[135], évoquant les défis croissants liés à la collecte de preuves numériques lors d'enquêtes criminelles, en raison de l'évolution rapide des technologies[136]. La décision de la GRC d'utiliser des OEE n'a pas été soumise à l'examen du Commissariat à la protection de la vie privée et a été discrètement révélée dans le cadre de la réponse de l'organisation à une question inscrite au *Feuilleton de la* Chambre des communes[137]. Au cours des audiences de 2022 organisées par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (« audiences du Comité ETHI »), organisées en réponse aux révélations de la GRC, le ministre de la Sécurité publique, Marco Mendicino, a insisté sur le fait que l'utilisation des technologies de surveillance par la GRC était réservée aux « infractions les plus graves » et que les interceptions de communications privées étaient effectuées conformément aux exigences d'autorisation judiciaire décrites dans le *Code criminel* canadien et dans les limites de la *Charte canadienne des droits et libertés*[138]. Si le ministre Mendicino a confirmé que la GRC n'utilisait pas le logiciel espion Pegasus du NSO Group, peu d'informations concrètes ont été rendues publiques concernant le logiciel en question, la fréquence de son utilisation ou son incidence sur les droits de la personne ou les droits protégés par la Constitution[139]. À l'heure actuelle, seule une unité interne de la GRC – le Programme national d'intégration des technologies – est chargée de veiller à ce que les OEE utilisés par la GRC respectent les normes juridiques et éthiques requises[140]. La GRC n'a pas informé ni consulté le Commissariat à la protection de la vie privée du Canada (CPVP) au sujet de ce programme interne[141]. Il n'existe aucun autre mécanisme de contrôle externe permettant de corroborer les informations de la GRC,

[135] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, « 031/1/44 – Témoignages – Le lundi 8 août 2022 » *la Chambre des communes, Canada* <https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/reunion-31/temoignages>.

[136] Maura Forrest (2022), « Canada's National Police Force Admits Use of Spyware to Hack Phones », *POLITICO* (29 juin 2022) <https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092>; Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », *la Chambre des communes, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf>, p. 5; Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, « 031/1/44 – Témoignages – Le lundi 8 août 2022 » *la Chambre des communes, Canada* <https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/reunion-31/temoignages>.

[137] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », *la Chambre des communes, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf>, pp. 12–14.

[138] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, « 031/1/44 – Témoignages – Le lundi 8 août 2022 » *la Chambre des communes, Canada* <https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/reunion-31/temoignages>; *Code criminel,* L.R.C 1985, ch. C-46, <https://laws-lois.justice.gc.ca/fra/lois/c-46/page-26.html#h-118925>, Partie VI, Interception des communications; *Charte canadienne des droits et libertés*, la Partie 1 de la *Loi constitutionnelle de 1982* étant l'annexe B de la *Loi* de 1982 *sur le Canada* (R.-U.), 1982, c 11 <https://laws-lois.justice.gc.ca/fra/const/page-12.html>.

[139] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », *la Chambre des communes, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf>, pp. 9–11.

[140] Gendarmerie royale du Canada (2021), « Réponse au rapport du Commissariat à la protection de la vie privée sur l'utilisation de Clearview AI par la GRC », *Gendarmerie royale du Canada, gouvernement du Canada* <https://grc.ca/fr w-ai> (« En mars 2021, nous avons créé le Programme national d'intégration des technologies [PNIT], afin de centraliser et de rendre plus transparents les processus qui régissent la façon dont la GRC sélectionne, évalue, surveille et approuve l'utilisation des technologies nouvelles et émergentes et des outils d'enquête qui requièrent la collecte et l'utilisation de renseignements personnels »); voir également : Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, « 031/1/44 – Témoignages – Le lundi 8 août 2022 » *la Chambre des communes, Canada* <https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/reunion-31/temoignages> (Commentaire du ministre Mendicino : « [PNIT] veillera à ce qu'une évaluation approfondie de la technologie soit effectuée, en s'assurant qu'elle respecte toutes les normes en matière de confidentialité, de droit et d'éthique ».)

[141] Commissariat à la protection de la vie privée du Canada (2022), « Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique sur l'étude des outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada : Déclaration de Philippe Dufresne Commissaire à la protection de la vie privée du Canada », *Commissariat à la protection de la vie privée du Canada* <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2022/parl_20220808/>.

et celle-ci n'est actuellement soumise à aucune obligation de rendre compte au public ni à aucune exigence de préparer des évaluations des répercussions sur la vie privée relativement à son utilisation d'OEE[142]. On ne sait pas non plus si d'autres organismes fédéraux, comme le Service canadien du renseignement de sécurité[143], le Centre de la sécurité des télécommunications ou l'Agence des services frontaliers du Canada, utilisent des logiciels espions similaires dans l'exercice de leurs fonctions[144].

Au cours des audiences du Comité ETHI, les représentants du gouvernement ont constamment invoqué la nécessité de protéger le secret opérationnel à des fins de sécurité nationale ou de sauvegarde de l'intégrité des enquêtes pour justifier leur refus de répondre directement aux questions du comité[145]. Si un certain degré de confidentialité des opérations peut s'avérer nécessaire dans le cadre d'enquêtes sensibles, ces puissantes technologies de surveillance ont fait la preuve qu'elles pouvaient être utilisées à mauvais escient en l'absence d'un contrôle indépendant strict ou de rigoureuses mesures de responsabilisation[146]. Le discours actuel qui justifie le manque de transparence au nom de l'intégrité opérationnelle pour lutter contre le terrorisme et les crimes graves est le même que celui avancé par d'autres gouvernements démocratiques ou quasi démocratiques, qui ont par la suite fait un usage abusif de ces technologies à des fins politiques contre des cibles illégales, telles que des militants civils, des dissidents et des journalistes. La Rapporteuse spéciale sur les droits de l'homme et la lutte antiterroriste a récemment démontré « qu'il est rare que les motifs avancés et les restrictions imposées soient légitimes et que l'argument selon lequel ces technologies sont employées à titre exceptionnel pour faire face à des problèmes de sécurité ne tient pas la route lorsque rien n'est fait dans la réalité pour restreindre l'utilisation généralisée et systématique des technologies de façon à préserver les droits de l'homme ou l'état de droit » justifient l'adoption de « technologies à haut risque très intrusives[147] ».

---

[142] Brenda McPhail (2022), « Oral Submission to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) for the Study of Device Investigation Tools Used by the Royal Canadian Mounted Police », *Association canadienne des libertés civiles* <https://ccla.org/wp-content/uploads/2022/08/9-Aug-2022-ETHI-Committee-Submission-on-RCMP-ODIT-Copy.pdf>; Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », *la Chambre des communes, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf>, pp. 13–14, 25–27 (M. Dufresne a dit que dans « sa réponse à la question inscrite au Feuilleton, la GRC a mentionné qu'elle avait commencé à préparer une [évaluation des facteurs relatifs à la vie privée] concernant ces outils en 2021, mais nous n'avons pas encore reçu cette évaluation ».)

[143] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, « 033/1/44 – Témoignages – Le mardi 9 août 2022 », *la Chambre des communes, Canada* <https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/reunion-33/temoignages> (L'ancien agent des services de renseignement, M. Juneau-Katsuya, a déclaré qu'il était probable que d'autres organismes utilisent une technologie similaire à Pegasus, admettant que le SCRS avait surveillé des parlementaires dans le passé parce qu'il craignait qu'ils ne soient recrutés ou rémunérés par des organisations étrangères).

[144] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », *la Chambre des communes, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf> at 10–11.

[145] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, « 031/1/44 – Témoignages – Le lundi 8 août 2022 », *la Chambre des communes, Canada* <https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/reunion-31/temoignages > (Voir p. ex. la réponse du ministre Mendicino à la question du député James Bezan concernant la technologie utilisée : « comme je l'ai mentionné à la fin de mes remarques… certaines techniques d'enquête doivent rester confidentielles. C'est essentiel pour préserver l'intégrité des opérations et traduire les suspects en justice, le cas échéant »).

[146] Brenda McPhail (2022), « Oral Submission to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) for the Study of Device Investigation Tools Used by the Royal Canadian Mounted Police », *Association canadienne des libertés civiles* <https://ccla.org/wp-content/uploads/2022/08/9-Aug-2022-ETHI-Committee-Submission-on-RCMP-ODIT-Copy.pdf>.

[147] Conseil des droits de l'homme des Nations Unies (2023) « Effets sur les droits de l'homme de la mise au point, de l'utilisation et du transfert de nouvelles technologies dans le cadre de la lutte antiterroriste et de la prévention et de la répression de l'extrémisme violent », 52e sess., Doc ONU A/HRC/52/39 <https://docs.un.org/fr/A/HRC/52/39>, p. 1; voir également : Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (2023), « Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach », *Procédures spéciales du Conseil des droits de l'homme*

Les audiences du Comité ETHI démontrent les lacunes des méthodes de responsabilité verticale en vigueur au Canada : l'instance gouvernementale ne dispose pas des informations nécessaires pour demander des comptes à l'acteur, et le manque de transparence ou la possibilité que les normes juridiques ne soient pas correctement respectées n'entraînent aucune conséquence réelle. Ce manque d'information a un effet domino sur les acteurs de la responsabilité horizontale (acteurs civils ou intervenants extérieurs au gouvernement), qui sont donc également privés d'une véritable possibilité de fournir un retour d'information, d'exprimer leurs préoccupations ou de désapprouver les politiques en place[148].

Ces lacunes en matière de responsabilité sont préoccupantes, non seulement parce qu'elles créent un vide juridique qui pourrait permettre aux organismes chargés de l'application de la loi d'agir en dehors du cadre prévu par celle-ci, mais aussi parce qu'elles menacent la sécurité nationale et la démocratie de manière plus générale, en compromettant la confiance du public dans les institutions gouvernementales et en déstabilisant l'intégrité de la gouvernance démocratique[149]. Plus précisément, l'effondrement des mécanismes de responsabilisation alimente à juste titre le scepticisme du public quant à la capacité des législateurs à garantir le respect de l'état de droite et à leur intention de prendre cette responsabilité au sérieux[150]. L'insistance sur la confidentialité et la réticence à divulguer des informations concernant l'utilisation de logiciels espions par le gouvernement affaiblissent donc « [traduction] la confiance dans le fait que les activités légales sont menées avec l'approbation ou le consentement démocratique des citoyens »[151]. Cette situation entraîne une certaine désaffection de la part du public envers les institutions chargées de le protéger[152]. Les récents scandales liés à la surveillance aux États-Unis et en Espagne démontrent que même les démocraties qui fonctionnent peuvent « [traduction] dégénérer en démocraties gravement déficientes dans l'avenir » et déstabiliser la sécurité d'une nation[153]. L'adoption de logiciels espions mercenaires en l'absence de systèmes de contrôle efficaces permettant de garantir leur utilisation conforme à la législation nationale par les organismes gouvernementaux canadiens risque de

---

des Nations Unies <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulat ion-ct-spyware-technology-trade.pdf>, p. 18 (Sur la manière dont les justifications liées à la lutte contre le terrorisme et les définitions vagues du terme « terrorisme » ont permis aux gouvernements d'acquérir des pouvoirs « en grande partie non contrôlés » pour surveiller les citoyens « tant que cela était lié, d'une manière ou d'une autre, à des objectifs généraux et autodéfinis de lutte contre le terrorisme ».)

[148] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, « 031/1/44 – Témoignages – Le lundi 8 août 2022 » *la Chambre des communes, Canada* <https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/reunion-31/temoignages> (Pour les commentaires du député Damien Kurek, notamment : « Sauf votre respect, monsieur le ministre, vous êtes le représentant élu, le ministre du Cabinet, qui assure la surveillance que les Canadiens attendent. Le fait que nous obtenions des réponses moins que directes m'apparaît très, très révélateur de cette culture du secret qui semble impliquer… Bien sûr, j'entends souvent des citoyens qui sont frustrés par les interventions de ce gouvernement lorsqu'il s'agit de sa réticence à faire preuve de transparence en répondant à ce que je pense être des questions très, très simples »).

[149] Voir p. ex. : Clark Campbell (2022), « A Government that Misses Step One in Transparency Sparks a Tizzy about 'Surveillance' », *The Globe and Mail* (11 janvier 2022) <https://www.theglobeandmail.com/politics/article-a-government-that-misses-step-one-in-transparency-sparks-a-tizzy> (Examen de la manière dont l'absence d'informations claires préalables concernant la collecte de données par l'Agence de la santé publique du Canada pour lutter contre la COVID-19 a contribué à susciter des inquiétudes au sein de la population quant à la surveillance de masse et à ébranler la confiance envers le gouvernement.)

[150] Parsons, Christopher, et Adam Molnar (2018), « Government Surveillance Accountability: The Failures of Contemporary Canadian Interceptions Reports », *Canadian Journal of Law and Technology* 1(16), p. 150.

[151] Parsons, Christopher, et Adam Molnar (2018), « Government Surveillance Accountability: The Failures of Contemporary Canadian Interceptions Reports », *Canadian Journal of Law and Technology* 1(16), p. 150.

[152] Consulter p. ex. : Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », *la Chambre des communes, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf>, p. 14.

[153] Peter Königs (2022), « Government Surveillance, Privacy and Legitimacy », *Philosophy and Technology* 8(35), p. 13.

porter atteinte aux droits de la personne et de contribuer à la « régression démocratique » observée dans le monde entier ces dernières années[154].

Menaces découlant de la prolifération des logiciels espions mercenaires

L'utilisation de logiciels espions contre des fonctionnaires, évoquée plus haut, fait de la prolifération de cette technologie une menace pressante pour la sécurité nationale. Le gouvernement canadien n'est pas à l'abri des risques liés à la multiplication des logiciels espions sur le marché. La prévalence de l'utilisation de ces produits rend les institutions et les fonctionnaires canadiens de plus en plus vulnérables à de tels actes de cyberespionnage, qui compromettent la mission des institutions gouvernementales canadiennes et nos intérêts en matière de sécurité nationale.

En se positionnant comme un autre client consentant (en supposant qu'il achète sur le marché privé), le gouvernement canadien contribue à la croissance mondiale du marché des logiciels espions et à la propagation des dangers qui y sont associés[155]. La stagnation de l'action législative du Canada dans ce domaine permet également au marché de prospérer. Comme l'a récemment souligné la Rapporteuse spéciale sur les droits de l'homme et la lutte antiterroriste :

> « La responsabilité de ces problèmes graves incombe non seulement aux entités privées qui développent ces technologies et qui soit les fournissent directement en toute connaissance de cause à des régimes coupables de violations des droits, soit manquent à leur devoir de précaution concernant l'utilisation finale de leur produit, mais aussi aux organes de l'État qui font une mauvaise utilisation de ces technologies, sans respecter le droit international et le droit interne, et aux États et organisations internationales qui soit contribuent activement à ce que ces technologies tombent entre de mauvaises mains, soit, faute de réglementation suffisamment solide, ne sont pas parvenus à l'empêcher[156]. »

Le Canada est à la traîne par rapport aux États-Unis et à l'Union européenne dans sa réponse aux menaces posées par les logiciels espions mercenaires. Le seul outil réglementaire concret au Canada qui a un impact sur le marché des logiciels espions est l'obligation pour les entreprises canadiennes de demander des licences pour exporter des technologies à double usage[157]. Toutefois, les recherches montrent que les contrôles à l'exportation n'ont pas permis à eux seuls de répondre aux préoccupations en matière de droits

---

[154] Ronald J. Deibert (2022), « Subversion Inc: The Age of Private Espionage », *Journal of Democracy* 2(33), p. 39.
[155] Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (2023), « Position paper on Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach », *Procédures spéciales du Conseil des droits de l'homme des Nations Unies* <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf>, p. 22 (« [traduction] Les États doivent être conscients du risque que le développement de telles technologies dans le secteur privé, ainsi que leur diffusion au moyen du commerce et de partenariats entre États, soulève des risques de transfert et de dispersion de cette technologie vers des environnements répressifs, et entre les mains de criminels ou d'organisations terroristes désignées par l'ONU »).
[156] [156] Conseil des droits de l'homme des Nations Unies (2023), « Effets sur les droits de l'homme de la mise au point, de l'utilisation et du transfert de nouvelles technologies dans le cadre de la lutte antiterroriste et de la prévention et de la répression de l'extrémisme violent », 52e sess., Doc ONU A/HRC/52/39 <https://docs.un.org/fr/A/HRC/52/39>, par. 46.
[157] Anstis, Siena, Ronald J. Deibert, et Angela Yang (2022), « Mémoire présenté au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11921005/br-external/CitizenLab-10662114_001-f.pdf ation-Privacy-and-Ethics.pdf>, p. 6.

de le personne associées aux logiciels espions[158]. Ces contrôles ne concernent notamment que l'exportation de technologies de surveillance qui relèvent du champ d'application précis des articles énumérés dans les dispositions relatives aux produits à double usage de la *Loi sur les licences d'exportation et d'importation*, L.R.C. (1985), chap. E-19. Cette loi ne réglemente pas l'achat ou l'utilisation de ces technologies par le gouvernement canadien.

Les audiences du Comité ETHI, tenues en 2022, ont constitué le premier débat public au Canada sur cette question de portée mondiale[159]. Le comité a ensuite publié un rapport contenant neuf recommandations concernant l'utilisation des OEE par la GRC[160]. Le rapport faisait notamment ressortir que l'absence de réponse politique significative de la part du gouvernement canadien compromet la protection des droits de la personne, la démocratie et l'état de droit, et menace la sécurité nationale. Il est difficile de savoir comment le gouvernement canadien a mis en œuvre l'une ou l'autre des recommandations et s'il existe une volonté politique ou un intérêt à le faire.

Conclusion et recommandations

L'inaction face à l'utilisation de logiciels espions par les organismes gouvernementaux canadiens, sans contrôle suffisant ni obligation de rendre compte, entraîne des risques importants pour les protections prévues par la Constitution canadienne et les droits de la personne. Elle menace également la sécurité nationale, car la prolifération de cette technologie rend les organismes gouvernementaux canadiens plus vulnérables à la surveillance par des acteurs hostiles. L'inaction face à des États autoritaires et quasi démocratiques qui utilisent illégalement des logiciels espions mercenaires nuit à la réputation internationale du Canada en tant que pays engagé à respecter et à défendre le droit international en matière de défense des droits de la personne[161]. En outre, le Canada ne protège pas les communautés vulnérables ciblées par cette technologie, comme les DDP, les journalistes et les dissidents qui se sont réfugiés au Canada ou y ont immigré.

Des mesures concrètes sont nécessaires pour contribuer à la prévention de l'utilisation abusive des logiciels espions à l'échelle nationale et pour lutter contre la croissance internationale de l'industrie

[158] McKune, Sarah, et Ronald J. Deibert (2017), « Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking », *Citizen Lab (Munk School of Global Affairs & Public Policy, Université de Toronto)* <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf>, p. 7; Heejin Kim (2021), « Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue », *The International & Comparative Law Quarterly* 2(70) <https://www.cambridge.org/core/journals/international-and-compar.tive-law-quarterly/article/global-export-controls-of-cybe r-surveillance-technology-and-the-disrupted-triangular-dialogue/3C755DA93E2E1F1F90D38179173334CA>, p. 380; Anstis, Siena, et RJ Reid (2023), « The Adverse Human Rights Impacts of Canadian Technology Companies: Reforming Export Control with the Introduction of Mandatory Human Rights Due Diligence », *Canadian Journal of Law and Technology* 1(19) <https://digitalcommons.schulichlaw.dal.ca/cjlt/vol19/iss1/3/>.

[159] Ronald J. Deibert, le directeur du Citizen Lab, a témoigné devant le Comité permanent au sujet des capacités technologiques uniques des logiciels espions, des risques pour les droits de la personne, le public et la sécurité nationale associés à ces logiciels, de la nature non réglementée de l'industrie mercenaire des logiciels espions, et de la nécessité de tenir un débat public et d'élaborer un cadre juridique particulier pour l'utilisation des logiciels espions par les organismes gouvernementaux.

[160] Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (2022), « outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », *Chambre des communes, Canada* <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf> pp. 3–4.

[161] Branda McPhail (2022), « Oral Submission to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) for the Study of Device Investigation Tools Used by the Royal Canadian Mounted Police », *Association canadienne des libertés civiles* <https://ccla.org/wp-content/uploads/2022/08/9-Aug-2022-ETHI-Committee-Submission-on-RCMP-ODIT-Copy.pdf>.

mercenaire des logiciels espions[162]. Dans ce contexte, nous demandons instamment au CPSNR de recommander au gouvernement du Canada de prendre les mesures préliminaires qui suivent concernant les logiciels espions mercenaires :

1. Imposer un moratoire sur la vente, l'exportation, le transfert et l'utilisation de logiciels espions jusqu'à ce qu'un régime de garanties respectueux des droits de la personne soit mis en place.
2. Créer un organe indépendant de surveillance de l'utilisation des logiciels espions par les organismes gouvernementaux canadiens.
3. Élaborer une législation visant à accroître la transparence du marché des logiciels espions, tant au niveau national qu'international (exiger par exemple que la communauté du renseignement présente au Parlement des rapports réguliers sur les sociétés de logiciels espions nationales et internationales et sur les menaces qui pèsent sur le Canada).
4. Prescrire légalement des conditions précises pour le piratage et la surveillance par le gouvernement à l'aide de logiciels espions, conformément à la Charte et au droit international en matière de droits de la personne (en particulier, par le biais d'éventuelles réformes du *Code criminel*).
5. Mettre en place des recours efficaces pour les victimes visées par des logiciels espions et infectées par ceux-ci, en réformant ou en renforçant les lois afin de faciliter la responsabilisation des gouvernements et des entreprises en cas d'utilisation abusive de ce type de logiciels.
6. Prévoir un processus national d'évaluation et de gestion des vulnérabilités.
7. Faire de la diligence raisonnable en matière de droits de la personne une obligation légale pour les entreprises de logiciels espions, en prévoyant des sanctions appropriées en cas de non-respect de celle-ci.
8. Imposer des sanctions aux entreprises et aux personnes actives dans le domaine des logiciels espions qui contribuent au non-respect des droits de la personne, notamment en établissant une liste noire afin d'identifier les entreprises auprès desquelles les organismes gouvernementaux canadiens ne peuvent acheter de technologies, et en harmonisant les sanctions avec celles des États-Unis et de l'Union européenne.
9. Mettre fin à la fourniture d'aide, d'équipements et de formations en matière de sécurité ou de surveillance à l'étranger auxquels des gouvernements étrangers pourraient avoir recours pour commettre des abus contre les droits de la personne.

[162] Conseil des droits de l'homme des Nations Unies (2023), « Effets sur les droits de l'homme de la mise au point, de l'utilisation et du transfert de nouvelles technologies dans le cadre de la lutte antiterroriste et de la prévention et de la répression de l'extrémisme violent », 52e sess., Doc ONU A/HRC/52/39 <https://docs.un.org/fr/A/HRC/52/39>. p. 46.