DANS LES MAILLES DE PREDATOR

LA MENACE MONDIALE D'UN LOGICIEL ESPION « RÉGLEMENTÉ PAR L'UNION EUROPÉENNE »

SYNTHÈSE

AMNESTY INTERNATIONAL

Amnesty International est un mouvement rassemblant 10 millions de personnes qui fait appel à l'humanité en chacun et chacune de nous et milite pour que nous puissions toutes et tous jouir de nos droits humains. Notre vision est celle d'un monde dans lequel les dirigeants et dirigeantes tiennent leurs promesses, respectent le droit international et sont tenus de rendre des comptes. Indépendante de tout gouvernement, de toute idéologie politique, de tout intérêt économique et de toute religion, Amnesty International est essentiellement financée par ses membres et des dons de particuliers. Nous avons la conviction qu'agir avec solidarité et compassion aux côtés de personnes du monde entier peut rendre nos sociétés meilleures.

Édition originale publiée en 2023
par Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Royaume-Uni

Index : ACT 10/7246/2023
Langue originale : anglais

amnesty.org

Illustration de couverture : *© Colin Foo 2023*

AMNESTY INTERNATIONAL

SYNTHÈSE

Ces dix dernières années, des organisations de la société civile, des chercheurs et chercheuses et des journalistes ont révélé que des gouvernements du monde entier prenaient illégalement pour cible des militant·e·s, des journalistes et des personnalités politiques au moyen d'outils conçus par des entreprises privées de cybersurveillance. Amnesty International et de nombreuses autres organisations de la société civile ont averti à maintes reprises que l'opacité du commerce et du déploiement par les États de technologies de surveillance fabriquées par des acteurs privés, en particulier de logiciels espions, provoquait une crise de la surveillance numérique, avec de graves effets préjudiciables sur les droits humains, la liberté de la presse et les mouvements sociaux à travers le monde. En 2021, les révélations du projet Pegasus (sur le caractère mondial et l'ampleur de la surveillance illégale permise par le logiciel espion Pegasus, du groupe NSO) et les recherches menées ensuite par la société civile ont contraint les gouvernements de la planète à reconnaître le caractère massif des utilisations abusives de logiciels espions et ont déclenché un début d'action visant à mettre un frein aux activités de certains vendeurs de logiciels espions les plus tristement célèbres. Cependant, les révélations récentes d'Amnesty International et les conclusions de la nouvelle enquête sur le logiciel espion Predator, coordonnée par le réseau d'investigation journalistique European Investigative Collaborations (EIC), ont mis au jour l'insuffisance et l'inefficacité des mesures prises par les gouvernements pour mettre un terme à l'utilisation abusive de logiciels espions. Le présent rapport détaille ces conclusions.

Dans le cadre de l'enquête sur Predator, le Security Lab d'Amnesty International a collaboré, en tant que partenaire technique, avec EIC, un réseau européen d'organisations du secteur des médias. Amnesty International a analysé les documents que s'était procurés EIC afin d'établir les spécifications techniques d'une suite de produits de surveillance conçus, mis en œuvre et commercialisés par l'alliance Intellexa (une alliance d'entreprises du secteur des technologies de surveillance) entre 2007 et 2022. Elle a découvert que cette suite comprenait un vaste éventail de technologies de surveillance ciblée et de surveillance de masse.

Parmi les outils de surveillance ciblée figurent des logiciels espions hautement intrusifs, comme Predator, qui peut être installé sur un appareil mobile au moyen d'une attaque « un clic » ou « zéro clic ». L'alliance Intellexa propose aussi différentes techniques pour installer le logiciel espion *via* des « attaques tactiques », qui permettent de prendre pour cible les appareils situés à proximité. Elle a par ailleurs élaboré, mis en œuvre et commercialisé des méthodes d'infection stratégique. Ces méthodes permettent à un acteur gouvernemental d'envoyer des tentatives d'infection silencieuse aux client·e·s des fournisseurs d'accès Internet qui acceptent de coopérer, ou aux internautes d'un pays entier si l'opérateur du logiciel espion a un accès direct au trafic Internet. Les systèmes d'infection stratégique s'apparentent à des outils de surveillance de masse car ils nécessitent de passer par le trafic Internet général pour attaquer des personnes individuelles et infecter leurs appareils. Les produits de surveillance de masse proposés par l'alliance Intellexa montrent une évolution des technologies en la matière : les méthodes de surveillance générale et non ciblée semblent en effet prendre le pas sur les systèmes d'interception légaux utilisés auparavant, qui permettaient une surveillance ciblée et individualisée des communications et étaient plus faciles à contrôler et à restreindre.

Amnesty International considère que ces deux types de technologies (les logiciels espions hautement intrusifs et les outils de surveillance de masse non ciblée) sont fondamentalement incompatibles avec les droits humains. Le logiciel espion Predator, ainsi que ses variantes aux noms divers, sont des logiciels espions hautement intrusifs qui peuvent accéder à une quantité illimitée de données sur les appareils infectés et qui ne peuvent, à l'heure actuelle, faire l'objet d'aucun contrôle indépendant. De ce fait, selon

l'analyse d'Amnesty International, Predator et les autres logiciels espions hautement intrusifs du même type ne peuvent pas être déployés dans le respect des droits fondamentaux, et doivent donc être interdits.

Dans ce rapport, Amnesty International révèle également une opération de surveillance ciblée, jusqu'ici restée secrète, menée par un client du logiciel espion Predator, en lien avec le Viêt-Nam. Ce client semble avoir des intérêts proches de ceux du gouvernement vietnamien et a pris pour cible, entre février et juin 2023, 50 comptes de réseaux sociaux appartenant à 27 particuliers et 23 institutions, au moyen d'outils d'espionnage numérique élaborés et vendus par l'alliance Intellexa. Il s'agissait d'attaques « un clic » : les personnes et institutions concernées ont reçu sur leurs comptes de réseaux sociaux un message du compte X (ex-Twitter) @Joseph_Gordon16 les invitant à cliquer sur un lien. Parmi les comptes visés par cette attaque figuraient ceux d'un site d'information indépendant basé à Berlin, de personnalités politiques du Parlement européen, de membres de la Commission européenne, de chercheurs et chercheuses universitaires, et de groupes de réflexion. Le message a aussi été envoyé à des responsables des Nations unies, la présidente taiwanaise, des sénateur·rice·s et représentant·e·s des États-Unis et d'autres autorités diplomatiques.

Le Groupe d'analyse des menaces de Google (TAG) a confirmé à Amnesty International avoir déterminé que les noms de domaine et les URL découverts par le Security Lab dans le cadre de ces attaques au logiciel espion étaient liés à Predator. Combinées aux éléments de preuve recueillis par nos partenaires de l'EIC, nos conclusions prouvent que des produits de surveillance de l'alliance Intellexa ont été vendus au ministère vietnamien de la Sécurité publique, et semblent indiquer que des membres des autorités vietnamiennes, ou des personnes agissant en leur nom, pourraient être derrière cette campagne d'espionnage numérique. La société Google a par ailleurs confirmé à l'EIC qu'elle « associait » la campagne menée au moyen du logiciel espion Predator et les indicateurs détaillés dans ce rapport à « un acteur gouvernemental au Viêt-Nam ».

Ces révélations s'appuient sur les recherches techniques menées de façon continue par le Security Lab d'Amnesty International pour suivre l'évolution et le déploiement des technologies de surveillance commercialisées par des entreprises mercenaires de logiciels espions, comme les technologies proposées par l'alliance Intellexa. Dans le cadre de ce travail, Amnesty International a analysé une infrastructure technique récente liée au système de logiciel espion Predator, qui révèle l'existence probable de clients actifs ou d'attaques de particuliers en Angola, en Égypte, en Indonésie, au Kazakhstan, à Madagascar, en Mongolie, au Soudan et au Viêt-Nam, entre autres.

Les conclusions du présent rapport se fondent également sur un entretien avec un journaliste vietnamien visé, sur l'analyse de registres de livraison et de données commerciales, et sur d'autres recherches et rapports de l'EIC sur les ventes de solutions de surveillance et d'infection de l'alliance Intellexa. Amnesty International a aussi examiné des rapports, des déclarations, des textes de loi et des études d'organes et de spécialistes des Nations unies et d'autorités régionales et nationales de différents niveaux, des rapports d'enquête et de politique d'organisations de la société civile, et des articles de presse.

D'autre part, ce rapport analyse les conséquences sur les droits humains des révélations de l'enquête sur Predator, qui montrent qu'une suite de technologies de surveillance hautement intrusives fournie par l'alliance Intellexa est vendue et transférée dans le monde entier en toute impunité. L'alliance Intellexa se compose de plusieurs entreprises vendant des outils de surveillance, qui sont présentes dans des États membres de l'Union européenne (UE) et ailleurs dans le monde. L'enquête révèle le caractère mondial et l'ampleur des transferts de technologies de surveillance réalisés par une seule alliance de vendeurs, qui a livré ses produits en Arabie saoudite, en Égypte, en France, en Libye, à Madagascar et au Viêt-Nam, entre autres, entre 2007 et 2022. Compte tenu de précédents cas de surveillance illégale dans ces pays et/ou de l'absence de garanties nationales susceptibles d'empêcher que ces technologies soient déployées illégalement contre la société civile, des journalistes ou des personnalités politiques d'opposition, il est hautement probable que ces transferts aient donné lieu à des violations des droits humains.

Enfin, ce rapport fait état d'antécédents d'atteintes aux droits humains liées à l'alliance Intellexa en Égypte, en Grèce et en Libye. Intellexa se vante d'être « une entreprise basée dans l'UE et soumise à la réglementation européenne ». L'alliance se compose semble-t-il de Nexa Technologies et d'Advanced Middle East Systems (qui forment le groupe Nexa), ainsi que de WiSpear, Cytrox et Senpai Technologies (qui forment le groupe Intellexa). Les groupes Nexa et Intellexa contrôlent de nombreuses entités commerciales, dont certaines ont été rebaptisées. Celles-ci sont basées dans différents pays, dans et en dehors de l'UE. La nature exacte des liens entre ces entreprises est entourée de secret, les entités commerciales et les structures qui les relient étant en constante mutation et évolution, et changeant régulièrement de nom ou de marque. Il apparaît que ces structures commerciales opaques et complexes permettent aux entreprises d'échapper plus facilement à l'obligation de rendre des comptes, à la transparence et aux réglementations gouvernementales, notamment aux contrôles régionaux et nationaux des exportations et aux mécanismes

d'obligation de diligence. Dans le cas de l'alliance Intellexa, le tableau est encore plus complexe, car les structures commerciales sont composées non seulement d'une entreprise principale, mais aussi de ses vendeurs associés de produits de surveillance, de ses sociétés mères et de leurs investisseurs. La nature alambiquée de cette entité commerciale risque de compliquer encore davantage l'obligation de rendre des comptes et la transparence en cas d'usages illégaux des outils de surveillance de cette alliance.

Comme l'indiquent les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme (Principes directeurs de l'ONU), les entreprises sont tenues de respecter les droits humains, quel que soit l'endroit dans le monde où elles mènent leurs activités. Pour remplir cette obligation, elles doivent faire preuve de la diligence requise en la matière. Les entreprises qui composent l'alliance Intellexa n'ont révélé, de leur propre initiative, aucune information sur leurs pratiques en ce sens. Les évaluations – si toutefois elles existent – des conséquences de leurs technologies de surveillance sur les droits fondamentaux sont tenues secrètes. En vertu du droit international relatif aux droits humains, les États ont également l'obligation de protéger les personnes des atteintes à leurs droits que pourraient commettre des tiers. Cela inclut l'obligation de réglementer le comportement des entreprises qui sont domiciliées sur leur territoire ou se trouvent sous leur autorité effective, afin de les empêcher de causer des atteintes aux droits humains ou d'y contribuer, même dans d'autres pays. Le fait que les États n'aient pas exercé un réel contrôle sur l'alliance Intellexa (notamment les États où sont basées les entreprises qui la composent, comme l'Allemagne, Chypre, les Émirats arabes unis, la France, la Grèce, la Hongrie, l'Irlande, Israël, la Macédoine du Nord, la République tchèque et la Suisse) a entraîné des violations des droits humains. Considérées conjointement, les conclusions évoquées ci-dessus montrent que la société civile et les journalistes sont toujours confrontés aux conséquences dévastatrices de la surveillance numérique illégale et non contrôlée, qui continue de menacer les droits au respect de la vie privée et à la liberté d'expression, d'association et de réunion pacifique des personnes visées. En outre, comme détaillé dans ce rapport, le fait que des membres d'autorités officielles régionales, nationales et internationales aient été pris pour cible montre une nouvelle fois que les logiciels espions commerciaux ont de graves répercussions à la fois sur les droits humains et sur la sécurité de l'écosystème numérique. Non réglementées, ces technologies de surveillance peuvent se retourner contre des gouvernements et autres autorités de pays tiers – ce qui a d'ailleurs déjà été le cas.

Ces conclusions ne sont que la partie émergée de l'iceberg. Tandis que les entreprises de surveillance et les États auxquels elles vendent leurs produits continuent de se cacher derrière les arguments de la sécurité nationale et de la confidentialité pour échapper à la transparence et à l'obligation de rendre des comptes, les attaques illégales menées au moyen d'outils fournis par l'alliance Intellexa ont toutes les chances de se multiplier et de prendre de l'ampleur. Sur la base des avertissements de la société civile et des enseignements tirés du projet Pegasus, on peut conclure que, dans chacun des pays où l'enquête révèle que l'alliance Intellexa a vendu ses technologies, la société civile risque d'être confrontée à une surveillance clandestine généralisée. Ces nouvelles révélations indiquent clairement, une nouvelle fois, que la vente et le transfert non contrôlés de technologies de surveillance risquent de continuer à favoriser des atteintes massives aux droits humains dans le monde entier, puisque les entreprises sont toujours autorisées à commercialiser librement leurs produits dans le plus grand secret. Nos conclusions montrent une fois de plus que toutes les affirmations des entreprises selon lesquelles les attaques illégales relèvent d'utilisations anormales de leurs technologies sont résolument fausses. Les atteintes aux droits humains sont une caractéristique de ce secteur, pas le résultat d'un dysfonctionnement.

À la suite des révélations du projet Pegasus, les États ont pris des mesures qui allaient dans le bon sens pour réglementer ce secteur et l'utilisation de ces technologies par les acteurs gouvernementaux. Certaines sont importantes et constituent un pas dans la bonne direction, qu'il convient de saluer. Cependant, les déclarations publiques, recommandations et engagements volontaires n'ont pas toujours été suivis des faits, et des personnes prises pour cible illégalement par des logiciels espions partout dans le monde n'ont toujours pas obtenu de comptes ou de réparations dignes de ce nom. Si certains États ont pris volontairement des initiatives, d'autres ont bloqué des enquêtes et n'ont pas fait preuve d'une véritable transparence. Des efforts plus concertés de leur part sont nécessaires pour mettre en place des garanties contraignantes et opposables visant à protéger les droits humains aux niveaux national, régional et international. En 2019, le rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression a déclaré : « Dire que le mécanisme global de contrôle de l'utilisation des technologies de surveillance ciblée ne fonctionne pas est un euphémisme. En réalité, ce mécanisme est pratiquement inexistant. » Amnesty International estime que c'est toujours le cas, malgré quelques premiers progrès.

En particulier, les dernières révélations dressent un tableau affligeant de l'incapacité de l'UE et de ses États membres à maîtriser des entreprises échappant à tout contrôle et des États membres indisciplinés, qui

continuent de profiter des larges failles manifestes des systèmes réglementaires régionaux et nationaux. La campagne de surveillance éhontée décrite dans ce rapport, menée au moyen de produits commercialisés par l'alliance Intellexa, montre les risques très directs de la prolifération et du transfert incontrôlés des outils de cybersurveillance depuis des pays de l'UE. Non seulement ceux-ci donnent lieu à des atteintes aux droits humains à l'étranger, mais ils constituent aussi une menace pour la sécurité et les droits fondamentaux au sein de l'UE.

Les exportations de logiciels espions à partir de l'UE sont soumises à autorisation en vertu du Règlement européen sur les biens à double usage, aux termes duquel les autorisations devraient, en théorie, tenir compte des risques que posent de telles exportations en matière de droits humains. Or, les révélations de l'enquête sur Predator montrent que des licences d'exportation de technologies de surveillance ont été accordées par des États membres alors qu'il existait un risque substantiel de violations des droits humains par les utilisateurs finaux. Les conclusions de l'enquête révèlent également que le recours à des structures et des entités commerciales opaques situées dans des pays tiers a permis de contourner la réglementation européenne relative au contrôle des exportations. Il est clair que le Règlement de l'UE sur les biens à double usage comporte d'importantes lacunes. Deux ans après sa refonte, il n'est toujours pas appliqué de façon ferme et transparente. La Commission d'enquête du Parlement européen chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (Commission PEGA) a aussi dénoncé le manque de volonté politique de l'UE et de ses États membres. Alors que des initiatives législatives en cours, comme la Proposition de directive sur le devoir de vigilance des entreprises en matière de durabilité, offrent une occasion opportune de commencer à s'attaquer aux préjudices causés par le secteur de la surveillance ciblée, les lacunes des propositions avancées par les colégislateurs de l'UE risquent d'avoir pour conséquence que cette directive ne s'appliquera pas correctement aux entreprises du secteur des technologies de surveillance.

PRINCIPALES RECOMMANDATIONS AUX ÉTATS

Compte tenu de l'inefficacité de la réglementation actuelle, ainsi que de la nature intrinsèquement abusive de Predator, tous les États doivent :

- (en particulier les États qui ont accordé des licences d'exportation) révoquer immédiatement toutes les autorisations de commercialisation et de d'exportation accordées à l'alliance Intellexa et mener une enquête indépendante, impartiale et transparente pour déterminer l'ampleur des actes illégaux commis, enquête qui devra déboucher sur une déclaration publique à propos des résultats des efforts menés et des mesures proposées pour empêcher de nouveaux préjudices à l'avenir ;
- interdire l'utilisation des logiciels espions hautement intrusifs. En effet, pour l'instant ces logiciels ne peuvent pas être contrôlés de façon indépendante et leurs fonctionnalités ne peuvent pas être limitées à ce qui est nécessaire et proportionné par rapport à un usage et un objectif spécifiques ;
- mettre en place un cadre réglementaire de protection des droits humains qui régisse les activités de surveillance et qui soit conforme aux normes internationales relatives aux droits humains. Tant qu'un tel cadre n'aura pas été mis en place, il conviendra d'appliquer un moratoire sur l'achat, la vente, le transfert et l'utilisation de tous les logiciels espions ;
- mettre en œuvre une législation nationale qui offre des garanties contre les atteintes aux droits humains causées par la surveillance numérique et créer des mécanismes d'obligation de rendre des comptes destinés à offrir une voie de recours aux victimes de surveillance abusive ;
- imposer juridiquement aux entreprises du secteur de la surveillance de faire preuve de la diligence requise en matière de droits humains dans leurs activités partout dans le monde, notamment en ce qui concerne l'utilisation de leurs produits et services.

PRINCIPALES RECOMMANDATIONS À L'UNION EUROPÉENNE ET À SES ÉTATS MEMBRES

- Les États membres de l'UE et la Commission européenne doivent veiller à ce que la réglementation européenne de 2021 sur le contrôle des exportations soit fermement appliquée, ce qui implique de prendre des mesures immédiates pour insister sur les obligations de diligence relative aux droits fondamentaux qui découlent du Règlement de l'UE sur les biens à double usage et pour créer un marché transparent des technologies de surveillance, soumis à des garanties efficaces en matière de droits humains.
- Les États membres de l'UE doivent adopter et mettre en œuvre une législation imposant à toutes les entreprises de respecter les droits humains et de prendre des mesures pour appliquer la diligence requise en la matière, conformément aux Principes directeurs de l'ONU. Dans le cadre des délibérations en cours sur la Proposition de directive sur le devoir de vigilance des entreprises en matière de durabilité, l'Union européenne doit exiger des entreprises qu'elles appliquent la diligence requise en matière de droits humains à toute leur chaîne de valeur, c'est-à-dire à l'achat, à la vente, au transfert, à l'exportation et à l'utilisation des produits. Les obligations découlant de la Directive sur le devoir de vigilance des entreprises en matière de durabilité doivent s'appliquer aux entreprises de tous les secteurs, y compris aux fabricants de logiciels espions, ainsi qu'aux institutions financières.

PRINCIPALES RECOMMANDATIONS AU GOUVERNEMENT VIETNAMIEN

Le gouvernement vietnamien doit mener une enquête indépendante, impartiale et transparente sur la surveillance ciblée illégale dont il est fait état dans ce rapport, afin notamment de déterminer s'il existe des liens entre cette campagne d'attaques au logiciel espion et des organes gouvernementaux.

PRINCIPALES RECOMMANDATIONS À L'ALLIANCE INTELLEXA

L'alliance Intellexa doit cesser la production et la commercialisation de Predator et de tout autre logiciel espion hautement intrusif ne contenant pas les garanties techniques nécessaires pour permettre son utilisation légale dans un cadre réglementaire respectueux des droits humains. Elle doit aussi offrir une indemnisation satisfaisante ou d'autres formes de réparation effective aux victimes de surveillance illégale.

AMNESTY INTERNATIONAL EST UN MOUVEMENT MONDIAL DE DÉFENSE DES DROITS HUMAINS. LORSQU'UNE INJUSTICE TOUCHE UNE PERSONNE, NOUS SOMMES TOUS ET TOUTES CONCERNÉ·E·S.

NOUS CONTACTER


info@amnesty.org


+44 (0)20 7413 5500

PRENDRE PART À LA CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty