DANS LES MAILLES DE PREDATOR

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

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 10/7245/2023
Langue originale : anglais

amnesty.org

Illustration de couverture : *© Colin Foo 2023*

AMNESTY INTERNATIONAL

SOMMAIRE

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

Index : ACT 10/7245/2023
Langue originale : anglais

amnesty.org

Illustration de couverture : *© Colin Foo 2023*

AMNESTY INTERNATIONAL

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

Index : ACT 10/7245/2023
Langue originale : anglais

amnesty.org

Illustration de couverture : *© Colin Foo 2023*

AMNESTY INTERNATIONAL

GLOSSAIRE

TERME	DÉFINITION
LOGICIEL ESPION	Un *logiciel espion* est un logiciel qui permet à un opérateur d'accéder secrètement aux informations contenues dans le système d'un ordinateur ou de tout autre appareil visé.
LOGICIEL ESPION COMMERCIAL	Un *logiciel espion commercial* ou *mercenaire* est un produit de surveillance élaboré et vendu par une entreprise à des gouvernements pour leur permettre de mener à bien des opérations de surveillance. Les logiciels espions commerciaux dits « de bout en bout » offrent une solution complète d'infection des appareils et de collecte de données. Ces solutions comprennent le code d'exploitation d'une faille de sécurité permettant d'installer le logiciel espion, un implant de logiciel espion qui tourne sur l'appareil infecté, et des dispositifs finaux de collecte et d'analyse des données de surveillance.
IMPLANT DE LOGICIEL ESPION	L'*implant d'un logiciel espion* est le code logiciel final qui est installé sur un ordinateur ou un téléphone après son infection. Cet implant se charge de collecter les données sur l'appareil, d'activer les capteurs tels que les micros ou les caméras, et de transmettre ces données à l'opérateur du logiciel espion.
VULNÉRABILITÉ LOGICIELLE	Une *vulnérabilité logicielle* est une faille ou une faiblesse technique dans un composant ou un élément de code d'un logiciel qui peut être exploitée par un attaquant pour contourner les défenses de sécurité.
CODE D'EXPLOITATION *(EXPLOIT)*	Un *code d'exploitation* (ou *exploit*) est un élément de logiciel ou de code qui met à profit (ou exploite) une ou plusieurs vulnérabilités logicielles pour accéder à un appareil. Sur les appareils mobiles modernes, les codes d'exploitation doivent contourner de nombreuses défenses de sécurité sur plusieurs niveaux et peuvent être très complexes. Une chaîne complète de codes d'exploitation visant les appareils les plus récents peut se vendre plusieurs millions d'euros.

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

Index : ACT 10/7245/2023
Langue originale : anglais

amnesty.org

Illustration de couverture : *© Colin Foo 2023*

AMNESTY INTERNATIONAL

TERME	DÉFINITION
PROCESSEUR DE BANDE DE BASE *(BASEBAND)*	Le terme *processeur de bande de base* (ou *baseband*) désigne les composants matériels et logiciels d'un téléphone mobile qui lui permettent de communiquer, *via* une interface radio, avec une antenne-relais ou une station de base de téléphonie mobile.
FAILLE NON CORRIGÉE *(ZERO-DAY)*	Une *faille non corrigée*, ou *vulnérabilité zero-day*, est une faille logicielle dont le développeur du logiciel n'a pas connaissance et pour laquelle il n'existe pas de correctif. Un code d'exploitation tirant profit d'une telle faille peut infecter avec succès même les appareils qui sont totalement à jour et ont bénéficié des corrections les plus récentes.
VECTEUR D'ATTAQUE	Dans le secteur de la surveillance, on appelle *vecteurs d'attaque* les différentes méthodes ou techniques pouvant être utilisées pour infecter un appareil visé au moyen d'un code d'exploitation, comme les vecteurs dits « un clic » et « zéro clic ».
UN CLIC	Une attaque *« un clic »* nécessite une action de la cible pour que l'infection de son appareil soit effective (généralement l'ouverture d'un lien malveillant). Différentes techniques d'ingénierie sociale sont utilisées pour duper la cible afin de l'inciter à ouvrir le lien en question, par exemple l'imitation de sites officiels ou d'articles d'actualités. Si l'on clique sur le lien, une chaîne de codes d'exploitation est téléchargée en vue d'affaiblir le navigateur Internet puis d'installer l'implant du logiciel espion sur l'appareil visé.
ZÉRO CLIC	Dans le secteur de la surveillance, on parle d'attaque *« zéro clic »* pour désigner un vecteur qui peut infecter un appareil sans aucune action de son utilisateur, par exemple sans qu'il ait à cliquer sur un lien. Les attaques « zéro clic » *entièrement à distance*, ou *sans interaction*, permettent une infection *via* le réseau Internet, souvent en exploitant des failles dans des applications de messagerie populaires comme iMessage ou WhatsApp. Les attaques « zéro clic » *avec interaction*, dites *tactiques,* peuvent infecter des appareils lorsque l'attaquant dispose d'un accès privilégié à un réseau ou se trouve à proximité physique de la cible.
INJECTION RÉSEAU	L'*injection réseau* est une technique qui consiste à injecter des paquets de données dans le trafic Internet afin de bloquer, intercepter ou manipuler ce trafic.
HOMME DU MILIEU – HDM *(MAN-IN-THE-MIDDLE – MitM)*	Un *homme du milieu* est un attaquant qui est en mesure de lire, modifier et bloquer le trafic réseau d'une cible. La fonction HDM peut être utilisée pour censurer la cible ou pour mener des attaques par injection réseau.

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

Index : ACT 10/7245/2023
Langue originale : anglais

amnesty.org

Illustration de couverture : *© Colin Foo 2023*

AMNESTY INTERNATIONAL

TERME	DÉFINITION
MAN-ON-THE-SIDE (MotS)	Dans le cadre d'une attaque de type *« man-on-the-side »*, l'attaquant peut lire et surveiller le trafic réseau mais n'est pas en capacité de le bloquer ou de le modifier directement. Cette situation est courante lorsqu'un attaquant a accès à une copie ou un miroir du trafic transmis par fibre optique. Des attaques par injection réseau peuvent aussi être lancées depuis cette position.
INFECTION TACTIQUE	Un vecteur d'*infection tactique* permet à l'attaquant d'attaquer les appareils situés à proximité. Des réseaux wifi et des stations de base de téléphonie mobile malveillants peuvent être utilisés pour rediriger insidieusement une cible physiquement proche vers un lien de code d'exploitation. Les attaquants peuvent aussi exploiter les vulnérabilités des logiciels de bande de base cellulaires et des interfaces wifi pour infecter les appareils situés à proximité au moyen d'ondes radio.
INFECTION STRATÉGIQUE	L'*infection stratégique* fait référence aux systèmes d'injection réseau déployés au niveau d'un fournisseur d'accès Internet ou du portail Internet d'un pays, qui peuvent être utilisés pour acheminer un logiciel espion. Ces systèmes peuvent intercepter les requêtes non chiffrées envoyées par la cible et rediriger insidieusement son appareil vers un lien de code d'exploitation.
SS7	Le *SS7 (Signaling System Number 7)* est une série de protocoles et de normes de signalisation utilisés dans les réseaux téléphoniques pour réaliser des actions comme l'établissement de la connexion, le routage et l'itinérance entre les opérateurs de téléphonie mobile nationaux et internationaux. Conçu sans les défenses de sécurité modernes, il est exploité par les vendeurs d'outils de surveillance commerciaux pour mener différents types d'attaques, comme le suivi de la localisation et l'interception des communications.
DÉNI DE SERVICE DISTRIBUÉ (DDoS)	Une attaque par *déni de service distribué* est une attaque qui vise à perturber un site Internet ou un réseau en surchargeant son système au moyen d'un trafic excessif ou de requêtes trop nombreuses. Une telle attaque peut rendre un site Internet indisponible pour les visiteurs légitimes.
AVATAR	Un *avatar* est une fausse identité ou un faux compte en ligne qui est utilisé pour recueillir des informations sur des plateformes en ligne ou pour interagir avec l'internaute visé. Ce type de profil ressemblant à un vrai peut servir à envoyer des liens malveillants ciblés ou à diffuser des informations en ligne *via* les réseaux sociaux ou les services de messagerie.

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

Index : ACT 10/7245/2023
Langue originale : anglais

amnesty.org

Illustration de couverture : *© Colin Foo 2023*

AMNESTY INTERNATIONAL

TABLEAU 1 : DESCRIPTIF DES ENTREPRISES

L'alliance Intellexa, ses filiales et ses partenaires ont évolué depuis leur création et sont devenus au fil du temps une structure mondiale complexe. Pour des questions de lisibilité, European Investigative Collaborations (EIC) et Amnesty International décomposent cette structure de la manière suivante :

Nexa group – Nexa Technologies (France)[1], Nexa Technologies CZ s.r.o (République tchèque), Advanced Middle East Systems (Émirats arabes unis), Trovicor fz (Émirats arabes unis)[2].

Groupe Intellexa – WiSpear/Passitora (Chypre)[3], Cytrox (Macédoine du Nord)[4], Cytrox Holdings Zrt (Hongrie), Intellexa S.A (Grèce)[5], Intellexa ltd (Irlande)[6], Thalestris ltd (Irlande)[7].

L'alliance Intellexa[8] est une alliance technologique et commerciale conclue en 2019 entre le groupe Intellexa et le groupe Nexa. Ces deux groupes d'entreprises ont gardé chacun leurs actionnaires. Dans le communiqué de presse annonçant la naissance de cette alliance, les entreprises membres étaient Nexa Technologies, Advanced Middle East Systems, Cytrox, WiSpear et Senpai Technologies[9]. Il est difficile de savoir si l'alliance entre le groupe Nexa et le groupe Intellexa est toujours active aujourd'hui.

Le groupe Intellexa a été créé en 2018 par un ancien militaire israélien, Tal Dilian, et plusieurs de ses associés, et vend le logiciel espion Predator. Depuis 2020, il est contrôlé par la holding Thalestris, qui est basée en Irlande. Les principales entreprises qui le composent sont Cytrox (Macédoine du Nord), développeur du système du logiciel espion Predator, WiSpear (Chypre), spécialiste de l'interception wifi, et Senpai Technologies (Israël), spécialiste de la création d'avatars virtuels et du renseignement obtenu à partir d'informations disponibles en libre accès.

Le groupe Nexa, opérant principalement depuis la France, s'est spécialisé dans les systèmes d'interception du trafic et de surveillance de masse (IP, voix, satellite, IMSI-catchers, analyse de mégadonnées). Il a été créé en 2012 pour reprendre les activités de surveillance de l'entreprise française Amesys. Au départ, il était constitué de Nexa Technologies (France) et d'Advanced Middle East Systems (Dubaï), une société sœur utilisée par Nexa comme bureau commercial. Entre 2019 et 2022, les entreprises du groupe Nexa ont été contrôlées par la holding Boss Industries (France)[10]. En 2019, Boss Industries a racheté l'entreprise Trovicor (Dubaï)[11], spécialisée dans l'« interception légale » (les systèmes de surveillance des communications téléphoniques). En 2020, le groupe Nexa a décidé d'abandonner la marque Nexa Technologies et a commencé à utiliser le nom commercial Trovicor Intelligence[12].

---

[1] Institut national de la propriété intellectuelle (INPI), « Présentation de l'entreprise RB 42 » (consulté le 26 septembre 2023), https://data.inpi.fr/entreprises/751230681?q=751230681#751230681.
[2] Trovicor Intelligence, "Legal Disclosure", https://trovicor.com/legal-disclosure/ (consulté le 26 septembre 2023).
[3] Service du registre des entreprises et de la propriété intellectuelle (consulté le 26 septembre 2023), https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=318328&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1.
[4] Dépositaire central de titres, "Известувања за корпоративни настани", https://www.cdhv.mk/известувања_за_корпоративни_настани.aspx (consulté le 26 septembre 2023).
[5] Chambre de commerce et d'industrie d'Athènes, "Intellexa ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ", 26 septembre 2023, https://directory.acci.gr/companies/details/140944573.
[6] Bureau d'enregistrement des entreprises, "Intellexa Limited", https://core.cro.ie/e-commerce/company/697890 (consulté le 26 septembre 2023).
[7] Bureau d'enregistrement des entreprises, "Thalestris Limited", https://core.cro.ie/e-commerce/company/693992 (consulté le 26 septembre 2023).
[8] Release Wire, "The Intellexa Intelligence Alliance Expands with the Addition of New Members and the Enhancement of Its End-to-End Offering", 20 juin 2019, http://www.releasewire.com/press-releases/the-intellexa-intelligence-alliance-expands-with-the-addition-of-new-members-and-the-enhancement-of-its-end-to-end-offering-1234811.htm.
[9] Ibid.
[10] INPI, « Présentation de l'entreprise BOSS INDUSTRIES » (consulté le 26 septembre 2023), https://data.inpi.fr/entreprises/853120541?q=Boss%20Industries%20#853120541.
[11] Clairfield, "Clairfield advises Boss Industries on the acquisition of Dubai-based company Trovicor", 17 décembre 2019, https://www.clairfield.com/clairfield-advises-boss-industries-on-the-acquisition-of-dubai-based-company-trovicor/.
[12] Intelligence Online, "France: Nexa renamed RB 42 with new cybersecurity focus", 3 avril 2023, https://www.intelligenceonline.com/surveillance--interception/2023/04/03/nexa-renamed-rb-42-with-new-cybersecurity-focus,109930650-art.

En 2022, Nexa Technologies a vendu ses actifs à l'entreprise française ChapsVision[13] ; en 2023, elle a changé de nom pour devenir RB 42 et a annoncé qu'elle avait cessé ses activités dans le secteur de la surveillance[14]. Boss Industries est toujours propriétaire de Trovicor, selon les documents publics disponibles[15].

Cytrox est une entreprise de Macédoine du Nord créée en 2017[16], qui est la première créatrice du logiciel espion Predator et a été rachetée par WiSpear en 2018[17].

Amesys, basée en France, était une entreprise de télécommunication et de défense, qui a créé un système de surveillance de masse baptisé Eagle, capable de surveiller le trafic Internet (IP) à l'échelle d'un pays tout entier[18]. Elle a cessé ses activités dans le secteur de la cybersurveillance en 2012, après avoir transféré ses actifs à Nexa Technologies, qui a rebaptisé Eagle « Cerebro ».

[13] Intelligence Online, "France: ChapsVision takes up strong position in interceptions thanks to Elektron takeover", 24 janvier 2022, https://www.intelligenceonline.com/surveillance--interception/2022/01/24/chapsvision-takes-up-strong-position-in-interceptions-thanks-to-elektron-takeover,109718567-art.
[14] Nexa Technologies, « Nexa Technologies. Une page se tourne », 2023, https://www.nexatech.fr/fr/about.
[15] Boss Industries, Comptes sociaux, 2021, p. 18.
[16] Dépositaire central de titres, "Известувања за корпоративни настани" (op. cit.), https://www.cdhv.mk/известувања_за_корпоративни_настани.aspx.
[17] Atooro, 25 mai 2020, http://web.archive.org/web/20200525234222/http://www.atooro.com/.
[18] Privacy International, "Amesys Brochure Eagle", février 2009, https://www.documentcloud.org/documents/409206-95-amesys-critical-system-architect.html.

1. 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.

2. MÉTHODOLOGIE

Ce rapport s'appuie sur les recherches techniques menées en continu par Amnesty International pour surveiller l'évolution et le déploiement des technologies de surveillance, notamment des logiciels espions ciblés visant les appareils mobiles, qui constituent une menace pour les défenseur·e·s des droits humains et la société civile à travers le monde[19]. Ce travail consiste notamment à identifier et à suivre l'évolution des produits de surveillance proposés par les entreprises de logiciels espions mercenaires, comme NSO Group, l'alliance Intellexa ou d'autres[20]. Le Security Lab d'Amnesty International surveille de près le logiciel espion Predator, vendu par l'alliance Intellexa, depuis 2021, ce qui lui a permis de trouver des victimes de Predator au sein de la société civile dans de nombreux pays. Ces recherches techniques ont conduit Amnesty International à identifier un compte X (ex-Twitter) public qui a transmis des liens d'infection de Predator en avril 2023. Cette étude de cas est détaillée dans le présent rapport.

Amnesty International a interrogé un journaliste d'origine vietnamienne, aujourd'hui installé en Allemagne, dont la plateforme médias a été prise pour cible dans le cadre de cette campagne d'attaques au logiciel espion en février 2023. Amnesty International a aussi analysé des registres de ventes et des données commerciales, et étudié une analyse d'autres registres commerciaux de l'alliance Intellexa obtenus par le réseau European Investigative Collaborations (EIC), qui donne des informations sur les ventes de solutions de surveillance et d'infection de l'alliance Intellexa. Par ailleurs, elle a 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.

En outre, dans le cadre de l'enquête sur Predator (dite enquête sur les « Predator Files »), le Security Lab d'Amnesty International a collaboré, en tant que partenaire technique, avec l'EIC, un réseau européen d'organisations du secteur des médias. Ce rapport contient les conclusions des recherches d'Amnesty International visant à analyser les spécifications techniques d'une suite de produits de surveillance proposés par l'alliance Intellexa, alliance d'entreprises du secteur des technologies de surveillance. Pour ce faire, Amnesty International a étudié les brochures commerciales et les documents techniques que s'était procurés l'EIC afin d'établir les capacités techniques et de déterminer les implications pour les droits humains de la suite de produits de surveillance conçus, mis en œuvre et commercialisés par l'alliance Intellexa entre 2007 et 2022.

Amnesty International a écrit au ministère vietnamien de la Sécurité publique le 19 septembre 2023 pour l'inviter à réagir aux conclusions de ce rapport, mais elle n'avait reçu aucune réponse à l'heure de la publication du document. Elle a aussi envoyé des courriers aux représentant·e·s du groupe Intellexa et du groupe Nexa le 20 septembre 2023, afin de leur demander leurs réactions à ses conclusions. Compte tenu de la structure évolutive et souvent délibérément opaque de beaucoup de ces sociétés (voir plus loin), il a été difficile de les contacter. Amnesty International s'est adressée aux entités les plus récentes d'après les informations publiquement disponibles figurant dans différents registres ou sur leurs sites Internet (voir le détail de la structure des entités dans le tableau 1). Elle leur a demandé des informations sur leurs pratiques

[19] Amnesty International, "Forensic Methodology Report: How to catch NSO Group's Pegasus", 18 juillet 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.
[20] Voir par exemple Amnesty International, « Piratage informatique. Amnesty International met en lumière une nouvelle campagne de piratage liée à une société mercenaire de cybersurveillance », 29 mars 2023, https://www.amnesty.org/fr/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/.

en matière de diligence requise dans le domaine des droits humains, ainsi que sur les mesures qu'elles avaient prises pour offrir réparation aux victimes de l'utilisation de leurs technologies identifiées dans de précédents rapports d'investigation. Elle n'avait reçu aucune réponse à l'heure de la publication du rapport. Le 26 septembre 2023, Amnesty International a aussi écrit à Delsons Hong Kong Limited à propos de ses conclusions concernant la vente de technologies de surveillance au Viêt-Nam, décrites ci-dessous au chapitre 4.5. Aucune réponse ne lui était parvenue au moment de la publication de ce rapport.

Si Amnesty International n'a pas reçu de réponse directe des groupes Intellexa et Nexa, d'anciens cadres et actionnaires principaux du groupe Nexa ont répondu au réseau EIC au nom de leurs entreprises, notamment Nexa Technologies et Advanced Middle East Systems. Leur réponse portait en partie sur leur implication dans les ventes au Viêt-Nam et a été intégrée au chapitre 4.5.

Amnesty International remercie vivement toutes les personnes qui ont participé à ces recherches, en particulier ses partenaires de l'EIC et Khoa Lê Trung. Le Security Lab d'Amnesty International tient aussi à remercier le laboratoire sur la sécurité numérique de Reporters sans frontières pour son aide dans la collecte d'informations scientifiques pendant cette enquête. Amnesty International adresse par ailleurs ses remerciements à Citizen Lab pour sa vérification indépendante de ses conclusions reliant les domaines d'attaque identifiés au logiciel espion Predator, ainsi que le groupe d'analyse des menaces de Google[21] pour lui avoir communiqué ses recherches sur l'infrastructure de surveillance de l'alliance Intellexa.

CONSEILS EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE

Le logiciel espion et les attaques numériques très élaborés dont il est question dans ce rapport sont utilisés contre des personnes qui intéressent tout particulièrement les opérateurs gouvernementaux de logiciels espions en raison de leur activité professionnelle, de leur action au sein de la société civile ou des informations qu'elles possèdent. Si vous pensez être une cible à risque, voici quelques mesures concrètes que vous pouvez prendre pour rendre plus difficiles ce type d'attaques numériques perfectionnées :

- Mettez à jour votre navigateur Internet et le logiciel système de votre téléphone mobile chaque fois que des mises à jour de sécurité sont disponibles pour vos appareils.
- Si vous utilisez un appareil Apple, activez le mode de haute sécurité « Isolement ». Il sera ainsi plus difficile pour un attaquant de réussir à infecter votre appareil.
- Méfiez-vous des liens provenant d'inconnus. Ne vous fiez pas uniquement à l'aperçu de l'URL qui s'affiche sur les applications de messagerie ou les plateformes de réseaux sociaux, il peut être trompeur.
- Faites attention à tout changement dans le fonctionnement de vos appareils (par exemple, une durée réduite de la batterie). Toutefois, ce seul élément n'est pas en soi un indicateur fort d'activité suspecte.
- Désactivez la fonction « Autoriser les demandes de message de tout le monde » sur X (ex-Twitter).
- Sur vos comptes Facebook personnels, gérez les paramètres de confidentialité afin de limiter la visibilité de votre profil à vos ami·e·s existants et évaluez toute demande de nouvel·le ami·e ou requête sur Messenger avant d'accepter.
- Si vous recevez une alerte vous avertissant que vous êtes la cible d'un attaquant soutenu par l'État, demandez l'aide de spécialistes afin de déterminer les risques éventuels pour vos comptes et appareils.

Si vous êtes un·e défenseur·e des droits humains, journaliste ou membre de la société civile et que vous pensez avoir été visé·e par cette campagne ou avez reçu des liens d'attaque similaires sur les réseaux sociaux, contactez-nous sur https://securitylab.amnesty.org/contact-us.

[21] Le groupe d'analyse des menaces de Google indique avoir été créé pour « contrer les attaques soutenues par les gouvernements ». Google, "Threat Analysis Group", https://blog.google/threat-analysis-group/ (consulté le 28 septembre 2023).

3. INTRODUCTION

Ces dix dernières années, des organisations de la société civile, des chercheurs et chercheuses et des journalistes ont montré, par une série de révélations régulières, que des gouvernements du monde entier prenaient illégalement pour cible des militant·e·s, des journalistes et des responsables 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, était à l'origine d'une crise de la surveillance numérique[22]. Cette crise a de graves effets préjudiciables sur les droits humains, la liberté des médias et les mouvements sociaux à travers le monde. En 2021, les révélations du projet Pegasus[23] (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[24] 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 et à demander l'obligation de rendre des comptes pour les victimes de surveillance illégale.

Toutefois, une nouvelle enquête coordonnée par le réseau d'investigation journalistique EIC a 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[25]. Les nouvelles révélations sur les Predator Files montrent que l'utilisation par les États de logiciels espions et d'outils de surveillance fabriqués par des entreprises privées reste hors de contrôle et constitue une menace pour les droits fondamentaux, tandis que les gouvernements et les vendeurs de technologies de surveillance continuent de les vendre, de les transférer et de les utiliser sans contrôle partout dans le monde[26].

Les révélations de l'enquête sur Predator montrent qu'une suite de technologies de surveillance hautement intrusives fournies par l'alliance Intellexa (qui est composée de différentes entreprises commercialisant des technologies de surveillance depuis des États membres de l'Union européenne [UE] ou d'autres pays) est vendue et transférée dans le monde entier en toute impunité. L'enquête révèle le caractère mondial et l'ampleur des ventes de technologies de surveillance réalisées par cette 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[27]. Compte tenu de précédents cas de surveillance illégale dans ces pays et/ou de

---

[22] Amnesty International, *La partie immergée de l'iceberg. La responsabilité des États et du secteur privé dans la crise de la surveillance numérique* (index : DOC 10/4491/2021), 23 juillet 2021, https://www.amnesty.org/fr/documents/doc10/4491/2021/fr ; Amnesty International, *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology* (index : DOC 10/4516/2021), 27 juillet 2021, https://www.amnesty.org/en/documents/doc10/4516/2021/en/.

[23] Le projet Pegasus a été un projet collaboratif unique en son genre auquel ont participé plus de 80 journalistes travaillant pour 17 médias dans 10 pays, coordonné par Forbidden Stories, média à but non lucratif basé à Paris, avec l'aide technique d'Amnesty International.

[24] Voir, par exemple : Access Now, "Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict", 25 mai 2023, https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict/ ; Citizen Lab, "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware", 12 janvier 2022, https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

[25] Le rapport complet de l'EIC sur les Predator Files (en anglais) est publié en même temps que le présent rapport. Voir le site de l'EIC à la rubrique "Projects" : https://eic.network/#projects.

[26] EIC, "Projects", https://eic.network/#projects.

[27] EIC, "Projects", https://eic.network/#projects.

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 donnent lieu à des atteintes aux droits humains.

Dans le cadre des recherches menées pour ce rapport, le Security Lab d'Amnesty International a aussi découvert une attaque jusqu'à présent non révélée menée au moyen du logiciel espion Predator, visant des cibles en lien avec les intérêts du gouvernement vietnamien. Cette campagne de surveillance a visé au moins 50 comptes de réseaux sociaux appartenant à 27 particuliers et 23 institutions à travers le monde au moyen de liens d'infection « un clic » reliés à l'infrastructure d'attaque du logiciel espion Predator, de l'alliance Intellexa. Parmi les cibles figuraient des personnalités politiques du Parlement européen, des membres de la Commission européenne, et des journalistes, des chercheurs et chercheuses universitaires et des groupes de réflexion basés dans l'UE. Cette tentative d'attaque a aussi visé des responsables des Nations unies, la présidente de Taiwan, des sénateurs et représentants des États-Unis et d'autres autorités diplomatiques. Les attaques les plus récentes remontent seulement à juin 2023. Amnesty International a aussi analysé des registres de ventes et des données commerciales et s'appuie, pour ce rapport, sur des recherches de ses partenaires de l'EIC concernant les ventes de solutions de surveillance et d'infection de l'alliance Intellexa. Ces recherches montrent que les outils en question ont été vendus, *via* différente sociétés vietnamiennes de courtage, à un utilisateur final gouvernemental, le ministère vietnamien de la Sécurité publique. Amnesty International n'a pas scientifiquement identifié d'infections réussies résultant de cette campagne, mais les capacités connues du logiciel espion Predator, associées à l'audace et, dans certains cas, à l'imprudence de cette opération de surveillance, montrent l'ampleur des risques posés par la prolifération et les transferts non contrôlés de tels outils.

L'analyse par Amnesty International d'une infrastructure technique récente liée au système de logiciel espion Predator 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. Cette analyse s'appuie sur des recherches menées en 2021 par Citizen Lab et Meta, qui ont recueilli des informations sur de possibles clients actifs de Predator en Allemagne, en Arabie saoudite, en Arménie, en Colombie, en Côte d'Ivoire, en Égypte, en Grèce, en Indonésie, à Madagascar, à Oman, aux Philippines, en Serbie, à Trinité-et-Tobago et au Viêt-Nam[28].

En analysant les documents commerciaux que s'était procurés l'EIC, Amnesty International a pu établir les capacités techniques de la suite de produits de surveillance conçus, mis en œuvre et commercialisés, entre 2007 et 2022, par les entreprises constituant ce qui est devenu l'alliance Intellexa[29]. Cette suite comprend 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 ». Le logiciel espion Predator a été développé à l'origine par l'entreprise de surveillance nord-macédonienne Cytrox, qui fait partie du groupe Intellexa (voir Tableau 1, Descriptif des entreprises).

Les révélations de l'enquête sur les Predator Files montrent aussi les différents « vecteurs » ou techniques proposés par l'alliance Intellexa pour installer le logiciel espion *via* des « attaques tactiques », qui permettent de prendre pour cible des appareils situés à proximité, au moyen de diverses méthodes d'injection réseau et d'attaques contre les processeurs de bande de base des téléphones mobiles. L'alliance Intellexa 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 de 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 à grande échelle 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[30]. Ces deux types de technologies (les

[28] Meta, *Threat Report on the Surveillance-for-Hire Industry*, 16 décembre 2021, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf ; Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", 16 décembre 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[29] Security Lab d'Amnesty International, "Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products", 6 octobre 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

[30] Wiki Leaks, document de description des produits d'Amesys pour la Conférence ISS World Europe 2008 à Prague, https://wikileaks.org/spyfiles/files/0/21_200810-ISS-PRG-AMESYS.pdf (consulté le 26 septembre 2023).

logiciels espions hautement intrusifs et les outils de surveillance de masse non ciblée) sont fondamentalement incompatibles avec les droits humains.

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 massivement prise pour cible sans aucun contrôle et en toute impunité. 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 aux droits humains dans le monde entier, puisque les entreprises sont toujours autorisées à commercialiser librement leurs produits dans le plus grand secret. Ces nouvelles preuves de ciblage illicite 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[31]. Les atteintes aux droits humains sont une caractéristique de ce secteur, pas le résultat d'un dysfonctionnement[32].

La société civile alerte depuis longtemps sur le fait qu'une véritable culture de l'impunité spécifique à la surveillance numérique ciblée s'est développée et qu'il est urgent d'y répondre. Les révélations régulières de la société civile auraient dû déclencher une action plus efficace des gouvernements à l'échelle nationale, régionale et multilatérale. Certes, quelques mesures allant dans le bon sens ont bien été prises, mais la dénonciation de ce secteur clandestin et de cet ensemble de pratiques étatiques échappant à tout contrôle reste à l'initiative de la société civile, des journalistes et des chercheurs et chercheuses, au moyen d'informations durement acquises[33].

Amnesty International a déjà alerté par le passé sur le fait que les révélations de la société civile ne devaient pas être la seule forme de contrôle exercée sur les États et les entreprises du secteur de la surveillance[34]. La poursuite du commerce des technologies de surveillance et de ses abus dénoncés dans ces dernières révélations doit davantage pousser les États à agir de façon urgente et concertée. Ils doivent faire preuve d'initiative pour mettre un terme aux atteintes aux droits humains découlant de l'utilisation illégale de technologies de surveillance ciblée et veiller à ce que de véritables voies existent pour rendre des comptes aux victimes de ces atteintes.

---

[31] Amnesty International, *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology* (op. cit), https://www.amnesty.org/en/documents/doc10/4516/2021/en.

[32] Amnesty International, *Operating in the shadows: Investor risk from the private surveillance industry* (index : DOC 10/4359/2021), 21 octobre 2021, https://www.amnesty.org/en/documents/doc10/4359/2021/en/.

[33] Amnesty International, *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology* (op. cit), https://www.amnesty.org/en/documents/doc10/4516/2021/en.

[34] Amnesty International, *La partie immergée de l'iceberg. La responsabilité des États et du secteur privé dans la crise de la surveillance numérique* (op. cit.), https://www.amnesty.org/fr/documents/doc10/4491/2021/fr.

4. L'ALLIANCE INTELLEXA ET SON LOGICIEL ESPION PREDATOR

Ce chapitre présente un résumé des antécédents de l'alliance Intellexa en matière de vente de technologies de surveillance à travers le monde. De nombreuses enquêtes journalistiques ont déjà fait la lumière sur des cas d'utilisation abusive des outils d'Intellexa pour cibler illégalement des personnes ou des organisations. Pourtant, nos travaux mettent une nouvelle fois en évidence les carences des garanties censées empêcher ce type de violations, y compris dans l'UE. S'appuyant sur des brochures et des documents techniques obtenus par l'EIC, le présent chapitre décrit comment Predator, le logiciel espion d'Intellexa, peut être utilisé pour infecter des appareils, et montre pourquoi cette technologie porte intrinsèquement atteinte aux droits humains.

La plus grande partie du chapitre est consacrée à un cas mis au jour par le Security Lab d'Amnesty International, dans lequel Predator a été utilisé pour attaquer diverses cibles. Cette étude de cas montre comment une entité utilisant les logiciels espions d'Intellexa peut cibler des comptes personnels et institutionnels et tenter d'infecter les appareils correspondants, en s'appuyant sur l'exemple d'une récente campagne d'attaques visant un journaliste vietnamien, des membres de la société civile, ainsi que des responsables de l'UE et plusieurs personnalités politiques, notamment américaines, travaillant sur des questions intéressant le gouvernement du Viêt-Nam. Le Security Lab d'Amnesty International n'a confirmé aucun cas d'infection réussie en lien avec cette étude de cas. Néanmoins, ces travaux mettent en évidence la possibilité pour un opérateur de prendre pour cible des personnes et des organisations dans le monde entier à l'aide d'un logiciel espion hautement intrusif. Enfin, la dernière section porte sur l'évaluation des responsabilités quant à l'utilisation du logiciel espion Predator telle que décrite dans ce chapitre.

4.1 UN LOURD PASSÉ DE SURVEILLANCE ABUSIVE

Le groupe Intellexa se vante d'être « une entreprise basée dans l'UE et soumise à la réglementation européenne[35] ». Selon les documents financiers annuels de la société mère d'Intellexa, Thalestris Ltd., l'activité principale de l'alliance est de « fournir des produits de renseignement aux institutions chargées de l'application des lois[36] ». L'alliance Intellexa 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)[37]. Les groupes Nexa et Intellexa contrôlent de nombreuses entités

[35] Intellexa, https://web.archive.org/web/20230719063910/https://intellexa.com/ (consulté le 19 juillet 2023)
[36] Thalestris Limited, *Annual report and consolidated financial statements for December 2021*, p. 29, (consulté en août 2023)
[37] Nexa Technologies, "Intellexa Alliance: Intellexa, The Intelligence Alliance, to Provide Unmatched End-To-End Intelligence Solutions for Law Enforcement and Intelligence Agencies", 16 février 2019,

commerciales, dont certaines ont été rebaptisées. Celles-ci sont basées dans différents pays dans et en dehors de l'UE, notamment en Allemagne, à Chypre, aux Émirats arabes unis, en France, en Grèce, en Hongrie, en Irlande, en Israël, en Macédoine du Nord, en République tchèque et en Suisse[38].

Les entités et les pays sus-cités ne rendent pas compte de façon exhaustive de la présence de l'alliance Intellexa. La nature exacte des liens entre ces entreprises est entourée de secrets, les entités commerciales et les structures qui les relient étant en constante mutation et évolution, et changeant régulièrement de nom ou de marque. De la même manière qu'avec d'autres fournisseurs de logiciels espions, tels que la société NSO Group, à la sombre réputation, ces structures commerciales opaques et infiniment 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 ainsi qu'aux mécanismes d'obligation de diligence[39]. Dans le cas de l'alliance Intellexa, le montage 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. Tout cela contribue à créer un tableau global particulièrement alambiqué et opaque, ce qui complique encore davantage les processus relatifs à l'obligation de rendre des comptes et à la transparence en cas d'usages illégaux des outils de surveillance de l'alliance.

Ces révélations sont loin d'être les premières pointant l'existence d'un lien entre des entreprises appartenant à l'alliance Intellexa et des atteintes aux droits humains dans le monde. En 2011, la Fédération internationale des ligues des droits de l'Homme (FIDH) et la Ligue des droits de l'Homme (LDH) ont déposé une plainte au pénal contre Amesys pour complicité d'actes de torture commis à travers la vente d'une technologie de surveillance à la Lybie en 2007[40].

En 2017, les deux organisations ont déposé une seconde plainte, à l'encontre de Nexa Technologies qui a vendu le même système de surveillance à l'Égypte en 2014, pour complicité de tortures et disparitions forcées, à la suite de laquelle la justice française a ouvert une nouvelle information judiciaire[41]. Nexa Technologies et plusieurs dirigeants de l'entreprise ont été mis en examen en 2021 dans le cadre de cette information judiciaire, mais la cour d'appel de Paris a annulé ces mises en examen l'année suivante[42].Nexa est une entreprise faisant partie de l'alliance Intellexa.

En 2021, Citizen Lab a découvert qu'un homme politique exilé et un journaliste, tous deux Égyptiens, avaient été victimes d'une infection au logiciel espion Predator[43]. En 2022, une série d'enquêtes et de révélations ont mis au jour que Thanasis Koukakis, un journaliste grec, et Nikos Androulakis, dirigeant d'un parti d'opposition grec et eurodéputé, avaient été pris pour cible au moyen de Predator et mis sur écoute par le Service national de renseignement grec[44]. Un journal a par ailleurs publié une liste de personnalités de

---

https://web.archive.org/web/20200109072024/https://www.nexatech.fr/intellexa-alliance-press-news ; Fast Company, "Inside the shadowy world of spyware makers that target activists and dissidents", 26 juin 2019, https://www.fastcompany.com/90369108/inside-the-shadowy-world-of-spyware-makers-that-target-activists-and-dissidents

[38] Département d'État des États-Unis, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities", 18 juillet 2023, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/ ; Parlement européen, *Enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (recommandation)*, 15 juin 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_FR.pdf ; Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (op. cit.), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/ ; https://www.business-humanrights.org/de/unternehmen/nexa-technologies/CRFS, Nexa Technologies https://www.crfs.com/partner/nexa-technologies/ (consulté le 26 septembre 2023) ; Intelligence Online, "France's Nexa acquires European interception specialist Trovicor", 3 décembre 2019, https://www.intelligenceonline.com/surveillance--interception/2019/12/03/france-s-nexa-acquires-european-interception-specialist-trovicor,108384645-art

[39] Amnesty International, *Operating from the Shadows: Inside NSO Group's Corporate Structure* (index AI : DOC 10/4182/2021), 31 mai 2021, https://www.amnesty.org/fr/documents/doc10/4182/2021/en/

[40] Fédération internationale des ligues des droits de l'Homme, « La FIDH et la LDH déposent une plainte mettant en cause la société Amesys pour complicité d'actes de torture », 19 octobre 2011, https://www.fidh.org/fr/regions/maghreb-moyen-orient/libye/La-FIDH-et-la-LDH-deposent-une

[41] Fédération internationale des ligues des droits de l'Homme, « Q/A - Surveillance et torture en Égypte et en Libye – des dirigeants d'Amesys et Nexa Technologies mis en examen », 22 juin 2021, https://www.fidh.org/fr/regions/maghreb-moyen-orient/egypte/q-a-surveillance-et-torture-en-egypte-et-en-libye-des-dirigeants-d

[42] Tech Xplore, "Charges dropped against French company over Egypt spyware", 14 décembre 2022, https://techxplore.com/news/2022-12-french-company-egypt-spyware.html

[43] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (op. cit.), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[44] Inside Story, "Από τον Κουκάκη στον Ανδρουλάκη: Νέα τροπή στην υπόθεση του spyware Predator", 27 juillet 2022, https://insidestory.gr/article/apo-koykaki-androylaki-nea-tropi-ypothesi-predator ; Parlement européen, *Rapport relatif à l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents,* 2022/2077(INI), 22 mai 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_FR.pdf ; Amnesty International, « Grèce. Le scandale de la

premier plan qui auraient été placées sous surveillance par l'État et/ou visées par Predator[45]. En 2023, il a été révélé qu'une cadre de nationalité gréco-américaine travaillant chez Meta avait été ciblée à l'aide de Predator et qu'elle aurait été mise sur écoute par le Service national de renseignement grec[46]. Dans le cadre d'une enquête menée par l'autorité grecque chargée de la protection de la vie privée (Hellenic Data Protection Authority) sur l'utilisation de Predator, 350 SMS visant à installer des logiciels de surveillance ont été découverts, et 92 « cibles » ont pu être identifiées[47].

En septembre 2023, Citizen Lab a révélé qu'un ancien député égyptien avait été entretemps visé par le logiciel espion Predator[48].

En juillet 2023, le Bureau de l'industrie et de la sécurité du gouvernement des États-Unis a placé quatre entreprises de l'alliance Intellexa sur sa liste des entités s'adonnant à des cyberactivités malveillantes, indiquant qu'elles « se livraient à du trafic de failles cyber permettant d'accéder à des systèmes d'information, ce qui représente une menace pour la vie privée et la sécurité des individus et des organisations dans le monde entier[49] ». Les entreprises ajoutées à cette liste sont les suivantes : Intellexa S.A. en Grèce, Intellexa Limited en Irlande, Cytrox AD en Macédoine du Nord, et Cytrox Holdings Crt en Hongrie.

Étant donné que des entreprises du groupe Nexa et des sociétés au sein même du groupe Intellexa ont déjà été soupçonnées d'avoir commis des atteintes aux droits humains en Grèce, en Égypte et en Libye, Amnesty International a écrit aux entités concernées pour leur demander quelles mesures elles avaient prises, depuis la publication de ces premières révélations, pour garantir un exercice de leurs activités respectueux des droits et des Principes directeurs des Nations unies, et pour apporter réparation aux personnes lésées. Aucune réponse n'était parvenue à l'organisation au moment de la publication de ce rapport. Cependant, d'anciens cadres de Nexa ont répondu à l'EIC au nom des entreprises du groupe, qui comprennent notamment Nexa Technologies et Advanced Middle East Systems. Voici les éléments de réponse avancés :

> « À aucun moment nous avons sous-estimé le dilemme éthique posé par notre activité. Nous avions conscience que certains des pays avec lesquels nous avons pu engager des relations commerciales étaient loin d'être parfaits sur le plan de l'état de droit. Mais nous étions tout aussi sensibles au fait que notre démarche s'inscrivait le plus souvent dans un élan de la communauté internationale d'accompagner ces pays vers la démocratie.
>
> « En exposant les dilemmes moraux et très concrets auxquels nous avons dû faire face au cours de notre vie professionnelle, nous venons d'évoquer la place des autorités et notamment des autorités françaises, lorsqu'il s'agit de l'exportation d'une solution française. Dans plusieurs des pays litigieux que vous citez, nous avons non seulement obtenu une autorisation d'export mais aussi n'avons fait qu'emprunter la voie d'une coopération étroite engagée par la France avec ces mêmes pays. »

Les anciens cadres ajoutent :

> « […] les sociétés françaises doivent être en mesure d'opérer dans un cadre réglementaire clair.
>
> « Nous faisions confiance aux autorités pour nous donner le feu vert. Depuis, à compter de 2021, nous essayons d'avancer avec des conseils externes de manière à mieux comprendre la réalité du terrain dans différents pays et de pouvoir évaluer les risques d'atteintes aux droits fondamentaux.

---

surveillance doit tous nous sortir de notre complaisance », 26 janvier 2023, https://www.amnesty.org/fr/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/

[45] Documento, "Αποκάλυψη: Αυτούς παρακολουθούσε – Αυτή την Κυριακή στο Documento", 5 novembre 2022, https://www.documentonews.gr/article/apokalypsi-aytoys-parakoloythoyse-ayti-tin-kyriaki-sto-documento/ ; Economist, "Fresh allegations in a Greek phone-hacking scandal", 10 novembre 2022, https://www.economist.com/europe/2022/11/10/fresh-allegations-in-a-greek-phone-hacking-scandal

[46] New York Times, "Meta Manager Was Hacked With Spyware and Wiretapped in Greece", 20 mars 2023, https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html ; Parlement européen, *Rapport relatif à l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents* (op. cit.), https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_FR.pdf

[47] Euractiv, "Privacy watchdog finds 92 'targets' in Greek wiretapping scandal", 21 juillet 2023, https://www.euractiv.com/section/politics/news/privacy-watchdog-finds-92-targets-in-greek-wiretapping-scandal/

[48] Citizen Lab, "Predator in the Wires: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions", 22 septembre 2023, https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

[49] Département d'État des États-Unis, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities" (op. cit.), https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/

> Nous avons ainsi instauré un process faisant appel à des personnes externes à la société et spécialisées dans les droits de l'Homme.
>
> « À la suite de leur avis, nous avons pris la décision de cesser toute relation commerciale avec un État. Au cours des deux dernières années, nous avons également refusé d'entrer en relation commerciale avec plusieurs autres États. »

Au sujet de la conformité avec les réglementations en matière de contrôle des exportations, ils déclarent :

> « Ainsi que nous l'avons exposé plus haut, tous les contrats de commercialisation par les sociétés que vous citez respectaient scrupuleusement les réglementations d'export.
>
> « Ainsi que nous l'avons expliqué en introduction, lorsque nous obtenions une autorisation du SBDU [Service des biens à double usage], nous considérions de bonne foi que notre produit pouvait s'exporter en toute régularité. Cela était d'autant plus vrai pour un pays comme l'Égypte avec lequel les autorités françaises exaltaient une coopération intense et sur le territoire duquel se jouait également notre propre sécurité [la sécurité de la France]. C'est précisément l'une des raisons pour lesquelles la Cour d'appel de Paris a annulé nos mises en examen en décembre 2022, ainsi que cela a été relaté dans la presse.
>
> « Contrairement à ce que vous pensez, l'implantation de nos sociétés n'a jamais eu pour but de contourner la législation. Elle répondait à une logique commerciale car nos clients exigeaient souvent une présence locale. »

Enfin, dans leur réponse à l'EIC à propos des ventes de Predator, ils expliquent :

> « […] nous avons dénoncé ces contrats [y compris celui avec le Viêt-Nam] après la perquisition de 2021, qui nous ont fait prendre conscience des risques portés par ces marchés. Nous avons réalisé que les autorisations accordées ne nous protégeaient pas suffisamment et ne constituaient aucunement une garantie contre les violations des droits de l'Homme. »

Au vu de la nature du marché des logiciels espions et de sa capacité à faciliter les atteintes aux droits humains, et compte tenu du fait que l'alliance Intellexa savait elle-même qu'il existait des précédents de telles violations, les entreprises de surveillance au sein de cette alliance avaient connaissance, ou auraient raisonnablement dû avoir connaissance, que des atteintes aux droits humains pouvaient être commises. En outre, les antécédents de violation des droits humains décrits plus haut constituaient pour les autorités chargées du contrôle des exportations et d'autres instances de l'État un avertissement suffisamment clair que la vente des produits de l'alliance Intellexa était susceptible de présenter de graves risques pour les droits humains.

4.2 PREDATOR, LE LOGICIEL ESPION D'INTELLEXA

Le système Predator développé par Intellexa est un logiciel espion hautement intrusif qui bénéficie par défaut d'un accès total à toutes les données stockées dans l'appareil infecté ou transmises par celui-ci, et qui est conçu pour n'y laisser aucune trace, afin d'empêcher toute forme de vérification indépendante d'un usage potentiellement abusif. Predator est donc par essence incompatible avec les droits humains et doit être interdit.

Le Security Lab d'Amnesty International a analysé des brochures et des documents techniques transmis par l'EIC, apportant de nouveaux éclairages sur le fonctionnement technique de ce logiciel espion et ses méthodes d'infection des appareils visés.

D'après ces documents, l'utilisation de Predator est gérée au moyen d'un système basé sur le Web, qu'Intellexa appelle « Cyber Operation Platform ». L'interface de Predator permet à l'opérateur du logiciel espion de lancer des attaques pour infecter un appareil cible. En cas de réussite, il devient possible d'accéder à des informations sensibles sur l'appareil infecté (photos, données de géolocalisation, messages, enregistrements, etc.) et de les récupérer.

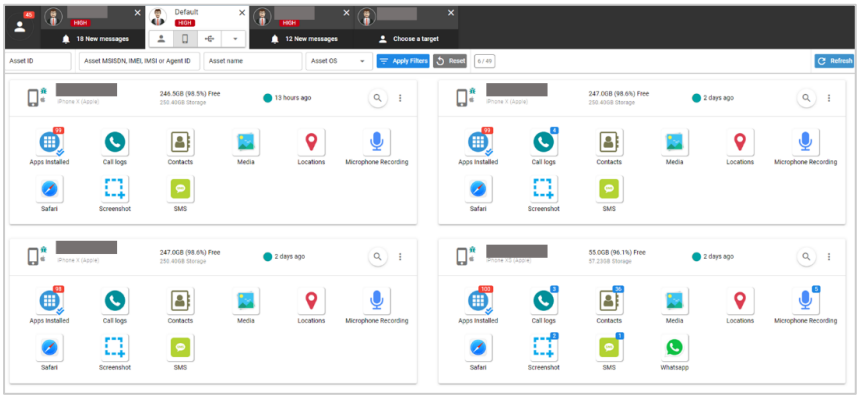


Figure 1 : Interface de Predator, le logiciel espion d'Intellexa (source : documents fournis par l'EIC)

Predator repose sur un système complet constitué de différents composants logiciels et d'infrastructure, comprenant l'implant du logiciel espion en tant que tel, qui s'installe sur l'appareil ciblé, ainsi que les exploits logiciels et les vecteurs d'attaques nécessaires à l'installation furtive du logiciel espion. Intellexa désigne ses produits de surveillance mobile par différents noms de marque, tels que Green Arrow pour son implant de logiciel espion Android et Red Arrow pour l'implant iOS, mais aussi Predator, Helios ou encore NOVA. Dans le présent rapport, tous ces produits de surveillance mobile sont regroupés sous le nom de Predator, car nous considérons que ces noms de produits renvoient tous à un même ensemble de technologies de cyberespionnage plus ou moins liées, qui ont été initialement conçues par Cytrox, et que l'alliance Intellexa continue de développer, de promouvoir et de commercialiser.

Le code d'exploit et les charges du logiciel espion sont acheminés jusqu'à un appareil cible à partir de ce qu'Intellexa appelle un « serveur d'installation ». Une fois que le téléphone est infecté par l'implant Predator, il se connecte à un réseau de commandement et de contrôle (CNC), grâce auquel les opérateurs peuvent envoyer des commandes à l'implant et lui ordonner de récupérer des fichiers ou d'activer le micro, par exemple. Ces commandes sont envoyées à l'appareil *via* un réseau d'anonymisation, dont l'objectif est de masquer la position et l'identité de l'opérateur, et de compliquer la tâche des personnes cherchant à identifier la source et la nature des attaques. Le serveur d'installation et les serveurs CNC doivent être accessibles publiquement sur Internet afin que les appareils ciblés puissent s'y connecter. D'autres serveurs, notamment le réseau d'anonymisation et le « Cyber Operations Core », peuvent être protégés par un pare-feu ou isolés au sein du réseau du client utilisant Predator.

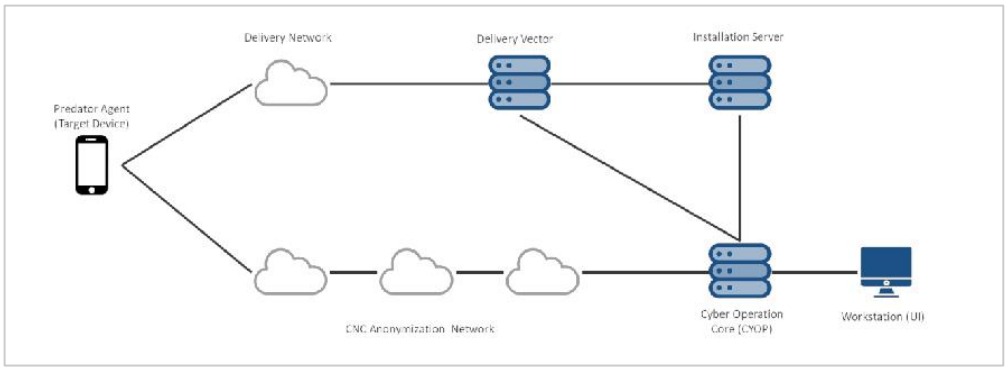


Figure 2 : Architecture de haut niveau des serveurs de Predator (source : documents fournis par l'EIC)

Un appareil peut être ciblé et infecté par différents vecteurs d'infection dits « un clic » ou « zéro clic ». Les attaques publiquement documentées associées à Predator s'appuient sur une technique d'ingénierie sociale consistant à envoyer des messages contenant une adresse URL malveillante. Ce mode opératoire est qualifié d'attaque « un clic »[50]. La réussite de ce type d'attaque repose sur la capacité de l'opérateur du logiciel

[50] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (op. cit.), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/ ; Inside Story, "Predatorgate: Τι έγραφαν τα SMS-παγίδα που έλαβαν επιχειρηματίες, υπουργοί και δημοσιογράφοι", 27 juillet 2023, https://insidestory.gr/article/predatorgate-ti-egrafan-ta-sms-pagida-poy-elavan-epiheirimaties-ypoyrgoi-kai-dimosiografoi

espion à instaurer une relation de confiance avec la personne visée, puis à lui envoyer une URL malveillante en l'intégrant à un message personnalisé de telle sorte à l'inciter à cliquer sur le lien. Le présent rapport traite principalement d'attaques « un clic », car il s'agit du type d'attaque employé dans la campagne d'infection décrite dans le point suivant[51].

Si l'appareil ciblé exécute un navigateur et une version du système d'exploitation qui sont exploitables, le cyberattaquant peut alors utiliser une chaîne de failles pour compromettre le navigateur dans un premier temps, puis obtenir des privilèges d'accès lui permettant d'installer l'implant du logiciel espion sur l'appareil. Ces attaques de type « un clic » sont particulièrement efficaces puisqu'elles permettent d'infecter un appareil vulnérable n'importe où dans le monde par une simple ouverture de lien.

4.3 ÉTUDE DE CAS D'UTILISATION DE PREDATOR : @JOSEPH_GORDON16

En avril 2023, le Security Lab d'Amnesty International a découvert qu'un compte Twitter (désormais X) au nom d'utilisateur « @Joseph_Gordon16 » partageait publiquement des liens contenant des URL malveillantes associées au système Predator d'Intellexa. Le compte a pu être repéré grâce à la recherche en ligne de domaines actifs liés à Intellexa, que le Security Lab avait identifiés en enquêtant sur l'infrastructure des logiciels espions de l'alliance.

Dans les deux mois qui ont suivi l'identification du compte du cyberattaquant, le Security Lab d'Amnesty International a observé des dizaines de cas dans lesquels @Joseph_Gordon16 a envoyé des tweets publics et des réponses à des tweets d'autres utilisateurs contenant des liens malveillants, qui renvoyaient à des URL personnalisées raccourcies et à des URL imitant les adresses d'authentiques sites d'information. Amnesty International a pu établir une correspondance entre ces liens et les domaines d'Intellexa associés à Predator précédemment identifiés. Plus précisément, le Security Lab avait déjà pu déterminer, dans le cadre de ses recherches, que les deux domaines Inktonews[.]co et witteridea[.]co, qui figuraient dans les tweets publiés par le compte @Joseph_Gordon16, étaient des domaines actifs utilisés pour diffuser des URL raccourcies associées à Predator. Les domaines servant à lancer des attaques « un clic » et à générer des URL raccourcies renvoyant à des logiciels espions portent souvent des noms trompeurs qui laissent entendre à la victime que le lien est authentique. Ainsi, le domaine Inktonews[.]co semble indiquer que le lien renvoie à un article, tandis que le deuxième domaine, witteridea[.]co, vise à imiter un lien associé à la plateforme Twitter/X.

[51] Ces URL sont en outre généralement assorties de restrictions temporelles et géographiques pour compliquer le travail des personnes cherchant à analyser en détail les liens malveillants ou à recueillir des éléments extrêmement précieux sur les failles non corrigées ayant permis d'infecter des appareils bénéficiant des toutes dernières mises à jour

Figure 3 : Capture d'écran du compte @Joseph_Gordon16

Après la découverte par Amnesty International des premiers tweets malveillants, le compte @Joseph_Gordon16 a continué de tweeter des liens suspects pointant vers des domaines fraîchement enregistrés, tels que asean-news[.]net, southchinapost[.]net et caavn[.]org. Les domaines asean-news[.]net et southchinapost[.]net présentaient tous deux des caractéristiques similaires à celles de serveurs Predator déjà connus.

Amnesty International a montré une partie de ces activités à d'autres chercheurs et chercheuses en sécurité, notamment des analystes du Groupe d'analyse des menaces de Google, qui a déjà enquêté sur des attaques et des campagnes d'exploitation de failles menées par l'alliance Intellexa et d'autres fournisseurs de produits de surveillance[52]. Ce groupe a indiqué à Amnesty International que Google avait déterminé de son côté que les domaines et les URL partagés par le compte @Joseph_Gordon16, notamment southchinapost[.]net, Inktonews[.]co et witteridea[.]co, faisaient partie du système de logiciel espion Predator d'Intellexa.

En outre, des chercheurs et chercheuses du Groupe d'analyse des menaces de Google sont également parvenus à accéder aux URL malveillantes associées à Predator figurant dans les tweets de @Joseph_Gordon16, alors que le compte était toujours actif. Reposant sur le domaine southchinapost[.]net, l'URL malveillante initiale, qui apparaissait sous une forme raccourcie, effectuait une redirection vers scanningandinfo[.]online, un serveur d'installation de Predator. Dans ce cas, le serveur d'installation n'a pas tenté d'exploiter une faille ou d'infecter l'appareil de test.

FONCTION	URL
Page cible de l'URL raccourcie	https://southchinapost[.]net/eNISDKnI
Serveur d'installation de Predator	https://scanningandinfo[.]online/jbz7xv9xox0bn2ya3gat39i64/xfer-ovc?sip=2d2c3a697858f315177940709c236a69
Serveur d'installation de Predator	https://scanningandinfo[.]online/jbz7xv9xox0bn2ya3gat39i64/xfer-ovc?r=true&sip=2d2c3a697858f315177940709c236a69

Tableau 2 : Exemple de chaîne de redirection d'un lien associé à Predator partagé par @Joseph_Gordon16

Le troisième domaine (caavn[.]org) utilisé par le compte X @Joseph_Gordon16 n'étant plus en ligne au moment de notre analyse, nous n'avons pas pu déterminer s'il correspondait à l'empreinte des serveurs d'Intellexa. Le domaine caavn[.]org était hébergé à l'adresse IP 212.90.121.247, qui hébergeait également deux autres domaines aux noms semblables à ceux d'authentiques sites Internet vietnamiens :

[52] Groupe d'analyse des menaces de Google, "Protecting Android users from 0-Day attacks", 19 mai 2022, https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/

xuatnhapcanhvn[.]info et tokhaiytehanoi[.]org[53]. Le fait que plusieurs noms de domaine en lien avec le Viêt-Nam aient été hébergés sur le même serveur Internet, à la même période, et enregistrés par le biais du même bureau d'enregistrement laisse supposer que ces trois domaines ont été enregistrés par le même opérateur.

Figure 4 : Utilisation du domaine caavn[.]org par le cyberattaquant pour imiter un article du South China Morning Post

Contrairement aux cas décrits plus hauts impliquant le partage d'URL raccourcies, le tweet s'appuyant sur le domaine caavn[.]org contenait une URL complète qui semblait renvoyer à un véritable article publié par le journal *South China Morning Post*. Cette méthode consistant à imiter un article ou une page Web authentiques fait partie des techniques d'attaque employées par les cyberattaquants pour inciter une cible à cliquer sur un lien. L'aperçu du lien qui s'affiche sur X indique le véritable nom de domaine du journal *South China Morning Post* (scmp.com), ce qui suggère que les cyberattaquants ont configuré le lien malveillant de manière à ce qu'une fausse redirection vers le site du *South China Morning Post* trompe le générateur d'aperçu de X afin que celui-ci affiche le vrai nom de domaine du journal (voir figure 4).

Le fait que certains des domaines d'Intellexa sur lesquels s'appuient les attaques aient été conçus pour imiter d'authentiques sites Web vietnamiens laisse à penser que des acteurs associés au Viêt-Nam sont impliqués. Cette hypothèse est corroborée par de nombreux éléments de preuve indirects, tirés d'une analyse du compte X du cyberattaquant et des antécédents des personnes visées. Le premier tweet du compte a été publié en 2020 en langue vietnamienne. Le compte a par la suite envoyé d'autres tweets contenant un nom de domaine malveillant, prenant pour cible Thời Báo, un site d'information vietnamien basé en Allemagne. Le cas de Thời Báo est traité plus en détail dans le point 4.4.1 ci-après.

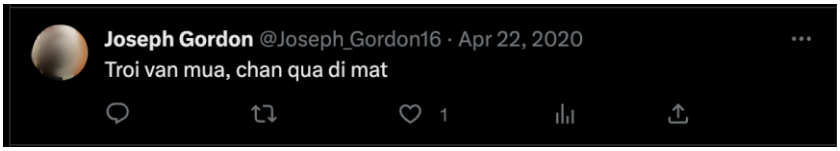


Figure 5 : L'un des premiers tweets de @Joseph_Gordon16, écrit en vietnamien

4.4 LES CIBLES DE @JOSEPH_GORDON16

Les tentatives d'infection commises par le compte X @Joseph_Gordon16, qui étaient publiques et visaient un large éventail de cibles, ont permis au Security Lab d'Amnesty International de se faire une idée des objectifs de l'opérateur à l'origine de cette campagne d'attaques menée à l'aide du logiciel espion d'Intellexa Predator. Parmi les personnes prises pour cible par ce compte figuraient des journalistes, des chercheurs et

[53] Ces deux noms de domaine ressemblent respectivement à l'adresse officielle du département de l'immigration du ministère vietnamien de la Police (xuatnhapcanh.gov.vn) et à celle d'un site Web vietnamien ayant servi au dépôt de déclarations de santé pendant la pandémie de COVID-19 (tokhaiyte.vn).

chercheuses universitaires travaillant sur des questions de sécurité dans la mer de Chine méridionale et le Viêt-Nam, ainsi que de hauts responsables politiques de l'UE, des États-Unis et d'ailleurs impliqués dans des activités en lien avec la réglementation internationale de la pêche, un sujet intéressant les autorités vietnamiennes (voir point 4.4.2).

La présente section s'attarde sur certaines des principales tentatives d'infection effectuées à l'encontre de journalistes, de membres de la société civile et de personnalités publiques. Si les cibles sont variées, tant par leur profil que par leur position géographique, elles ont bien souvent un lien avec des intérêts vietnamiens en matière politique, militaire et de renseignement.

La liste complète des tweets figure à l'Annexe II du présent rapport.

CATÉGORIE	NOMBRE DE TENTATIVES D'INFECTION AU LOGICIEL ESPION
Médias d'information	16
Universitaires	2
Personnalités politiques/institutions	27
Groupes de réflexion	6
Autre	7

Tableau 3 : Nombre de tentatives d'infection au logiciel espion lancées par le compte X @Joseph_Gordon16 en fonction de la catégorie des cibles

4.4.1 LE SITE INTERNET THOIBAO.DE PRIS POUR CIBLE

L'un des premiers tweets malveillants envoyés par le compte X @Joseph_Gordon16 visait Thời Báo, un site Web d'information indépendant basé à Berlin couvrant l'actualité du Viêt-Nam. Le tweet en question a été envoyé en réponse à un article publié par Thời Báo, qui concernait une enquête sur la corruption mettant en cause le ministère vietnamien de la Défense. Dans la réponse écrite en langue vietnamienne, l'opérateur du compte indique que l'enquête sur la corruption est liée à des conflits internes ou à une lutte de pouvoir entre le ministère de la Sécurité publique du Viêt-Nam et l'armée (voir figure 6).

Figure 6 : Tweet malveillant ciblant Thoibao.de – Texte : Công an đấu đá nội bộ, Bộ Công an bắt công an Hải Dương

Le lien figurant dans le tweet (Inktonews.co), qui semble renvoyer à un site d'information, est en fait une URL pointant vers une infrastructure d'infection associée à Predator. Il semble que cette infrastructure est à l'origine de tentatives d'installation du logiciel espion Predator sur les appareils de personnes en lien avec ce média.

DATE	DESTINATAIRE	URL	PLATEFORME
9 février 2023	thoibao_de	https://lnktonews[.]co/MEmK	X

Tableau 4 : Lien malveillant vers Predator envoyé à Thoibao.de sur X

Cette prise pour cible et cette tentative d'infection par logiciel espion d'un média basé en UE et de ses collaborateurs et collaboratrices portent clairement atteinte à la capacité des journalistes à couvrir ouvertement des sujets intéressant leur public, ce problème allant jusqu'à toucher des membres de la diaspora. En outre, il existe un risque extrêmement grave que des sources communiquant avec des journalistes soient également infectées par la suite[54].

Khoa Lê Trung dans son bureau.
© Amnesty International

KHOA LÊ TRUNG, RÉDACTEUR EN CHEF DE THOIBAO.DE

Khoa Lê Trung est un journaliste originaire du Viêt-Nam vivant à Berlin, en Allemagne. Il est le rédacteur en chef du média Thoibao.de, dont le compte X a fait l'objet d'une attaque « un clic » lancée au moyen de Predator, le logiciel espion d'Intellexa.

Thời Báo couvre l'actualité politique, économique et environnementale vietnamienne et internationale. En raison du climat de répression dans lequel baigne le paysage médiatique du Viêt-Nam, où les personnes exprimant des opinions critiques en ligne risquent de sévères représailles, le droit de rechercher, de recevoir et de communiquer librement des informations est limité de manière abusive dans le pays[55]. Khoa Lê Trung tente de lutter contre cette tendance à travers Thời Báo et son travail journalistique, qui visent à offrir une source d'informations fiables aux Vietnamien·ne·s. Comptant 20 millions de visites par mois, le site Web de Thời Báo figure parmi les médias en ligne vietnamiens basés à l'étranger les plus consultés.

La surveillance ciblée décrite dans le présent rapport fait partie des nombreuses formes de répression auxquelles sont de plus en plus confrontés les journalistes dans le cadre de leur travail, que ce soit au Viêt-Nam ou dans le monde. Cette surveillance s'accompagne souvent d'actes d'intimidation, de harcèlement et de censure en ligne. L'attaque lancée contre Thời Báo au moyen de Predator n'est qu'un exemple parmi d'autres, Khoa Lê Trung étant victime d'actes de répression en ligne et hors ligne depuis plusieurs années.

[54] Voir par exemple Amnesty International, « Ouzbékistan. La surveillance de masse s'étend au-delà des frontières », 31 mars 2017, https://www.amnesty.org/fr/latest/news/2017/03/uzbekistan-tentacles-of-mass-surveillance-spread-across-borders/
[55] Amnesty International, *Viet Nam: Let us breathe! Censorship and criminalization of online expression in Viet Nam* (index AI : ASA 41/3243/2020), 30 novembre 2020, https://www.amnesty.org/fr/documents/asa41/3243/2020/en/

« On ne devrait pas pouvoir vendre [ces technologies de surveillance] à des pays comme le Viêt-Nam […] ces logiciels et équipements occidentaux se retournent contre l'Allemagne ou [des pays] européens. Cela constitue également une atteinte à la liberté de la presse et à la liberté d'expression des gens ici en Allemagne. »

Khoa Lê Trung

Dans le cadre de son travail pour Thời Báo, Khoa Lê Trung a reçu des menaces de mort et subi de l'intimidation alors qu'il exerçait simplement son droit à la liberté d'expression. Il a déclaré à Amnesty International : « Je reçois également des menaces, surtout de la part de Vietnamiens en Allemagne ; il y a également des gens qui m'appellent ou m'envoient des messages pour me menacer […] de me décapiter si je continue. Il y a aussi des personnes qui viennent directement dans mon bureau pour me dire "Cessez de travailler sur vos reportages, ce n'est pas bon pour vous." » En raison de ces menaces, Khoa Lê Trung est placé sous protection policière à Berlin depuis 2018.

Si cette protection le rassure quelque peu quant à sa sécurité, elle lui impose également certaines restrictions dans sa vie quotidienne. « Chaque fois que je me rends à un événement, je dois me demander si c'est pertinent ou non, et si cela vaut le coup, car je dois systématiquement prévenir la police avant d'y aller. Au cas où il se passerait quelque chose lors de cet événement », a-t-il déclaré à Amnesty International.

La répression dont il est victime sévit également sur Internet. En effet, Khoa Lê Trung a reçu des menaces, fait l'objet de campagnes de dénigrement en ligne, et a souvent été qualifié de « traître ». Il a confié à Amnesty International que le site Web de Thời Báo était bloqué au Viêt-Nam depuis 2017, car il avait couvert cette année-là une affaire politiquement sensible concernant l'enlèvement d'un homme d'affaires vietnamien à Berlin. L'ambassade du Viêt-Nam avait fait pression sur lui pour qu'il retire son article. Il a ajouté que son compte Facebook personnel avait également été bloqué dans le pays. En outre, il affirme que les vidéos qu'il publie sur les réseaux sociaux sont souvent censurées. Obtenir la remise en ligne de reportages vidéo qui ont été retirés par les entreprises de réseaux sociaux à la demande des autorités demande du temps et des efforts. Dans certains cas, les vidéos sont retirées à jamais. « Nous devons déployer des efforts considérables pour qu'elles [les vidéos] soient republiées », a-t-il déclaré à Amnesty International. « J'arrive à obtenir la remise en ligne de certaines vidéos, mais pour d'autres, c'est impossible », a ajouté Khoa Lê Trung.

Les attaques au logiciel espion Predator décrites dans le présent rapport ne sont pas les premières cyberattaques dont il a été la cible. En effet, il a expliqué à Amnesty International que le site Web de Thời Báo avait déjà été visé par des attaques par déni de service distribué (DDoS, voir glossaire), qui avaient provoqué son plantage. Les tentatives d'infection à l'aide de liens malveillants publiés sur les réseaux sociaux, comme celles dont il est question dans le présent rapport, constituent un danger non seulement pour lui, mais aussi pour d'autres journalistes travaillant pour Thời Báo.
Khoa Lê Trung a expliqué à Amnesty International qu'« il y a également de nombreux commentaires sur Thoibao.de qui représentent un danger si on clique dessus, qui sont susceptibles d'infecter des ordinateurs, de provoquer des dysfonctionnements, ou de permettre le vol de données. C'est très dangereux. C'est pourquoi je dois me montrer extrêmement prudent, notamment pour les personnes qui travaillent pour mon site Web. » À cause de ces attaques, Khoa Lê Trung a investi un temps et des ressources considérables pour garantir sa propre cybersécurité ainsi que celle de son site Web et de son personnel, alors qu'il aurait pu les consacrer à du travail journalistique et à des reportages.

Khoa Lê Trung a indiqué à Amnesty International que ces attaques à des fins de surveillance ciblée avaient des conséquences extrêmement néfastes sur les journalistes et les blogueur·euse·s au Viêt-Nam. Il se dit convaincu que ces attaques émanent d'autorités vietnamiennes, qui, selon lui, investissent massivement dans des campagnes de cyberattaques visant des dissident·e·s sur Internet, y compris contre son média d'information en ligne.

> Il a expliqué à Amnesty International que les gouvernements européens étaient tenus de contrôler la vente et le transfert des technologies de surveillance. « On ne devrait pas pouvoir vendre [ces technologies de surveillance] à des pays comme le Viêt-Nam […] de sorte que ces logiciels et équipements occidentaux se retournent contre l'Allemagne ou [des pays] européens. Cela constitue également une atteinte à la liberté de la presse et à la liberté d'expression des gens ici en Allemagne », a-t-il dit à Amnesty International.

Des recherches menées par Amnesty International ont déjà mis au jour d'autres campagnes d'attaques au logiciel espion visant des militant·e·s et blogueur·euse·s vietnamiens basés en Allemagne, qui étaient soupçonnées d'avoir été orchestrées par des acteurs proches du pouvoir. Une enquête de février 2021 a montré que Bui Thanh Hieu, blogueur et militant en faveur de la démocratie, avait été pris pour cible au moyen d'un logiciel espion Windows au moins quatre fois entre février 2018 et décembre 2019[56]. Ce militant de premier plan avait été harcelé à maintes reprises par les autorités vietnamiennes avant de trouver refuge en Allemagne, où il vit depuis 2013. Un autre blogueur, installé quant à lui au Viêt-Nam et dont le nom n'a pas été révélé pour des raisons de sécurité, a été visé trois fois entre juillet et novembre 2020. Les cyberattaquants qui ont tenté d'infecter avec un logiciel espion des militant·e·s vietnamiens se trouvant en Allemagne sont liés à un groupe connu sous le nom d'« Ocean Lotus » dans le milieu de la cybersécurité. À plusieurs reprises, des entreprises de sécurité informatique ont également constaté qu'Ocean Lotus avait visé des dissident·e·s politiques vietnamiens, des États étrangers et des entreprises[57].

4.4.2 DES RESPONSABLES DES NATIONS UNIES ET DE L'UNION EUROPÉENNE TRAVAILLANT SUR LA PÊCHE PRIS POUR CIBLE

Le compte X @Joseph_Gordon16 s'en est pris à une deuxième catégorie de personnes : des universitaires et des responsables s'intéressant à des questions maritimes, notamment des chercheur·euse·s et fonctionnaires travaillant sur des politiques de l'UE et de l'ONU relatives à la pêche illicite ou non déclarée.

L'UE s'est engagée à lutter contre la pêche illicite, non déclarée et non réglementée en adoptant le règlement INN. C'est dans le cadre de ce règlement qu'en octobre 2017, la Commission européenne a adressé au Viêt-Nam un avertissement, prenant la forme d'un « carton jaune », pour l'insuffisance de ses mesures de lutte contre la pêche illicite, invitant les autorités vietnamiennes « à engager une procédure formelle de dialogue afin de résoudre les problèmes recensés et de mettre en œuvre le plan d'action[58] ». Cet avertissement visait non pas à mettre fin aux importations en UE de poissons et de produits de la pêche en provenance du Viêt-Nam, mais à prévenir le pays du risque qu'il courait d'être recensé en tant que pays non coopérant.

Le 16 mai 2023, le compte @Joseph_Gordon16 a répondu publiquement à un·e universitaire espagnol travaillant sur la pêche illégale et les politiques relatives au braconnage (bien que cette personne ne s'intéressait pas aux questions liées au Viêt-Nam). Le tweet contenait un lien malveillant vers Predator, hébergé cette fois sur le domaine asean-news[.]net (voir figure 7). Ce tweet était écrit en espagnol et faisait directement référence au système de « carton jaune » de l'UE : « ¿Cuál es su solución para deshacerse de la tarjeta amarilla? » (« Quelle solution proposez-vous pour faire retirer ce carton jaune ? »).

[56] Amnesty International, "Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks", 24 février 2021, https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks/

[57] Amnesty International, « Viêt-Nam. Des militant·e·s visés par un groupe de pirates tristement célèbre », 24 février 2021, https://www.amnesty.org/fr/latest/press-release/2021/02/viet-nam-hacking-group-targets-activist/ ; Reuters, "Facebook tracks 'OceanLotus' hackers to IT firm in Vietnam", 11 décembre 2020, https://www.reuters.com/article/facebook-vietnam-cyber-idCAKBN28L03Y

[58] Commission européenne, « La Commission adresse un avertissement au Viêt Nam concernant l'insuffisance de ses mesures de lutte contre la pêche illicite », 23 octobre 2017, https://ec.europa.eu/commission/presscorner/detail/fr/ip_17_4064

Figure 7 : Tweet malveillant envoyé à un·e universitaire espagnol travaillant sur les politiques relatives à la pêche

Le 8 février 2023, le compte a envoyé à deux reprises des liens malveillants à Charlina Vitcheva (@vitcheva_eu), la directrice générale de la direction générale des affaires maritimes et de la pêche de la Commission européenne (DG MARE). Les deux tweets contenaient le même lien malveillant renvoyant au domaine witteridea[.]co, associé à Predator, ainsi que le message « Comment cette question sera-t-elle résolue ? ». La DG MARE est chargée d'administrer les mécanismes de l'UE en matière de pêche illicite, non déclarée et non réglementée, y compris le système de carton jaune. L'un des tweets malveillants a été envoyé en réponse à un tweet public (voir figure 8) de Charlina Vitcheva, qui mentionnait plusieurs comptes institutionnels et publics, dont celui de Pierre Karleskind (@Pierre_Ka), eurodéputé français et président de la Commission de la pêche du Parlement européen (voir figure 9). Sur X, tous les comptes mentionnés dans un tweet initial reçoivent les messages envoyés en réponse à ce tweet, tels que celui envoyé par le cyberattaquant. La liste complète des comptes visés par ce tweet malveillant figure dans le tableau 5. Le compte X associé à la mission « Restaurer notre océan et notre milieu aquatique » de l'UE a également été visé deux fois à l'aide de deux liens différents, le 9 février 2023 et le 1er juin 2023 (voir figure 10). Le fait que l'un des messages malveillants fasse directement référence au « carton jaune » de l'UE et que cet universitaire espagnol ainsi que des responsables et personnalités politiques de l'UE travaillant sur la pêche illicite aient été pris pour cible laisse supposer que cette question intéresse directement les responsables de cette campagne d'attaques au logiciel espion Predator.

Figure 8 :
Tweet de @vitcheva_eu sur la pêche mentionnant d'autres comptes auquel le cyberattaquant a répondu

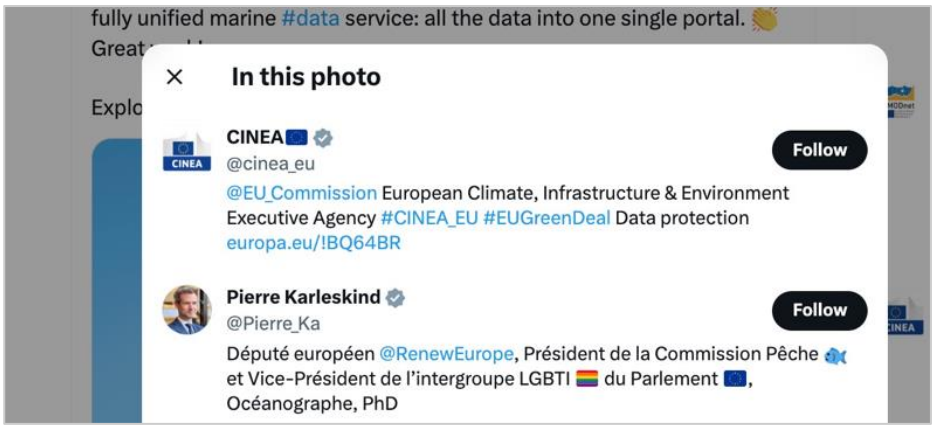


Figure 9 : Le compte @Pierre_Ka a été mentionné par @vitcheva_eu dans son tweet initial et inclus dans le tweet malveillant envoyé en réponse

Figure 10 : Lien malveillant vers Predator envoyé le 1er juin 2023

4.4.3 D'AUTRES INSTITUTIONS ET FONCTIONNAIRES VISÉS

Notre enquête a également établi que @Joseph_Gordon16 avait lancé des attaques à l'encontre d'autres fonctionnaires de l'UE et de 11 institutions liées à l'UE (les attaques visant le compte associé à la mission « Restaurer notre océan et notre milieu aquatique » décrites au point 4.4.2 en font partie).

Le compte X public de la présidente du Parlement européen Roberta Metsola, notamment, a été pris pour cible le 1er juin 2023 par @Joseph_Gordon16, qui lui a envoyé une URL malveillante contenant le domaine southchinapost[.]net, associé à Predator.

Figure 11 : Lien malveillant envoyé à Roberta Metsola, la présidente du Parlement européen

Presque au même moment, le compte institutionnel officiel de la Commission européenne a également été visé sur X par @Joseph_Gordon16, qui a utilisé le même lien malveillant que celui envoyé à Roberta Metsola.

Figure 12 : Lien malveillant envoyé au compte X officiel de la Commission européenne

Le compte X de l'ambassadrice de l'Allemagne aux États-Unis a lui aussi été pris pour cible par @Joseph_Gordon16, le 8 mars 2023.

Figure 13 : Lien malveillant envoyé à Emily Haber, ambassadrice de l'Allemagne aux États-Unis au moment de l'attaque

DATE	DESTINATAIRE	URL	PLATEFORME
8 février 2023	@vitcheva_eu @EMODnet @cinea_eu @Pierre_Ka @EUgreenresearch @CMEMS_EU @FSUMDC @UNDPOceanInnov @REA_research @EU_ENV @EUClimateAction @eumissionocean	https://witteridea[.]co/LFJeZQu	X (anciennement Twitter)
8 février 2023	vitcheva_eu	https://witteridea[.]co/LFJeZQu	X
8 mars 2023	GermanAmbUSA	https://Inktonews[.]co/CVgp	X
1er juin 2023	EP_President	https://southchinapost[.]net/VuAfn	X
1er juin 2023	EU_Commission	https://southchinapost[.]net/VuAfn	X
1er juin 2023	EU_Commission	https://southchinapost[.]net/VuAfn	X
1er juin 2023	eumissionocean	https://southchinapost[.]net/VuAfn	X

Tableau 5 : Liens malveillants envoyés à des personnalités politiques et à des institutions européennes

ATTAQUES CONTRE DES REPRÉSENTANT·E·S DE L'ÉTAT À TAIWAN ET AUX ÉTATS-UNIS

L'opérateur du compte @Joseph_Gordon16 a envoyé un tweet contenant un lien malveillant en réponse à Tsai Ing-wen, la présidente de Taiwan, le 14 avril 2023. Un sénateur des États-Unis pour le Dakota du Nord, John Hoeven (@SenJohnHoeven), était mentionné dans le tweet initial publié par Tsai Ing-wen. Par conséquent, le tweet de réponse et son lien malveillant ont également été envoyés indirectement au compte X du sénateur (voir figure 14).

Figure 14 : Lien malveillant envoyé à Tsai Ing-wen (@iingwen) et au sénateur américain John Hoeven

Le site Web géré par le cyberattaquant et hébergé sur le domaine caavn[.]org était vraisemblablement configuré de façon à rediriger les requêtes que X envoie pour générer l'aperçu d'un lien vers l'authentique site Internet du *South China Morning Post*, afin de créer un aperçu plausible. Cette tactique est fréquemment utilisée pour infecter des appareils avec un logiciel espion. Dans le cas présent, l'aperçu contient des informations issues d'un véritable article publié sur le site du *South China Morning Post* au sujet de la coopération entre les États-Unis et Taiwan en matière de sécurité.

Toujours le 14 avril, @Joseph_Gordon16 a également envoyé un tweet de réponse contenant un lien malveillant au compte X du ministère taiwanais des Affaires étrangères. Comme @Joseph_Gordon16 répondait à un tweet dans lequel était mentionné le membre de la Chambre des représentants des États-Unis Michael McCaul, qui représente la 10e circonscription du Texas, celui-ci a également reçu le message malveillant de façon automatique. Michael McCaul était mentionné dans le tweet initial en sa qualité de

président de la Commission des affaires étrangères de la Chambre des représentants du Congrès des États-Unis.

Figure 15 : Lien malveillant envoyé au ministère taiwanais des Affaires étrangères et au député Michael McCaul

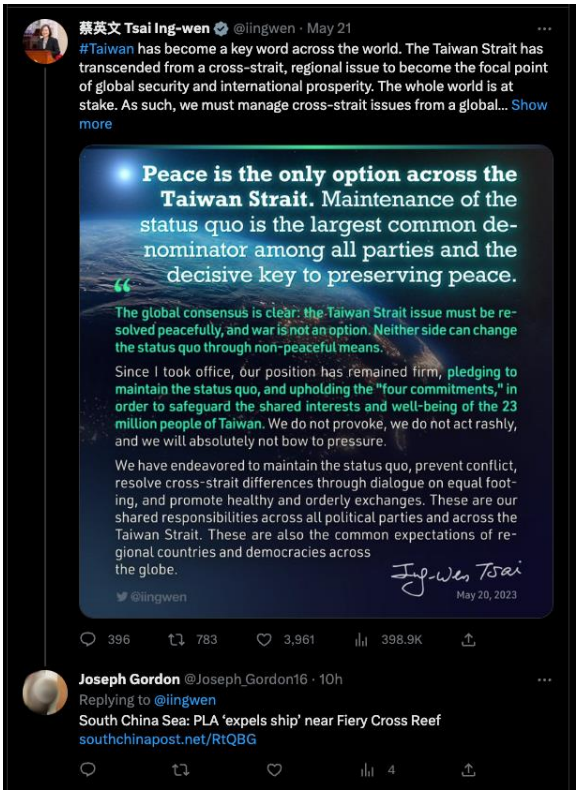


Figure 16 : Lien malveillant envoyé à Tsai Ing-wen (@iingwen) s'appuyant sur un autre domaine associé à Predator, southchinapost[.]net

L'opérateur du compte @Joseph_Gordon16 a de nouveau pris pour cible Tsai Ing-wen le 21 mai 2023. Cette tentative d'infection à Predator reposait cette fois sur le domaine southchinapost[.]net (voir figure 16).

HAUTS FONCTIONNAIRES ET INSTITUTIONS AMÉRICAINS ET TAIWANAIS PRIS POUR CIBLE AU MOYEN DU LOGICIEL ESPION PREDATOR

DATE	DESTINATAIRE	URL	PLATEFORME
14 avril 2023	@iingwen @SenJohnHoeven	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@MofaTaiwan	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
22 mai 2023	@iingwen	https://southchinapost[.]net/RtQBG	X

Tableau 6 : Liens malveillants envoyés à des fonctionnaires et à des institutions américains et taiwanais

4.4.4 AUTRES TENTATIVES D'INFECTION AU LOGICIEL ESPION PREDATOR LIÉES AU MÊME OPÉRATEUR

Outre le compte X @Joseph_Gordon16, Amnesty International a déterminé qu'un autre compte de réseau social avait envoyé des liens pointant vers les mêmes domaines associés à Predator. En effet, le compte Facebook « Anh Tran » a partagé des liens qui contenaient le domaine caavn[.]org renvoyant au logiciel espion. Le fait que les mêmes noms de domaine personnalisés figurent dans les liens envoyés par les deux comptes indique que ceux-ci sont vraisemblablement liés au même opérateur de Predator.

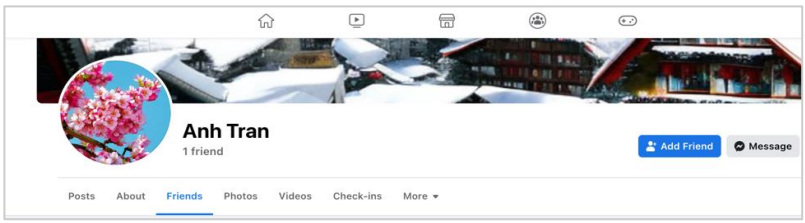


Figure 18 : Profil Facebook du compte Anh Tran

Amnesty International a constaté que ce compte avait publié deux commentaires en mars 2023 sur la page Facebook publique du groupe d'opposition politique vietnamien « Liên Minh Dân Tộc Việt Nam », basé aux États-Unis[59]. Les liens malveillants étaient insérés dans des commentaires Facebook publics, et les URL imitaient cette fois-ci celles d'articles publiés sur le site Web d'information vietnamien Tiếng Dân (voir figure 19)[60]. Ce site avait déjà fait l'objet d'attaques DDoS et été pris pour cible par le groupe Ocean Lotus par le passé[61].

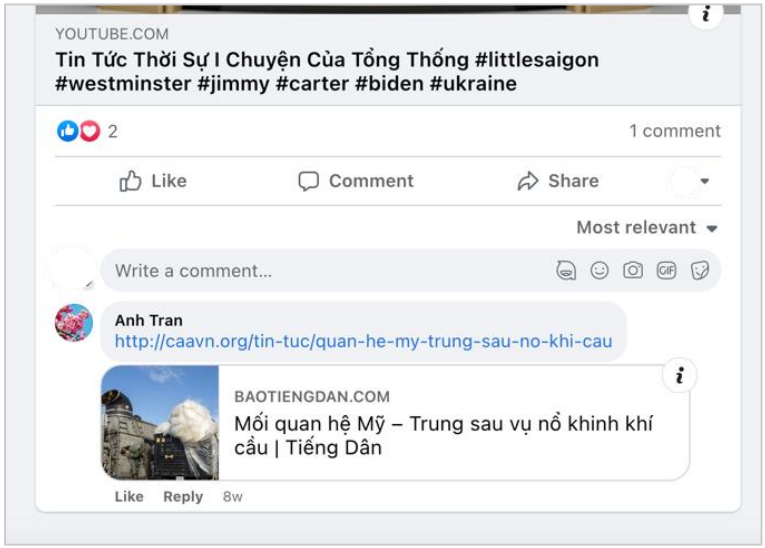


Figure 19 : Lien malveillant imitant l'adresse du site baotiengdan.com

Cette nouvelle tentative d'infection visant un groupe politique de la diaspora vietnamienne sur Facebook illustre la persistance des objectifs poursuivis par l'opérateur de Predator à l'origine de ces attaques. Ces liens malveillants partagés publiquement ne représentent probablement qu'une partie des attaques ciblées lancées dans le cadre de cette campagne de surveillance. En effet, les tentatives d'infection effectuées au moyen d'applications de messagerie instantanée ou de messages directs sont plus difficiles à détecter pour les chercheur·euse·s.

[59] Facebook, Liên Minh Dân Tộc Việt Nam, https://www.facebook.com/LMDTVN/ (consulté le 26 septembre 2023)
[60] Tiếng Dân, https://baotiengdan.com/ (consulté le 26 septembre 2023)
[61] Deflect, "News From Deflect Labs: DDoS attacks against Vietnamese Civil Society", 7 septembre 2018, https://deflect.ca/ddos-attacks-vietnamese-civil-society/

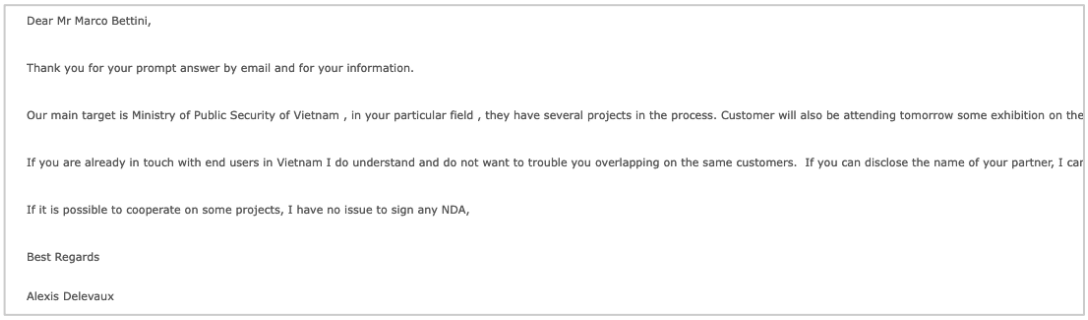
4.5 TRANSACTIONS ENTRE L'ALLIANCE INTELLEXA ET LE VIÊT-NAM

Amnesty International a examiné les rapports et les analyses que l'EIC a préparés sur la base de documents d'entreprise confidentiels, auxquels les médias partenaires du réseau ont pu accéder dans le cadre de l'enquête sur les « Predator files ». Ces travaux, qui ont été communiqués à Amnesty International avant leur publication, font état des ventes par l'alliance Intellexa de ses technologies de surveillance aux autorités vietnamiennes. Corroborées par les éléments et l'expertise techniques exposés dans la section 4.4, les conclusions de l'EIC, dont font notamment partie Mediapart et *Der Spiegel*, viennent renforcer le faisceau de preuves techniques concernant l'origine des attaques.

L'enquête de l'EIC indique que Nexa Technologies a conclu début 2020 un contrat portant sur des « solutions d'infection » avec le ministère vietnamien de la Sécurité publique, par l'intermédiaire d'Advanced Middle East Systems, une filiale commerciale du groupe Nexa basée aux Émirats arabes unis. L'analyse de l'EIC révèle en outre que ce projet, répondant au nom de code « poisson-pêcheur », prévoyait l'octroi d'une licence de deux ans et se chiffrait à 5,6 millions d'euros. L'EIC a pu consulter un deuxième document de Nexa Technologies, daté de janvier 2021, indiquant que ce contrat devait générer un chiffre d'affaires de 3,36 et 2,44 millions d'euros en 2021 et 2022, respectivement.

Un autre document obtenu dans le cadre de l'enquête, daté du 26 janvier 2021 et relatif à des prévisions de ventes, révèle qu'Advanced Middle East Systems essayait d'obtenir la « prolongation » du contrat de 800 000 euros portant sur Blue Arrow que l'entreprise avait conclu avec le ministère vietnamien de la Sécurité publique. Les entités de l'alliance Intellexa ont vendu leurs solutions de cybersurveillance associées à Predator sous la marque « Arrow », qui apparaît notamment dans les noms de produit « Green Arrow » et « Red Arrow ». La documentation disponible ne permet toutefois pas de déterminer si la prolongation du contrat a bien été signée.

D'après d'autres pièces que l'EIC a examinées, un mois plus tard, le 19 février 2021, Advanced Middle East Systems a vendu le logiciel espion Arrow à l'entreprise Delsons Hong Kong Limited, immatriculée à Hong Kong. Des informations publiques figurant dans le registre des sociétés de Hong Kong[62] indiquent que Delsons Hong Kong appartient à Alexis Delevaux, un homme d'affaires suisse vivant en Asie et occupant par ailleurs la fonction de consul honoraire de Monaco à Hanoï. Une série de courriels liés au fournisseur de logiciels espions Hacking Team, qui a été rendue publique, comprend des messages envoyés par M. Delevaux en 2011, dans lesquels il fait part à Hacking Team de son souhait de lui acheter son logiciel espion[63] pour le compte de clients au sein du ministère vietnamien de la Sécurité publique (voir figure 20)[64].



Dear Mr Marco Bettini,

Thank you for your prompt answer by email and for your information.

Our main target is Ministry of Public Security of Vietnam , in your particular field , they have several projects in the process. Customer will also be attending tomorrow some exhibition on the

If you are already in touch with end users in Vietnam I do understand and do not want to trouble you overlapping on the same customers. If you can disclose the name of your partner, I car

If it is possible to cooperate on some projects, I have no issue to sign any NDA,

Best Regards

Alexis Delevaux

Figure 20 : Courriel de 2011 rendu public portant sur l'achat à Hacking Team de logiciels espions pour le compte du ministère vietnamien de la Sécurité publique

[62] Registre des sociétés de Hong Kong, https://www.icris.cr.gov.hk/csci/ (consulté le 2 octobre 2023)
[63] Hacking Team était un développeur italien de logiciels espions. On lui doit le logiciel espion Galileo, qui a été vendu à de nombreux pays dans le monde entier
[64] WikiLeaks, "Hacking Team: [BULK] RE: demand information Vietnam following Milipol", 8 juillet 2015, https://wikileaks.org/hackingteam/emails/emailid/571541

Des registres d'exportation[65] obtenus par Amnesty International et l'EIC révèlent que Delsons Hong Kong Ltd. a fait livrer par avion au Viêt-Nam 30 pièces de matériel informatique d'une valeur de 8,5 millions de dollars des États-Unis, le 1er novembre 2021. Ces marchandises étaient destinées à « BCA – Thang Long Co., Ltd », une société publique établie au Viêt-Nam en 1993 par décret du ministre de la Sécurité publique. Comme l'indique son site Internet, cette société exerce entre autres des activités d'import-export pour le ministère vietnamien de la Sécurité publique[66].

Parmi les produits livrés figuraient un « module de surveillance pour PC », un « centre de contrôle » et un « module de surveillance pour smartphone » faisant partie d'un « système logiciel professionnel » (voir figure 21). D'une valeur de 8,4 millions de dollars, ces trois articles ont été fabriqués par « AS ». L'EIC, qui a examiné les travaux d'Amnesty International, a confirmé que « AS » était une abréviation employée dans les documents internes du groupe Nexa pour désigner Advanced Middle East Systems. La commande comprenait 27 autres articles, dont la valeur totale s'élevait à 167 600 dollars des États-Unis. Il s'agissait notamment de serveurs et d'ordinateurs de bureau Dell, d'équipement de réseau et d'un ordinateur portable.

Les informations obtenues par Amnesty et l'EIC concernant cette cargaison proviennent de trois bases de données de registres d'exportation différentes. Les données concordent parfaitement en ce qui concerne tous les aspects de la cargaison (prix, quantité et description des marchandises, date de livraison, entreprises exportatrices et importatrices), sauf le pays d'origine. En effet, deux des bases de données indiquent que les marchandises ont été expédiées depuis les Émirats arabes unis, tandis que la troisième mentionne Israël comme pays d'expédition. L'EIC a contacté la douane israélienne et le gouvernement émirati en vue d'obtenir des précisions, mais la première a refusé de s'exprimer au sujet de cette cargaison, et le second n'a pas répondu.

Amnesty International pense que cette commande envoyée par Delsons Hong Kong Ltd. est liée à la vente au Viêt-Nam du système de logiciel espion Predator. Amnesty International a adressé une lettre à Delsons afin d'obtenir une réponse concernant ces constatations, mais la société n'avait toujours pas répondu au moment de la publication de ce rapport. L'EIC a également contacté Delsons Hong Kong Ltd. pour demander des explications.

[65] Les registres d'exportation, aussi appelés registres d'expédition ou lettres de transport, sont des documents utilisés par un transporteur pour attester la réception de marchandises. Y figurent notamment le mode de transport, la valeur déclarée, la quantité d'unités, l'expéditeur, le destinataire, le type de marchandises et leur description

[66] BCA – Thang Long Co., Ltd, https://bca-thanglong.vn/ (consulté le 26 septembre 2023)

< 10/13 >

Transaction date	2021/11/01
B/L No.	--
Buyers	Bca Thang Long One Member Limited Company
Supplier	Delsons Hong Kong Ltd.
Import area	Vietnam
Export area	Israel
Product description	MOBILE SMART PHONE MONITORING MODULE BELONGING TO PROFESSIONAL SOFTWARE SYSTEM, MANUFACTURER: AS @ Translate
HS code	84714190
Quantity	1.0 OTHER
Weight	--
Total price	2800000.0
Unit price	2800000.0
POL	--
POD	--
Shipping methods	Air Transport
Contact person	--

Figure 21 : Vente à BCA – Thang Long Co. d'un « module de surveillance pour smartphone » d'une valeur déclarée de 2,8 millions de dollars[67]

D'autres registres d'exportation auxquels Amnesty International a pu accéder montrent qu'Advanced Middle East Systems a expédié directement des composants de réseau informatique pendant la même période, en octobre 2021, à une société vietnamienne dénommée i-Globe. Selon son site Internet, cette société opère dans le domaine des « solutions de sécurité, de chiffrement, informatiques et spécialisées, dédiées aux organisations gouvernementales spéciales, aux entreprises…[68] » Sur son compte Facebook, i-Globe affirme travailler avec le ministère vietnamien de la Sécurité publique[69].

Figure 22 : Capture d'écran du site Web d'i-Globe

D'après l'analyse réalisée par l'EIC de la documentation interne accessible au consortium, ainsi que les informations complémentaires concernant la cargaison évoquées plus haut, Amnesty International pense que Predator, le logiciel espion d'Intellexa, a été vendu par Advanced Middle East Systems, une filiale commerciale du groupe Nexa, à un client vietnamien au sein du ministère de la Sécurité publique du Viêt-

[67] 52wmb.com, registres d'exportation, https://www.52wmb.com/ (consulté le 26 septembre 2023)
[68] i-Globe, https://iglobe.com.vn/en/ (consulté le 26 septembre 2023)
[69] "i-Globe Techno J. Is Specialised company who serves for customers from MoD, MoPS and other." Voir Facebook, i-Globe Technology Investment & Development Joint Stock Company, 15 novembre 2021, https://www.facebook.com/connectingworldtechnologies/posts/pfbid025VoHTQp81AUVAskXRK14hRUkZvu48cgnZTCAx5ZnvMBqhW76B8MfsambnDuaU67SI

Nam, par le truchement de plusieurs entreprises intermédiaires internationales et locales. Dans une lettre de réponse envoyée à l'EIC, des représentants du groupe Nexa ont déclaré :

> « Advanced Middle East Systems a ensuite collaboré brièvement avec Intellexa pour l'aider à commercialiser ses solutions. Advanced Middle East Systems agissait en qualité de revendeur/intermédiaire et n'avait pas la charge de l'*export control*. Il appartenait au fabricant de la solution de solliciter les autorisations d'export en fonction des pays dans lesquels la solution pouvait être installée.
>
> « Sur ce sujet, vos informations sont inexactes. S'il est vrai que certains contrats d'intermédiation ont été signés, en total respect des règles d'export, concernant des technologies que vous qualifiez "d'offensives", aucun de nos contrats n'a été exécuté. En 2021, nous les avons tous dénoncés avant que ceux-ci soient opérationnels parce que nous jugions que ces technologies sont trop controversées. »

Dans une réponse complémentaire, les représentants de Nexa confirment que des contrats portant sur des technologies informatiques offensives ont été conclus avec le Viêt-Nam. Ils affirment cependant avoir mis un terme à leur contribution relative à la partie des contrats portant sur le logiciel espion, pour ne conserver que la partie traitant de la cybersécurité :

> « Nous vous confirmons que les dénonciations des contrats de Lutte Informatique Offensive (LIO) sur les pays cités sont effectives et réelles. Sur le Viêt-Nam seule la partie [du contrat] traitant de la Cybersécurité a été conservée. Encore une fois, nous avons pris la décision de tourner la page et d'arrêter toute action dans le domaine de la LIO. »

À la suite de cette réponse de Nexa Technologies, l'EIC a demandé des précisions sur les transactions entre Delsons et le Viêt-Nam évoquées dans la présente section. Au moment de la publication de ce rapport, l'EIC n'avait pas encore reçu de réponse.

4.6 ÉVALUATION DES RESPONSABILITÉS QUANT AUX ATTAQUES

Notre étude de cas démontre le risque que font peser les produits d'Intellexa sur le travail des défenseur·e·s des droits humains, des journalistes et des représentant·e·s d'institutions internationales, entre autres. Nous avons vu dans ce chapitre, qui se fonde sur les recherches menées par le Security Lab d'Amnesty International, comment l'opérateur du compte @Joseph_Gordon16 a tenté d'infecter des cibles au moyen d'attaques « un clic » lancées à l'aide d'un système de logiciel espion. Amnesty International conclut, avec un degré de certitude élevé, que les tentatives d'infection décrites dans ce rapport sont liées à Predator, le logiciel espion d'Intellexa, et à l'infrastructure de cybersurveillance associée.

Valides et limitées dans le temps, les URL malveillantes utilisées dans le cadre de ces attaques n'ont pu être générées que par un opérateur ayant accès à l'interface administrative *back-end* d'un client de Predator. Ces éléments laissent supposer que l'opérateur du compte @Joseph_Gordon16 est soit un client direct d'Intellexa, soit une entité collaborant en temps réel et de façon continue et opérationnelle avec un client s'étant procuré Predator auprès d'Intellexa. Comme le montre la section précédente, des registres d'expédition et d'autres documents indiquent que le Viêt-Nam a acheté des logiciels espions à l'alliance Intellexa.

Cette campagne d'attaques récemment mise au jour visait la société civile et des journalistes vietnamiens, ainsi que des responsables politiques travaillant sur des questions intéressant le gouvernement du Viêt-Nam. Les tentatives d'infection au logiciel espion lancées dans le cadre de cette campagne s'appuyaient sur des URL conçues pour imiter celles d'authentiques sites Web vietnamiens. Amnesty International a communiqué des éléments techniques concernant cette campagne d'attaques à des spécialistes du groupe d'analyse des menaces de Google, qui ont indiqué à l'EIC qu'elle était selon eux « liée à un acteur gouvernemental au Viêt-Nam ». En outre, des chercheurs et chercheuses en sécurité de Meta ont précédemment identifié un client s'étant procuré Predator auprès de Cytrox (une entreprise de l'alliance Intellexa). Selon eux, ce client serait basé au Viêt-Nam[70].

[70] Meta, *Threat Report on the Surveillance-for-Hire Industry* (op. cit.), https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

S’appuyant notamment sur les recherches menées par l’EIC dans le cadre de l’enquête sur les « Predator files », le présent chapitre a également exposé les antécédents d’Intellexa en matière de vente de logiciels espions au Viêt-Nam. Les analyses techniques, auxquelles s’ajoutent les preuves attestant des transactions entre l’alliance Intellexa et le Viêt-Nam, laissent à penser que l’opérateur du compte entretenait des liens étroits avec le Viêt-Nam et qu’il était susceptible d’avoir agi pour le compte des autorités vietnamiennes ou de groupes d’intérêts du pays. Amnesty International a communiqué ces conclusions aux autorités vietnamiennes avant la publication de l’enquête. L’organisation n’avait reçu aucune réponse au moment de la publication du présent rapport.

5. LES CONSÉQUENCES SUR LES DROITS HUMAINS DE L'UTILISATION DE LOGICIELS ESPIONS

5.1 INTERDICTION DES LOGICIELS ESPIONS HAUTEMENT INTRUSIFS

Afin d'éviter tout abus, les États ne peuvent procéder à une surveillance numérique ciblée qu'en présence de garanties suffisantes en matière de droits humains. En vertu des normes internationales relatives aux droits humains, la surveillance ciblée ne peut être exercée que lorsqu'elle est motivée par des soupçons raisonnables et individualisés, dans le respect du droit, lorsqu'elle est strictement nécessaire pour atteindre un objectif légitime et lorsqu'elle est proportionnelle à cet objectif et non discriminatoire[71].

Cependant, même un cadre réglementaire respectueux des droits humains ne suffirait pas à empêcher les atteintes aux droits humains liées à l'utilisation de certains logiciels espions hautement intrusifs. Ceux-ci permettent un accès illimité à l'appareil visé et leur utilisation ne peut pas faire l'objet d'un contrôle indépendant. Ils ne peuvent jamais être utilisés dans le respect des droits fondamentaux et doivent être interdits de façon permanente. Comme l'a fait observer le Contrôleur européen de la protection des données, en cas d'utilisation de ce type d'outils hautement intrusifs, « le niveau d'immixtion dans l'exercice du droit à la vie privée est d'une gravité telle que la personne se trouve en réalité privée de ce droit. En d'autres termes, il est porté atteinte à l'essence même du droit. L'utilisation d'un tel logiciel ne peut donc pas être considérée comme proportionnelle – que la mesure puisse ou non être jugée nécessaire[72]. » La rapporteuse spéciale des Nations unies sur les droits de l'homme et la lutte antiterroriste a tenu un raisonnement

[71] Pacte international relatif aux droits civils et politiques, Observation générale n° 34 du Comité des droits de l'homme, 12 septembre 2011, https://undocs.org/fr/CCPR/C/GC/34.
[72] Contrôleur européen de la protection des données, *Preliminary Remarks on Modern Spyware*, 15 février 2022, p. 8 [traduction non officielle].

similaire, affirmant que tout logiciel espion dont les fonctionnalités ne peuvent pas être restreintes de façon efficace et dont l'utilisation ne peut pas faire l'objet d'un contrôle indépendant doit être interdit[73].

Le logiciel espion Predator, ainsi que ses variantes aux noms divers, sont des logiciels espions hautement intrusifs qui peuvent accéder par défaut à une quantité illimitée de données sur les appareils infectés et qui ne peuvent actuellement faire l'objet d'aucun contrôle indépendant. En conséquence, il est impossible de déterminer si leurs fonctionnalités peuvent, à l'heure actuelle, être limitées. De ce fait, selon l'analyse d'Amnesty International, Predator est un logiciel espion hautement intrusif et ne peut donc pas être déployé dans le respect des droits fondamentaux.

De même, 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[74]. Amnesty International considère que rien ne saurait raisonnablement justifier le recours à la surveillance de masse non ciblée. En effet, ce type de surveillance ne respecte jamais les principes de nécessité et de proportionnalité, en vertu desquels les États doivent utiliser les outils de surveillance disponibles qui sont les moins restrictifs pour les droits. La surveillance de masse ne peut pas répondre à ces exigences car elle collecte des quantités illimitées de données, et son utilisation ne peut pas être respectueuse des droits humains.

5.2 INSUFFISANCE DES GARANTIES EXISTANTES EN MATIÈRE DE DROITS HUMAINS

L'utilisation de logiciels espions hautement intrusifs comme Predator doit faire l'objet d'une interdiction générale en raison des risques qu'elle entraîne pour les droits fondamentaux. Les autres types de logiciels espions moins intrusifs dont les fonctionnalités peuvent être restreintes et dont l'utilisation peut faire l'objet d'une vérification et d'un contrôle indépendants doivent être soumis à un moratoire en attendant l'élaboration de garanties relatives aux droits humains capables d'empêcher leur utilisation abusive. Ces garanties pourraient être, par exemple, la réglementation des exportations de technologies de surveillance afin que les autorisations d'exportation soient systématiquement refusées dès lors qu'il existe un risque substantiel que le produit exporté soit utilisé pour violer les droits humains, la mise en œuvre d'une législation nationale qui offre des garanties contre les atteintes aux droits humains causées par la surveillance numérique, et la création de mécanismes d'obligation de rendre des comptes destinés à offrir une voie de recours aux victimes de surveillance abusive.

Amnesty International et de nombreuses autres organisations de la société civile[75], ainsi que le Haut-commissariat aux droits de l'homme[76], plusieurs expert·e·s régionaux et des Nations unies[77], et au moins un État, le Costa Rica[78], ont demandé l'instauration d'un moratoire sur la vente, le transfert, l'exportation et l'utilisation des logiciels espions jusqu'à ce qu'un système adéquat de garanties en matière de droits humains soit en place.

---

[73] Rapporteuse spéciale des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach,* avril 2023, § 66, 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.

[74] Security Lab d'Amnesty International, "Predator Files: Technical deep-dive into Intellexa Alliance surveillance products" (op. cit.), https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

[75] Amnesty International, *Global Digital Compact: joint submission on targeted surveillance* (index : IOR 10/6726/2023) 1er mai 2023, https://www.amnesty.org/en/documents/ior10/6726/2023/en/.

[76] Rapport du Haut-Commissariat aux droits de l'homme des Nations unies, *The right to privacy in the digital age*, août 2022, A/HRC/51/17.

[77] Organisation des Nations unies, "Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech", 12 août 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening ; Organisation des États américains, "IACHR and RFOE: Dominican Republic must investigate spying on investigative journalist using Pegasus spyware", 1er juin 2023, https://www.oas.org/en/iachr/jsForm/?File=/en/iachr/media_center/preleases/2023/106.asp ; Conseil des droits de l'homme des Nations unies, Rapport du Groupe de travail sur les disparitions forcées ou involontaires (en anglais), 11 septembre 2023, A/HRC/54/22/Add.5, § 21, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G23/182/83/PDF/G2318283.pdf?OpenElement.

[78] Access Now, "Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology", 13 avril 2022 (mis à jour le 26 janvier 2023), https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/.

À la suite des révélations du projet Pegasus, quelques progrès ont été faits dans la réglementation des logiciels espions. Le Bureau de l'industrie et de la sécurité (BIS) du gouvernement des États-Unis a placé de nombreuses sociétés vendant des logiciels espions sur sa liste des entités ayant des activités numériques malveillantes, dont deux entreprises de l'alliance Intellexa, ainsi que des vendeurs de logiciels espions tristement célèbres comme NSO Group et Candiru[79]. La Maison-Blanche a publié un décret interdisant au gouvernement américain d'utiliser des logiciels espions commerciaux qui « présentent des risques importants en matière de contre-espionnage ou de sécurité pour le gouvernement des États-Unis ou des risques d'utilisation abusive par un gouvernement étranger ou une personne étrangère[80] ». Par ailleurs, 11 États ont annoncé conjointement des initiatives de lutte contre la prolifération et l'utilisation abusive des logiciels espions commerciaux[81]. Au Sommet pour la démocratie, 45 pays ont adopté de nouveaux principes directeurs sur l'utilisation des technologies de surveillance par les gouvernements[82]. Sous l'égide des États-Unis, quelques États ont signé un Code de conduite sur l'amélioration du contrôle des exportations des biens et des technologies susceptibles d'être mal utilisés et de donner lieu à de graves atteintes aux droits humains[83]. Des actions en justice et diverses enquêtes nationales sont en cours dans plusieurs pays, par exemple en Espagne, aux États-Unis, en France, en Hongrie, en Inde, en Israël, en Pologne, au Royaume-Uni et en Thaïlande[84]. En mai 2023, le Parlement européen a conclu les travaux de la Commission d'enquête chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (PEGA), condamnant des utilisations abusives de logiciels espions dans plusieurs États membres de l'UE et réclamant des réformes.

Ces mesures 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 donné lieu à des mesures décisives, et les 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, comme indiqué ci-dessus, certains États ont pris volontairement des initiatives, d'autres ont bloqué des enquêtes et n'ont pas fait preuve d'une véritable transparence. Par exemple, le parquet hongrois a clos son enquête sur l'utilisation illégale de Pegasus dans le pays, évoquant « l'absence de collecte d'informations non autorisée et secrète ainsi que d'utilisation d'un dispositif dissimulé[85] ». En Espagne, un tribunal de Barcelone a dû suspendre une enquête faute d'avoir reçu les informations rogatoires demandées aux autorités israéliennes[86]. En 2021, la Cour suprême indienne a mis sur pied un comité technique chargé d'enquêter sur les utilisations abusives du logiciel Pegasus. Ce comité a conclu son enquête en 2022, mais la Cour n'a pas rendu publiques les conclusions de son rapport[87]. Elle a en outre noté que les autorités indiennes « n'avaient pas coopéré » avec l'enquête du comité technique[88].

Les conséquences dramatiques de la surveillance illégale et non contrôlée continuent de menacer les droits au respect de la vie privée et à la liberté d'expression, d'association et de réunion pacifique des personnes

---

[79] Département d'État des États-Unis, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities", 3 novembre 2021, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/ ; Département d'État des États-Unis, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities", 18 juillet 2023, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/.

[80] Maison blanche, "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security", 27 mars 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.

[81] Maison blanche, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware", 30 mars 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.

[82] Département d'État des États-Unis, "Guiding Principles on Government Use of Surveillance Technologies", 30 mars 2023, https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/.

[83] Département d'État des États-Unis, "Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy", 30 mars 2023, https://www.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy/#:~:text=The%20Export%20Controls%20and%20Human,technology%20that%20violate%20human%20rights.

[84] Citizen Lab, "Litigation and other formal complaints related to mercenary spyware", 12 décembre 2018 (mis à jour le 31 juillet 2023), https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#NSO.

[85] Al Jazeera, "Hungary prosecutors open investigation into Pegasus spying claims", 22 juillet 2021, https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims.

[86] El Nacional, "Judge suspends first Catalan espionage case; lawyer demands reopening and widening", 30 mai 2022, https://www.elnacional.cat/en/politics/judge-closes-torrent-maragall-pegasus-spyware-catalonia_765453_102.html.

[87] "Indian supreme court orders inquiry into state's use of Pegasus spyware", *The Guardian*, 27 octobre 2021 https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware.

[88] The Wire, "Pegasus: Malware Found in 5 Phones, Government 'Refused to Cooperate' With Probe, Says CJI", 25 août 2022, https://thewire.in/law/supreme-court-pegasus-technical-committee.

visées. Les répercussions sur les femmes défenseures des droits humains[89], ainsi que sur les personnes victimes de formes multiples et croisées de discrimination fondée sur la race, l'appartenance ethnique, l'identité religieuse, le handicap, l'orientation sexuelle et l'identité de genre, restent particulièrement graves. Les femmes racisées, issues de minorités ethniques ou religieuses, en situation de handicap, lesbiennes, bisexuelles ou transgenres, ainsi que les personnes ne se conformant pas aux normes de genre, sont exposées à des préjudices spécifiques et exacerbés.

Par ailleurs, quand un logiciel espion continue d'être utilisé sans contrôle et en l'absence de toute garantie, il a un effet dissuasif sur le travail en faveur des droits humains, car les militant·e·s s'autocensurent par crainte d'être surveillés[90]. En outre, les répercussions vont bien au-delà des personnes visées. Elles touchent toutes les personnes qui risquent de renoncer à exercer leurs droits à la liberté d'expression, d'association et de réunion pacifique, entre autres, sachant que les données relatives à leurs activités pourront être utilisées contre elles.

Les dernières révélations montrent que la société civile reste confrontée au fléau des logiciels espions non réglementés, notamment les médias, les journalistes et les chercheurs et chercheuses universitaires. Par ailleurs, le fait que des autorités officielles nationales, régionales et internationales, dont des responsables diplomatiques, aient été prises pour cible confirme une fois encore ce qu'Amnesty International dénonce de longue date : les logiciels espions commerciaux ont de graves répercussions à la fois sur les droits humains et sur la sécurité de l'écosystème numérique dans son ensemble. Non réglementées, ces armes numériques peuvent se retourner contre des gouvernements et autres autorités de pays tiers – ce qui a d'ailleurs déjà été le cas.

Les récentes initiatives volontaires des États viennent s'ajouter à des initiatives existantes, comme l'Arrangement de Wassenaar relatif aux contrôles des exportations d'armes conventionnelles et de biens et technologies à double usage, dans lequel les États participants acceptent d'harmoniser leurs régimes d'exportation. Cependant, l'Arrangement de Wassenaar n'est pas juridiquement contraignant et repose sur les engagements volontaires des États. Amnesty International a en outre déjà fait remarquer que son mandat ne couvrait pas la protection des droits humains[91]. D'ailleurs, dans ses recommandations au Conseil européen et à la Commission européenne à la suite de l'enquête de la commission PEGA, le Parlement européen a appelé à ce que cet instrument devienne contraignant et a souligné qu'il devrait prévoir un cadre relatif aux droits humains pour l'évaluation des licences d'exportation[92].

La mise en œuvre des déclarations volontaires des États doit être étroitement surveillée afin de vérifier si ceux-ci respectent vraiment leurs engagements publics et font ce qu'ils ont promis. Des efforts plus concertés de la part des États 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[93]. » Amnesty International estime que c'est toujours le cas, malgré quelques premiers progrès. Les entreprises et les États qui achètent leurs produits continuent d'œuvrer dans le plus grand secret pour déployer des logiciels espions intrusifs contre la société civile et des journalistes pour la seule raison qu'ils exercent leurs droits fondamentaux et font leur travail pour protéger les droits d'autrui. Les dernières révélations présentées dans ce rapport viennent nous rappeler qu'une action étatique plus efficace et plus concertée est nécessaire à l'échelle nationale et internationale.

---

[89] Access Now, "Unsafe anywhere: women human rights defenders speak out about Pegasus attacks", 17 janvier 2022 (mis à jour le 8 mai 2023), https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.
[90] Rapport du Haut-Commissariat des Nations unies aux droits de l'homme, *Le droit à la vie privée à l'ère du numérique*, 30 juin 2014, doc. ONU A/HRC/27/37, § 20.
[91] Amnesty International, *Operating from the Shadows: Inside NSO Group's Corporate Structure* (op. cit.), https://www.amnesty.org/en/documents/doc10/4182/2021/en/.
[92] Parlement européen, Enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (recommandation), 15 juin 2023, recommandations 54 et 56, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_FR.pdf.
[93] Conseil des droits de l'homme des Nations unies, Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 28 mai 2019, doc. ONU A/HCR/41/35, § 46, https://undocs.org/A/HRC/41/35.

5.3 OBLIGATIONS DES ÉTATS EN MATIÈRE DE DROITS HUMAINS

En vertu du droit international relatif aux droits humains, les États ont l'obligation de protéger les personnes des atteintes à leurs droits que pourraient commettre des tiers[94]. 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[95].

Or, les révélations de l'enquête sur Predator confirment ce que nous savons depuis longtemps : en ce qui concerne la surveillance, nombreux sont les États qui ne se préoccupent guère de respecter, et *a fortiori* de protéger, les droits humains. Le fait que les États où sont basées les entreprises qui composent l'alliance Intellexa, 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, n'aient pas exercé un réel contrôle sur cette alliance a entraîné des atteintes aux droits humains[96].

5.4 RESPONSABILITÉ DES ENTREPRISES DE RESPECTER LES DROITS HUMAINS

Comme l'indiquent les Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme, les entreprises sont aussi tenues de respecter les droits humains, quel que soit l'endroit dans le monde où elles mènent leurs activités. Ces Principes directeurs indiquent que les entreprises doivent prendre des mesures volontaristes pour faire en sorte de ne pas provoquer d'atteintes aux droits humains ni y contribuer dans le cadre de l'ensemble de leurs activités, et pour y remédier si et quand de telles atteintes se produisent. Pour remplir cette obligation, elles doivent faire preuve de la diligence requise en matière de droits humains pour « identifier leurs incidences sur les droits de l'homme, prévenir ces incidences et en atténuer les effets, et rendre compte de la manière dont elles y remédient ». La responsabilité des entreprises de respecter les droits humains ne se limite pas à leurs propres activités. Par ailleurs, elle existe indépendamment de la capacité ou de la volonté des États de remplir leurs propres obligations en la matière et prévaut sur le respect des lois et règlements nationaux qui protègent les droits fondamentaux[97].

Les entreprises ont aussi l'obligation de rendre des comptes pour les conséquences négatives sur les droits humains de toute leur chaîne de valeur, y compris de l'usage qui est fait de leurs produits et services. Les Principes directeurs de l'ONU précisent que « les entreprises peuvent avoir une part dans les incidences négatives sur les droits de l'homme soit par le biais de leurs propres activités soit par suite de leurs relations commerciales avec d'autres parties » et que l'on entend « par "relations commerciales" les relations avec ses partenaires commerciaux, les entités de sa chaîne de valeur, et toute autre entité non étatique ou étatique directement liée à ses activités, ses produits ou ses services commerciaux[98] ». Dans ce contexte,

---

[94] Comité des droits de l'homme des Nations unies, Observation générale n° 31 [80], La nature de l'obligation juridique générale imposée aux États parties au Pacte, 26 mai 2004, doc. ONU CCPR/C/21/Rev.1/Add.13, § 8.

[95] Les États ont la responsabilité d'assurer une protection contre les atteintes aux droits humains commises par des entreprises privées même en dehors de leurs frontières. Ce principe est bien accepté et directement applicable aux droits bafoués dans les cas révélés par le présent projet. Voir, par exemple, Comité des droits économiques, sociaux et culturels des Nations unies, Observation générale n° 24 sur les obligations des États en vertu du Pacte international relatif aux droits économiques, sociaux et culturels dans le contexte des activités des entreprises, 10 août 2017, doc. ONU E/C.12/GC/24, § 26 ; Comité des droits de l'homme des Nations unies, Observation générale n° 36, Droit à la vie, 3 septembre 2019, doc. ONU CCPR/C/GC/36, § 63 ; Rapport de la rapporteuse spéciale des Nations unies sur les exécutions extrajudiciaires, sommaires ou arbitraires, annexe, Investigation into the unlawful death of Mr. Jamal Khashoggi, 19 juin 2019, doc. ONU A/HRC/41/CRP.1.

[96] Un léger progrès a été réalisé en janvier 2023 : l'Autorité grecque de protection des données a semble-t-il infligé à Intellexa A.E. une amende de 50 000 euros pour violation du Règlement général sur la protection des données [Règlement (UE) 2016/679] au motif que l'entreprise n'avait pas fourni toutes les informations requises. Voir : "Greek Authorities Fine Spyware Firm Owned by Former Israeli Intel Officer", *Haaretz*, 16 janvier 2023, https://www.haaretz.com/israel-news/security-aviation/2023-01-16/ty-article/.premium/greek-authorities-fine-intellexa-chief-over-spyware-scandal/00000185-bab3-deab-ad97-fafbd8ae0000.

[97] Haut-Commissariat des Nations unies aux droits de l'homme, Principes directeurs relatifs aux entreprises et aux droits de l'homme, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_fr.pdf.

[98] Haut-Commissariat des Nations unies aux droits de l'homme, Principes directeurs relatifs aux entreprises et aux droits de l'homme (op. cit.), Principe directeur n° 13, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_fr.pdf.

une entreprise qui vend des équipements de surveillance peut être considérée comme complice des atteintes aux droits humains perpétrées au moyen des équipements qu'elle fournit. Un groupe d'expert·e·s de la Commission internationale de juristes a étudié de manière approfondie la question de la complicité des entreprises dans les atteintes aux droits humains et a clairement établi la responsabilité juridique (civile et pénale) qui pourrait découler d'une telle complicité. Ce groupe a estimé qu'un lien pourrait facilement être établi en droit dans les cas où le comportement de l'entreprise a permis, aggravé ou facilité les atteintes aux droits humains, et si celle-ci savait, ou aurait raisonnablement dû savoir, que de telles atteintes allaient se produire. Une entreprise peut permettre, aggraver ou faciliter des atteintes aux droits humains par la fourniture de biens et de services, entre autres[99].

Les entreprises qui composent l'alliance Intellexa n'ont révélé, de leur propre initiative, aucune information sur leurs pratiques en matière de diligence requise dans le domaine des droits humains. Les évaluations – si toutefois elles existent – des conséquences de leurs technologies de surveillance sur les droits fondamentaux sont tenues secrètes. Amnesty International a écrit à l'alliance Intellexa pour l'inviter à lui faire part de ses commentaires sur les informations fournies dans le présent rapport et lui demander des informations sur ses pratiques en matière de diligence requise, et notamment d'indiquer si elle avait appliqué de façon détaillée le principe de diligence due en matière de droits humains dans chacun des pays utilisateurs finaux auxquels elle vend ses produits. Aucune réponse ne lui était parvenue au moment de la publication de ce rapport[100].

[99] Commission internationale de juristes, *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1er janvier 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

[100] L'EIC a toutefois reçu une réponse d'anciens cadres et actionnaires principaux du groupe Nexa au nom de leurs entreprises, notamment Nexa Technologies et Advanced Middle East Systems. Celles de leurs réponses qui étaient pertinentes par rapport aux questions envoyées par Amnesty International figurent ci-dessus au chapitre 4.1.

6. « UNE ENTREPRISE BASÉE DANS L'UE ET SOUMISE À LA RÉGLEMENTATION EUROPÉENNE »

6.1 INCAPACITÉ DE L'UNION EUROPÉENNE ET DE SES ÉTATS MEMBRES À METTRE UN TERME À L'UTILISATION ABUSIVE DE LOGICIELS ESPIONS

Les dernières révélations dressent un tableau affligeant de l'incapacité de l'Union européenne 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 au sein de l'UE. La campagne de surveillance éhontée décrite dans ce rapport, menée au moyen de produits commercialisés par l'alliance Intellexa, montre les risques et les conséquences très directs de la prolifération des outils de cybersurveillance vendus par des entreprises basées dans l'UE et soumises à la réglementation européenne à des opérateurs de pays tiers, qui les ont ensuite utilisés contre des personnes et des institutions situés dans le monde entier, dont l'Union européenne.

Les révélations de l'enquête sur Predator montrent que des licences d'exportation de technologies de surveillance ont été accordées à des entreprises de l'alliance Intellexa en France[101]. Par ailleurs, la Commission d'enquête du Parlement européen chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (PEGA) note dans son rapport que les autorités grecques ont accordé des licences d'exportation à Intellexa pour la vente de Predator à Madagascar et au Soudan[102]. Il est difficile de savoir si ces États membres ont mené une quelconque évaluation des risques de violation des droits humains avant d'accorder ces licences d'exportation. On ne sait pas non plus si des licences d'exportation

[101] EIC, "Projects", https://eic.network/#projects.
[102] Parlement européen, Enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (recommandation), op. cit., § Q, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_FR.pdf.

ont été demandées et accordées par d'autres États membres de l'UE, ni quelles évaluations ont éventuellement été menées dans le cadre du processus d'attribution de telles licences.

Les révélations sur les « Predator Files » montrent en outre que les mécanismes de contrôle des exportations dans les États membres de l'UE, en particulier en France, ont été contournés et que des exportations ont semble-t-il eu lieu sans l'autorisation des autorités françaises. Elles auraient été effectuées à partir d'une entité de l'alliance Intellexa basée aux Émirats arabes unis, échappant ainsi à la réglementation européenne[103].

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. Le fait que des licences d'exportation aient été accordées malgré un risque substantiel de violations des droits humains par les utilisateurs finaux et que la réglementation européenne sur le contrôle des exportations ait été contournée au moyen de structures opaques et d'entités dans des pays tiers montre clairement que le Règlement européen sur les biens à double usage comporte d'importantes lacunes, qui ont de graves conséquences sur les droits fondamentaux au sein et en dehors de l'UE. Par exemple, dans son rapport annuel, la Commission européenne ne précise pas quels types de produits ont été exportés vers quels pays ni qui a fourni les licences[104]. Elle ne respecte donc pas les exigences de transparence qui sont nécessaires pour une véritable obligation de rendre des comptes en matière de droits humains[105]. Deux ans après la refonte du Règlement sur les biens à double usage, la Commission ne donne toujours aucune indication aux États et aux autorités délivrant les licences d'exportation sur la manière de réaliser une évaluation des risques en matière de droits humains dans le contexte de l'exportation de technologies de cybersurveillance[106].

Si les attaques décrites dans ce rapport ont été peu méthodiques, les préjudices potentiels de la vaste prolifération d'outils de cybersurveillance dans des pays ayant un bilan catastrophique en matière de droits humains et/ou ne disposant pas dans leur législation de garanties suffisantes pour protéger ces droits sont très clairs : non seulement ces outils donnent lieu à des violations des droits humains à l'étranger, mais ils sont aussi une menace pour la sécurité et les droits humains au sein de l'UE, puisqu'il a été constaté qu'ils avaient été utilisés contre des responsables de l'UE eux-mêmes.

6.1.1 ACTION DE L'UE EN MATIÈRE DE RÉGLEMENTATION

À la suite des révélations du projet Pegasus, le Parlement européen a lancé une enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (PEGA). Au bout d'un an d'audiences et d'investigations, la Commission PEGA a adopté un rapport à destination du Conseil et de la Commission de l'Union européenne, dans lequel elle constate de graves violations du droit européen et demande de véritables mesures de l'UE et de ses États membres, à qui elle adresse des recommandations détaillées, mais non contraignantes.

Le rapport de la Commission PEGA dénonce aussi le manque de volonté politique de l'UE et de ses États membres, constatant que « les gouvernements et les parlements des États membres n'ont pas communiqué d'informations utiles au Parlement européen sur les cadres juridiques régissant l'utilisation de logiciels espions au-delà des informations déjà de notoriété publique[107] ». De façon encore plus accablante, il « conclut que ni les États membres, ni le Conseil, ni la Commission ne semblent vouloir tout mettre en œuvre pour faire toute la lumière sur le recours abusif à des logiciels espions, et qu'ils protègent ainsi sciemment des gouvernements de l'Union qui portent atteinte aux droits de l'homme à l'intérieur et à l'extérieur de l'Union[108] ».

---

[103] EIC, "Projects", https://eic.network/#projects.
[104] Commission européenne, Rapport de la Commission au Parlement européen et au Conseil sur l'application du Règlement (UE) 2021/821 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage, 1er septembre 2022, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52022DC0434.
[105] Access Now, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules*, mars 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf.
[106] CIRCABC, 14 juin 2023, https://circabc.europa.eu/ui/group/654251c7-f897-4098-afc3-6eb39477797e/library/e7dc5aae-bce0-4f45-b1e5-bb15b272b66b?p=1&n=10&sort=modified_DESC.
[107] Parlement européen, Enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (recommandation), op. cit., § V, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_FR.pdf.
[108] Parlement européen, Enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (recommandation), op. cit., art. 13, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_FR.pdf.

Comme indiqué plus haut, les mécanismes fondés sur le volontariat, tels que l'Arrangement de Wassenaar et la décision récente de plusieurs États membres de l'UE de s'associer à l'initiative du Sommet de la démocratie[109], sous l'égide des États-Unis, visant à lutter contre l'usage abusif des logiciels espions, ont le mérite d'exister mais restent des engagements non contraignants. Malgré les enquêtes menées dans plusieurs États membres (Hongrie, Espagne et Grèce) après le projet Pegasus et les précédentes révélations sur l'usage de Predator en Grèce, aucun compte n'a été rendu aux victimes de logiciels espions et elles n'ont toujours pas obtenu réparation[110].

Les efforts de réglementation au sein de l'UE restent donc nettement insuffisants ou ne donnent pas lieu à une mise en œuvre satisfaisante. Depuis des années, la société civile alerte sur le fait que les règles européennes de contrôle des exportations de biens à double usage, conçues pour empêcher les atteintes aux droits humains dans le cadre de l'autorisation des exportations de logiciels espions par l'UE (voir ci-dessus le chapitre 6.1), ne sont pas suffisantes pour prévenir les conséquences sur les droits fondamentaux des exportations dans des pays où le risque de violations des droits humains est élevé. Or, malgré les avertissements de la société civile, la refonte du Règlement sur les exportations de biens à double usage adoptée en 2021 demande seulement aux États de « tenir compte » du risque d'atteintes aux droits humains avant d'accorder une licence d'exportation, mais ne leur impose pas de critères en la matière et les laisse libres, au final, d'accorder ou non la licence[111]. Ces lacunes dans la réglementation laissent toute liberté aux États de fermer les yeux sur les risques en matière de droits humains liés à l'exportation de tels outils. La société civile réclame depuis longtemps des garanties relatives aux droits fondamentaux, notamment une plus grande transparence dans la déclaration des exportations, qui devraient faire l'objet d'un rapport annuel présentant des données ventilées par utilisateur final, destination et utilisation prévue, et précisant l'autorité gouvernementale concernée, la valeur de la licence et si la licence a été accordée ou non et pourquoi[112].

6.2 OBLIGATION DE DILIGENCE DES ENTREPRISES EN MATIÈRE DE DROITS HUMAINS

La Commission PEGA a demandé « l'adoption d'une législation européenne supplémentaire imposant aux entreprises qui produisent et/ou exportent des technologies de surveillance d'inclure des cadres relatifs aux droits de l'homme et au devoir de vigilance, conformément aux principes directeurs des Nations unies[113] ». L'Union européenne est en train de négocier une Proposition de directive sur le devoir de vigilance des entreprises en matière de durabilité qui, si elle était adoptée, imposerait aux entreprises d'une certaine taille menant des activités au sein de l'UE, dans tous les secteurs, de faire preuve de la diligence requise en matière de droits humains et d'environnement pour évaluer les risques et les conséquences de leurs activités et de leur chaîne de valeur dans ces domaines et y remédier.

La Proposition de directive sur le devoir de vigilance des entreprises en matière de durabilité est une occasion opportune de commencer à s'attaquer aux préjudices causés par le secteur de la surveillance. Toutefois, 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. Par exemple, elle risque de ne s'appliquer qu'aux très grandes sociétés, ce qui pourrait exclure de son champ d'application un certain nombre de compagnies, dont des sociétés de l'alliance Intellexa.

En outre, le Parlement européen et le Conseil de l'Union européenne ont proposé que, aux termes de la directive, les entreprises n'aient pas à évaluer les utilisations abusives potentielles de leurs produits ou

[109] Département d'État des États-Unis, "Guiding Principles on Government Use of Surveillance Technologies" (op. cit.), https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/.
[110] En décembre 2022, le Parlement grec a adopté une loi controversée qui ne prévoyait pas des garanties suffisantes pour les personnes placées sous surveillance et légalisait l'utilisation de la technologie des logiciels espions par les autorités. Voir : Amnesty International, « Grèce. Le scandale de la surveillance doit tous nous sortir de notre complaisance », 26 janvier 2023, https://www.amnesty.org/fr/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/.
[111] Union européenne, Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte), 11 juin 2021, PE/54/2020/REV/2, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021R0821.
[112] Access Now, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules*, mars 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf.
[113] Parlement européen, Enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (recommandation), op. cit., recommandation 66, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_FR.pdf.

services lors de l'exercice de leur diligence requise en matière de droits humains et d'environnement[114]. Le Conseil de l'Union européenne a aussi tenté d'introduire une exception pour les entreprises qui fabriquent des produits soumis aux contrôles à l'exportation, ce qui inclurait les technologies de surveillance.

[114] Pour lire l'analyse réalisée par Amnesty International de la Proposition de directive sur le devoir de vigilance des entreprises en matière de durabilité, voir Amnesty International, *Des lacunes à combler. Directive européenne sur le devoir de diligence des entreprises en matière de durabilité : recommandations pour une loi efficace pour les détenteurs et détentrices de droits* (index : IOR 60/6539/2023), 15 mai 2023, https://www.amnesty.org/fr/documents/ior60/6539/2023/fr/.

7. RECOMMANDATIONS

À L'UNION EUROPÉENNE ET À SES ÉTATS MEMBRES

Recommandations d'action au sein de l'Union européenne

- Tous les États membres de l'UE qui ont accordé des licences d'exportation à l'alliance Intellexa doivent annuler immédiatement ces licences et mener une enquête indépendante, impartiale et transparente pour déterminer l'ampleur des attaques illégales ayant pu être commises, 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.
- Les États membres de l'UE doivent interdire les logiciels espions hautement intrusifs, dont les fonctionnalités ne peuvent pas être limitées à ce qui est nécessaire et proportionnel à un usage et un objectif spécifiques, ou qui ne peuvent pas faire l'objet d'un contrôle indépendant.
- Les États membres de l'UE doivent 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 autres logiciels espions.
- Les États membres de l'UE doivent veiller à ce que les victimes de surveillance ciblée illégale reçoivent véritablement réparation et à ce que les responsables aient à rendre compte des violations commises. Ils doivent également s'engager à réformer les lois existantes qui font obstacle à l'octroi de réparations à ces victimes et faire en sorte que des voies de recours judiciaires et non judiciaires soient concrètement disponibles.
- 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. Les entreprises doivent avoir l'obligation d'identifier, d'empêcher et d'atténuer toutes les répercussions négatives potentielles ou réelles de leurs activités et de l'ensemble de leur chaîne de valeur sur les droits fondamentaux. Par conséquent, 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 ;
    - veiller à ce que les dispositions de cette directive s'appliquent aux entreprises de tous les secteurs, y compris aux fabricants de logiciels espions, ainsi qu'aux institutions financières.
- Les États membres de l'UE doivent adopter et mettre en œuvre une législation nationale qui offre des garanties contre les atteintes aux droits humains causées par la surveillance numérique illégale. Cette législation devra être conforme à l'arrêt de 2015 de la Cour européenne des droits de l'homme dans l'affaire *Roman Zakahrov c. Russie*, et respecter les principes de nécessité et de proportionnalité.
- Les États membres de l'UE et la Commission européenne doivent veiller à ce que la réglementation européenne sur le contrôle des exportations entrée en vigueur le 9 septembre 2021 avec la refonte du Règlement sur les biens à double usage soit fermement appliquée, ce qui implique de prendre des mesures immédiates pour insister sur les obligations de diligence relative aux droits fondamentaux qui

découlent de ce Règlement et pour créer un marché transparent des technologies de surveillance, soumis à des garanties efficaces en matière de droits humains :

  - Le Règlement sur les biens à double usage prévoit que la Commission doit présenter chaque année un rapport public au Parlement et au Conseil. Ce rapport doit au minimum contenir des informations indiquant le nombre de demandes de licences d'exportation par produit, le nom de la société exportatrice, une description de l'utilisateur final, la destination du produit et son utilisation prévue, l'autorité gouvernementale concernée, la valeur de la licence et si la licence a été accordée ou non et pourquoi.
  - Les mesures de contrôle des transactions prises par les États membres doivent comprendre une évaluation du caractère stratégique des produits et des risques de violation des droits humains qu'ils présentent. Les autorités nationales doivent rendre compte de la façon dont les responsabilités et les obligations de diligence sont appliquées et encourager les entreprises à informer le grand public de l'ampleur, de la nature et des conclusions des procédures de diligence requise qu'elles ont mises en œuvre.
  - Les États membres doivent veiller à ce que les pays exportateurs mettent en place des mécanismes offrant un recours effectif pour les violations des droits humains commises à l'aide des technologies transférées. Les orientations qui seront publiées conformément à l'article 26(1) du Règlement 2021/821/EU sur les biens à double usage devront détailler ce qui est attendu des pays exportateurs en termes de programmes de conformité internes et de diligence requise en vertu de ce Règlement, sur la base des Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme et des Principes directeurs de l'Organisation de coopération et de développement économiques (OCDE) à l'intention des entreprises multinationales.
  - La Commission européenne doit immédiatement mener une enquête sur toutes les licences d'exportation accordées par l'UE et ses États membres, y compris sur l'autorisation générale d'exportation de l'Union européenne EU005, qui couvre notamment les logiciels destinés aux équipements de surveillance et d'interception, et veiller à ce que les États membres annulent toutes les autorisations de commercialisation et d'exportation dès lors qu'il existe un risque important que les technologies en question contribuent à des violations des droits humains. Si les pratiques d'un État membre en matière d'attribution des licences d'exportation s'avèrent être contraires aux normes réglementant les exportations, la Commission européenne doit engager une procédure d'infraction.

- Les États membres de l'UE doivent agir fermement pour mettre un terme à la répression transnationale des défenseur·e·s des droits humains et des journalistes au sein de l'UE, en veillant à ce que tout instrument européen sur les défenseur·e·s des droits humains contienne des engagements à lutter contre la répression transnationale de ces personnes, notamment contre la surveillance ciblée illégale.

Recommandations d'action par le biais des instruments de politique étrangère

Compte tenu de leur ambition d'être un modèle mondial en matière de droits humains, l'UE et ses États membres peuvent et doivent jouer un rôle dans la protection des droits fondamentaux et du respect de l'état de droit dans le domaine numérique sur leur territoire et à l'étranger. Cela découle des obligations de l'UE et de ses États membres de protéger et de défendre les droits humains partout dans le monde, comme stipulé à l'article 21 du Traité de Lisbonne. C'est aussi conforme aux engagements de l'UE figurant dans les Conclusions du Conseil intitulées « Façonner l'avenir numérique de l'Europe », dans le Plan d'action de l'UE en faveur des droits de l'homme et de la démocratie et dans les orientations de l'UE relatives aux droits humains. Les dirigeant·e·s de l'Union européenne, notamment la présidente de la Commission Ursula Von Der Leyen et le haut-représentant Josep Borrell, ont déjà souligné l'importance de protéger la société civile et de défendre le droit au respect de la vie privée et la liberté d'expression en ligne à l'ère numérique.

- L'UE et ses États membres doivent énoncer clairement leur position sur la surveillance ciblée illégale, et notamment, par le biais de déclarations officielles :
  - exprimer leur préoccupation à propos des attaques visant des journalistes, des militant·e·s et des personnalités politiques, en soulignant que de telles pratiques sont inacceptables et violent les droits à la liberté d'expression, à la liberté de réunion pacifique et au respect de la vie privée ;
  - insister sur la nécessité d'améliorer de toute urgence la transparence et la responsabilité juridique du secteur de la surveillance au vu du nombre croissant d'attaques numériques et de cas de surveillance ciblée de défenseur·e·s des droits humains, de journalistes et de membres de la société civile par des gouvernements qui cherchent à réduire au silence et à intimider ces acteurs partout dans le monde ;

- appeler les États à prendre des mesures urgentes pour mieux réglementer le secteur de la cybersurveillance, garantir l'obligation de rendre des comptes pour les violations des droits humains liées à ce secteur et renforcer la supervision de ce secteur mal réglementé.

- L'Union européenne et ses États membres doivent engager des démarches bilatérales en direction des autorités concernées au Viêt-Nam.
- L'Union européenne et ses États membres doivent demander des éclaircissements aux autorités vietnamiennes et, notamment :
  - appeler les autorités concernées à mener immédiatement une enquête indépendante, transparente et impartiale sur tout cas de surveillance illégale et, si c'est approprié, à engager des démarches judiciaires pour offrir réparation aux victimes et demander des comptes aux responsables, conformément aux normes internationales relatives aux droits humains ;
  - souligner que l'utilisation de logiciels espions à des fins de surveillance n'est légale que sous certaines conditions très strictes, définies par le droit international relatif aux droits humains, et que ce type de surveillance doit être légale, nécessaire, proportionnelle et limitée dans le temps ;
  - engager les autorités vietnamiennes à respecter leurs obligations et leurs engagements aux termes du droit international relatif aux droits humains, notamment ceux qui sont inscrits dans le Pacte international relatif aux droits civils et politiques (PIDCP) et dans la Déclaration des Nations unies sur les défenseurs des droits de l'homme ;
  - évoquer auprès des autorités au plus haut niveau les cas des défenseur·e·s des droits humains, journalistes et militant·e·s qui ont été pris pour cible au Viêt-Nam et dans les États membres de l'UE et offrir une aide politique, technique ou autre à ces personnes, conformément aux Orientations de l'Union européenne concernant les défenseurs des droits de l'homme, aux Orientations de l'UE relatives à la liberté d'expression en ligne et hors ligne, et au Plan d'action de l'UE en faveur des droits de l'homme et de la démocratie ;
  - appeler le gouvernement vietnamien à mettre un terme à la surveillance ciblée illégale des défenseur·e·s des droits humains et des militant·e·s vietnamiens à l'étranger, notamment dans les États membres de l'UE, et lui faire clairement savoir que ce type de répression transnationale est inacceptable.
- Les États membres de l'UE doivent demander aux pays tiers exportateurs d'annuler immédiatement toutes les autorisations de commercialisation et d'exportation accordées à l'alliance Intellexa et de mener une enquête indépendante, impartiale et transparente pour déterminer l'ampleur de la surveillance numérique illégale réalisée au moyen des outils d'Intellexa. Ces pays doivent notamment procéder à une évaluation complète, suivie d'une réforme, du système d'autorisation des exportations afin qu'il soit adapté en droit et en pratique, et qu'il empêche de futures atteintes aux droits humains liées à l'exportation d'équipements de surveillance depuis leur territoire. Une fois l'évaluation terminée, ses résultats doivent être présentés publiquement et des mesures doivent être prises pour empêcher d'autres atteintes à l'avenir.
- Conformément aux Conclusions du Conseil du 20 février 2023 sur les priorités de l'UE dans les enceintes des Nations unies compétentes en matière de droits de l'homme, l'UE et ses États membres doivent participer aux principales initiatives, notamment au niveau du Conseil des droits de l'homme des Nations unies, de l'Assemblée générale des Nations unies et lors des cycles de l'examen périodique universel, visant à élaborer des normes solides relatives aux droits humains pour régir le développement, la vente, le transfert et l'utilisation des équipements de surveillance, et à déterminer quelles sont les cibles inacceptables de la surveillance numérique. Cela implique également de soutenir l'appel à l'interdiction de l'utilisation des logiciels espions hautement intrusifs.

LE GOUVERNEMENT VIETNAMIEN DOIT :

- s'engager publiquement à mettre immédiatement un terme à l'utilisation de logiciels espions pour attaquer illégalement des défenseur·e·s des droits humains, des membres de la société civile et des journalistes au Viêt-Nam comme à l'étranger ;
- 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 ;

- mettre en œuvre un cadre réglementaire de protection des droits humains régissant les activités de surveillance 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 ;
- abroger ou réviser les articles 117, 118 et 331 du Code pénal de 2015, qui restreignent abusivement l'exercice des droits à la liberté d'expression, de réunion pacifique et d'association, afin de les mettre en conformité avec le droit international relatif aux droits humains ;
- réviser et modifier la Loi relative à la cybersécurité pour la mettre en conformité avec les normes internationales en matière de droits humains, et en particulier :
    - abroger ou modifier ses articles 8, 16, 17 et 26 afin qu'ils soient conformes aux normes internationales relatives aux droits humains régissant la liberté d'expression,
    - y ajouter des garanties spécifiques visant à empêcher son application arbitraire et discriminatoire,
    - en supprimer toutes les dispositions qui imposeraient aux fournisseurs d'accès à Internet ou aux entreprises technologiques de révéler des données personnelles sans garanties suffisantes pour empêcher les abus ;
- abroger ou modifier les articles 99, 100 et 101 du Décret 15/2020/ND-CP afin de les mettre en conformité avec les normes internationales relatives aux droits humains régissant la liberté d'expression et le droit au respect de la vie privée ;
- abroger ou modifier les articles 5, 22 et 25 du Décret 72/2013/ND-CP afin de les mettre en conformité avec les normes internationales relatives aux droits humains régissant la liberté d'expression et le droit au respect de la vie privée, et ne pas procéder aux modifications de ce décret qui sont actuellement proposées, notamment les modifications de son article 23.d.

TOUS LES ÉTATS DOIVENT :

- interdire les logiciels espions hautement intrusifs, dont les fonctionnalités ne peuvent pas être limitées à ce qui est nécessaire et proportionnel à un usage et un objectif spécifiques, ou qui ne peuvent pas faire l'objet d'un contrôle indépendant ;
- mettre en œuvre 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 ;
- 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, y compris en ce qui concerne l'utilisation de leurs produits et services ;
- adopter et mettre en application un cadre juridique exigeant la transparence des sociétés privées de surveillance, avec notamment l'obligation de fournir des informations sur leur identification et leur enregistrement, sur les produits et services qu'elles proposent et sur leurs ventes ;
- rendre publiques les informations relatives aux contrats qui ont été, sont ou seront passés avec des sociétés privées de surveillance, soit en répondant aux demandes d'informations, soit de leur propre initiative ;
- En cas de levée du moratoire sur la vente et le transfert de logiciels espions, les États devront en outre, au minimum, suivre les recommandations suivantes :
    - appliquer une législation nationale qui apporte une protection contre les atteintes aux droits humains causées par la surveillance numérique et qui crée des mécanismes d'obligation de rendre des comptes destinés à offrir une voie de recours aux victimes de surveillance abusive ;
    - réformer les lois existantes qui font obstacle à l'octroi de réparations aux victimes de surveillance illégale et veiller à ce que des voies de recours judiciaires et non judiciaires soient disponibles dans la pratique ;
    - appliquer des normes d'achat qui limitent les contrats gouvernementaux relatifs aux technologies et services de surveillance aux seules entreprises qui sont en mesure de prouver

qu'elles respectent les droits humains conformément aux Principes directeurs de l'ONU et qu'elles ne vendent pas à des clients qui utilisent la surveillance de façon abusive ;

- réglementer l'exportation des technologies de surveillance, et notamment :
  - veiller à ce que les autorisations d'exportation ne soient pas accordées dès lors qu'il existe un risque substantiel que le produit en question soit utilisé pour porter atteinte aux droits humains ou si le pays de destination ne dispose pas de garanties juridiques, procédurales et techniques suffisantes pour prévenir les atteintes aux droits humains,
  - mettre à jour leurs critères de contrôle des exportations afin de prendre en compte le bilan de l'utilisateur final en matière de droits humains ainsi que la légalité de l'utilisation d'outils de surveillance perfectionnés dans le pays de destination, en stipulant que les demandes qui posent un risque substantiel pour les droits humains doivent être rejetées,
  - veiller à ce que, dans le cadre du processus d'examen des demandes de licences, toutes les technologies concernées fassent l'objet d'une vérification approfondie visant à déterminer les risques en matière de droits humains avant leur transfert,
  - garantir la transparence au sujet du volume, de la nature, de la valeur, de la destination et du pays de l'utilisateur final des transferts de technologies de surveillance, par exemple en publiant des rapports annuels sur les importations et les exportations de telles technologies,
  - modifier toutes les lois existantes qui imposent des restrictions excessives sur la divulgation de telles informations,
  - faire en sorte que les outils de chiffrement et les recherches légitimes en matière de sécurité ne soient pas soumis à des contrôles à l'exportation ;

- participer aux principales initiatives multilatérales visant à élaborer des normes solides relatives aux droits humains pour régir le développement, la vente, le transfert et l'utilisation des équipements de surveillance, et à déterminer quelles sont les cibles inacceptables de la surveillance numérique ;
- mettre en place des comités publics de supervision chargés de surveiller et de valider l'achat ou l'utilisation de nouvelles technologies de surveillance, qui aient le pouvoir d'approuver ou de rejeter les projets en fonction des obligations des États en matière de droits humains, des dispositions relatives à l'information du public et des rapports à établir.

L'ALLIANCE INTELLEXA DOIT, AU MINIMUM :

- 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 ;
- mettre immédiatement un terme à l'utilisation, l'assistance à l'utilisation et la vente de ses technologies dans des pays où des logiciels de cybersurveillance ont été utilisés de manière abusive pour attaquer illégalement des défenseur·e·s des droits humains, des journalistes et des membres de la société civile ;
- offrir une indemnisation satisfaisante ou d'autres formes de réparation effective aux victimes de surveillance illégale ;
- prendre de toute urgence des mesures volontaristes pour faire en sorte de ne pas provoquer ni favoriser des atteintes aux droits humains, et pour y remédier quand elles se produisent. Pour s'acquitter de cette responsabilité, l'alliance Intellexa doit faire preuve de la diligence requise concernant les droits humains, conformément aux normes internationales relatives à la responsabilité des entreprises en matière de droits humains, et faire le nécessaire pour que les défenseur·e·s des droits humains, les journalistes et les membres de la société civile ne soient plus la cible d'une surveillance illégale menée au moyen des technologies qu'elle propose ;
- faire preuve de transparence en ce qui concerne le volume, la nature, la valeur, la destination et l'utilisateur final de ses transferts de technologies de surveillance.

8. ANNEXES

ANNEXE I – INDICATEURS DE COMPROMISSION

Domaines du logiciel espion Predator d'Intellexa liés à cette campagne

La première infrastructure de Predator utilisée dans cette campagne a été enregistrée en juillet 2022. De précédents domaines de Predator utilisant des thèmes vietnamiens ont été observés pour la première fois en mars 2022. Une nouvelle infrastructure de Predator associée aux domaines d'attaque utilisés dans cette campagne était toujours active en septembre 2023.

NOM DE DOMAINE	PREMIÈRE DÉTECTION
ietnamnews[.]com	23 mars 2022
lnktonews[.]co	19 juillet 2022
witteridea[.]co	19 juillet 2022
caavn[.]org	5 août 2022
xuatnhapcanhvn[.]info	5 août 2022
tokhaiytehanoi[.]org	5 août 2022
southchinapost[.]net	2 mai 2023
scanningandinfo[.]online	9 mai 2023
asean-news[.]net	9 mai 2023
southchinapost[.]net	8 juin 2023
asean-news[.]co	8 juin 2023
scanningandinfo[.]co	8 juin 2023
newsworldsports[.]co	13 juillet 2023

Tableau 7 : domaines du logiciel espion Predator d'Intellexa liés à cette campagne

Comptes X (Twitter) liés à cette campagne

COMPTE	PREMIÈRE DÉTECTION	DERNIÈRE ACTIVITÉ CONSTATÉE
Joseph_Gordon	1er octobre 2019	Début juin 2023
AlexMarcos71	4 avril 2023	16 mai 2023

Tableau 8 : comptes X (Twitter) liés à cette campagne

Comptes Facebook liés à cette campagne

COMPTE	NOM DU TITULAIRE DU COMPTE	PREMIÈRE DÉTECTION	DERNIÈRE ACTIVITÉ CONSTATÉE
https://www.facebook.com/profile.php?id=100090236330335	Ahn Tran	10 février 2023	23 mars 2023

Tableau 9 : comptes Facebook liés à cette campagne

ANNEXE II – TWEETS

Cette annexe recense toutes les publications du compte @Joseph_Gordon observées sur les réseaux sociaux qui contenaient des liens d'attaque.

DATE	DESTINATAIRE	URL	PLATEFORME
12 avril 2023	@CollinSLKoh	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12 avril 2023	@CollinSLKoh	https://lnktonews[.]co/ODFwNI	X
17 mai 2023	@CollinSLKoh	https://southchinapost[.]net/WzMqB	X

Tableau 10 : tweets envoyés à des cibles liées à Singapour

DATE	DESTINATAIRE	URL	PLATEFORME
9 février 2023	@thoibao_de	https://lnktonews[.]co/MEmK	X

Tableau 11 : tweets envoyés à des cibles liées à l'Allemagne

DATE	DESTINATAIRE	URL	PLATEFORME
12 avril 2023	@FMangosingINQ	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12 avril 2023	@FMangosingINQ	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@FMangosingINQ	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
23 mai 2023	@FMangosingINQ	https://southchinapost[.]net/RtQBG	X

Tableau 12 : tweets envoyés à des cibles liées aux Philippines

DATE	DESTINATAIRE	URL	PLATEFORME
10 avril 2023	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12 avril 2023	@PdChina	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
26 mai 2023	@PDChinese	https://southchinapost[.]net/faePtONi	X
14 avril 2023	@SpotlightonCN	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tableau 13 : tweets envoyés à des cibles liées à la Chine

DATE	DESTINATAIRE	URL	PLATEFORME
10 avril 2023	@Duandang	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tableau 14 : tweets envoyés à des cibles liées au Viêt-Nam

DATE	DESTINATAIRE	URL	PLATEFORME
14 avril 2023	@jojjeols	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tableau 15 : tweets envoyés à des cibles liées à la Suède

DATE	DESTINATAIRE	URL	PLATEFORME
10 avril 2023	@willripleyCNN @CNN @jimsciutto @EricCheungw	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
12 avril 2023	@GMFAsia	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X

Tableau 16 : tweets envoyés à des cibles liées aux États-Unis

DATE	DESTINATAIRE	URL	PLATEFORME
12 avril 2023	@Indopac_INFO	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12 avril 2023	@Indopac_INFO	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@Indopac_INFO	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
14 avril 2023	@Indopac_INFO	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
17 mai 2023	@Indopac_INFO	https://southchinapost[.]net/WzMqB	X
22 mai 2023	@IMOSINT	https://southchinapost[.]net/fLwoASy	X
12 avril 2023	@ItsTheEnforcer	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X

Tableau 17 : tweets envoyés à des comptes liés au renseignement obtenu à partir d'informations disponibles en libre accès

DATE	DESTINATAIRE	URL	PLATEFORME
12 avril 2023	@Manu_FAO	https://witteridea[.]co/LFJeZQu	X
16 mai 2023	@HugBallesteros	https://asean-news[.]net/HpjXXwRU	X

Tableau 18 : tweets envoyés à des autorités et des chercheurs·euses du secteur des affaires maritimes et de la pêche

DATE	DESTINATAIRE	URL	PLATEFORME
8 mars 2023	@SariArhoHavren	https://Inktonews[.]co/CVqp	X
14 mars 2023	@SariArhoHavren	https://witteridea[.]co/mBxp	X
21 mai 2023	@ElBridgeColby	https://southchinapost[.]net/fLwoASy	X
12 avril 2023	@AsiaMTI	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@AsiaMTI @cnnphilippines	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@AsiaMTI	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
17 mai 2023	@GordianKnotRay	https://southchinapost[.]net/WzMqB	X

Tableau 19 : tweets envoyés à groupes de réflexion et des chercheurs·euses

DATE	DESTINATAIRE	URL	PLATEFORME
8 février 2023	@vitcheva_eu @EMODnet @cinea_eu @Pierre_Ka @EUgreenresearch @CMEMS_EU @FSUMDC @UNDPOceanInnov @REA_research @EU_ENV @EUClimateAction @eumissionocean	https://witteridea[.]co/LFJeZQu	X
8 février 2023	@vitcheva_eu	https://witteridea[.]co/LFJeZQu	X
8 mars 2023	@GermanAmbUSA	https://Inktonews[.]co/CVgp	X
1er juin 2023	@EP_President	https://southchinapost[.]net/VuAfn	X
1er juin 2023	@EU_Commission	https://southchinapost[.]net/VuAfn	X
1er juin 2023	@EU_Commission	https://southchinapost[.]net/VuAfn	X
1er juin 2023	@eumissionocean	https://southchinapost[.]net/VuAfn	X

Tableau 20 : tweets envoyés à des responsables et institutions européens

DATE	DESTINATAIRE	URL	PLATEFORME
14 avril 2023	@iingwen @SenJohnHoeven	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14 avril 2023	@MofaTaiwan @RepMcCaul	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
22 mai 2023	@iingwen	https://southchinapost[.]net/RtQBG	X

Tableau 21 : tweets envoyés à de hauts responsables et des institutions américains et taiwanais

DATE	DESTINATAIRE	URL	PLATEFORME
1er juin 2023	@erionveliaj	https://southchinapost[.]net/eNISDKnI	X
1er juin 2023	@AlMissionEU @AlbanianDiplo	https://southchinapost[.]net/eNISDKnI	X
1er juin 2023	@AlMissionUNGen @AlbanianDiplo @AlEmbDenmark @AlMissionUN @AlMissionVienna	https://southchinapost[.]net/eNISDKnI	X
1er juin 2023	@MirelaKumbaro	https://southchinapost[.]net/eNISDKnI	X
1er juin 2023	@GjonajEtilda @ChrisMurphyCT @GaryPeters	https://southchinapost[.]net/eNISDKnI	X
1er juin 2023	@MonicaMerino_D @AlbGob @MirelaKumbaro	https://southchinapost[.]net/eNISDKnI	X

Tableau 22 : tweets envoyés à des responsables et institutions albanais

DATE	DESTINATAIRE	URL	PLATEFORME
10 avril 2023	@AnarchoTerran	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
10 avril 2023	@MarioNawfal	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tableau 23 : autres liens Predator envoyés à des comptes X

ANNEXE III – AUTRES LIENS PREDATOR PARTAGÉS SUR LES RÉSEAUX SOCIAUX

DATE	DESTINATAIRE	URL	PLATEFORME
23 mars 2023	« Liën Minh Dân Chù »	http://caavn[.]org/tin-tuc/chien-su-ukraine	Facebook
23 mars 2023	« Liën Minh Dân Chù »	http://caavn[.]org/tin-tuc/quan-he-my-trung-sau-no-khi-cau	Facebook

Tableau 24 : liens visant une organisation politique vietnamienne basée aux États-Unis

ANNEXE IV – ANALYSE DE COMPTES DE RÉSEAUX SOCIAUX LIÉS À L'ATTAQUANT PRÉSUMÉ

Amnesty International a analysé d'autres comptes qui étaient suivis par le compte de l'attaquant @Joseph_Gordon16 ou qui le suivaient. Parmi les comptes X suivis par @Joseph_Gordon16 figurent de nombreux comptes pris pour cible qui ont par la suite reçu des liens d'attaques de Predator.

Sur le petit nombre de comptes qui suivaient @Joseph_Gordon16, beaucoup s'intéressaient semble-t-il à des sujets liés au Viêt-Nam et à la cybersécurité. Un certain nombre d'entre eux avaient des photos de profil copiées sur celle d'un éminent homme d'affaires vietnamien. Certains de ces comptes pourraient être des avatars supplémentaires liés à l'opérateur se trouvant derrière cette campagne ou contrôlés par lui.

Parmi les comptes qui suivaient @Joseph_Gordon16 figure le compte X @bisngoo27345032, avec pour nom de profil Bí Ngô, qui veut dire « citrouille » en vietnamien. Ce compte suivait de nombreux chercheurs·euses vietnamiens travaillant dans le domaine de la sécurité, ainsi que des entreprises de cybersécurité basées au Viêt-Nam. Ce compte semble avoir un intérêt particulier pour la cybersécurité et les nouvelles techniques d'attaque.

Un autre compte qui suivait @Joseph_Gordon16 est @AlexMarcos71. Ce compte affirme être basé aux Philippines mais suit de nombreux comptes vietnamiens et publie des tweets en vietnamien.

Figure 23 : profil du compte @AlexMarcos71 lié à l'attaquant

Les comptes X @AlexMarcos71 et @Joseph_Gordon16 ont tous deux envoyé des tweets à un universitaire basé dans l'UE qui mène des recherches sur la pêche illégale, avec des commentaires au sujet du « carton jaune » reçu par le Viêt-Nam de la part de l'Union européenne. Le tweet de @Joseph_Gordon16 comprenait un lien vers le logiciel espion Predator.

Le compte @AlexMarcos71 a aussi tweeté au sujet du système de « carton jaune » (voir figure 24) et a envoyé un message de réponse mentionnant l'universitaire de l'UE visé par une attaque de @Joseph_Gordon16 (voir figure 25). La coordination entre ces deux comptes laisse à penser qu'ils sont tous les deux contrôlés ou gérés par l'opérateur qui est derrière cette campagne d'attaque.

Figure 24 : tweet en espagnol du compte @AlexMarcos71 à propos du système de « carton jaune »

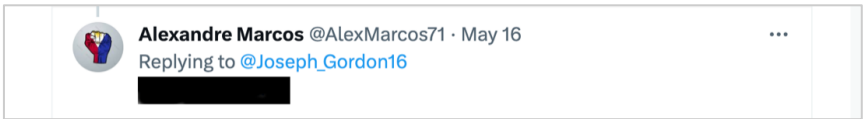


Figure 25: tweet de réponse envoyé par @AlexMarcos71 mentionnant l'universitaire espagnol visé

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