



Les vétérans du Mossad à la tête de NSO, Pegasus et Silicone Valley, investissent la région maghrébine : Les technologies israéliennes impactent le quotidien

Par [Jonathan Cook](#)

Mondialisation.ca, 13 juillet 2022

[lexpressquotidien.dz](#) 6 juillet 2022

Région : [Moyen-Orient et Afrique du Nord](#)

Thème: [Services de renseignements](#)

Comme on le sait, la question du Sahara occidental a été au cœur de l'espionnage par le Maroc via le logiciel Pegasus de tout le voisinage, y compris la France. Dans la proche périphérie de l'Algérie, au sud, dans la région saharo-sahélienne, IAI, Israël Shipyards, Mer Group et toute l'industrie militaire israélienne tentent de s'implanter.

Le monde des logiciels israéliens exploités contre les Palestiniens produit de nouvelles armes cybernétiques qui sont rapidement intégrées aux plateformes numériques à l'échelle mondiale.

Les armes de l'ère numérique développées par Israël pour opprimer les Palestiniens sont rapidement réutilisées pour des applications beaucoup plus larges, contre les populations occidentales qui ont longtemps considéré leurs libertés pour acquises.

Le statut d'Israël en tant que « nation startup » a été établi il y a plusieurs décennies. Mais sa réputation d'innovation en haute technologie a toujours reposé sur une face obscure, de plus en plus difficile à ignorer.

Il y a quelques années, le critique israélien Jeff Halper a averti qu'Israël avait joué un rôle central dans la fusion des nouvelles technologies numériques avec l'industrie de la sécurité intérieure. Le danger était que nous devenions tous progressivement des Palestiniens.

Israël, a-t-il noté, a traité efficacement – comme des cobayes dans des laboratoires à ciel ouvert – les millions de Palestiniens soumis à son régime militaire. Ils ont servi de banc d'essai pour mettre au point non seulement de nouveaux systèmes d'armes classiques, mais également de nouveaux outils de surveillance et de contrôle de masse.

Comme l'a récemment signalé un rapport publié sur Haaretz, l'opération de surveillance menée par Israël contre les Palestiniens est « parmi les plus vastes du genre au monde. Cela inclut la surveillance des médias, des médias sociaux et de la population dans son ensemble ».

Commercialiser Big Brother

Mais ce qui a commencé dans les territoires occupés ne va jamais rester confiné en

Cisjordanie, à Jérusalem-Est et à Gaza. Il y avait tout simplement trop d'argent et d'influence à gagner d'un commerce de ces nouvelles formes hybrides de technologie numérique agressive.

Aussi petit soit-il, Israël est depuis longtemps un chef de file mondial dans un commerce [trafic] d'armes extrêmement lucratif, vendant à des régimes autoritaires du monde entier ses systèmes d'armes testés sur le champ de bataille des Palestiniens.

Ce commerce de matériel militaire est de plus en plus éclipsé par un marché de logiciels agressifs : des outils pour mener une guerre cybernétique.

Ces armes de nouvelle génération sont très demandées par les États, non seulement contre les ennemis extérieurs, mais aussi contre des citoyens et des militants des droits de l'homme considérés comme dissidents.

Israël peut légitimement prétendre être une autorité mondiale en la matière, contrôlant et opprimant les populations placées sous son autorité militaire. Mais il a tenu à marquer ses empreintes digitales sur une grande partie de cette nouvelle technologie à la « Big Brother », en externalisant le développement de ces outils informatiques au profit de diplômés de ses infâmes unités de sécurité et de renseignement militaire.

Néanmoins, Israël valide implicitement ces activités en fournissant des licences d'exportation à ces entreprises – et les plus hauts responsables de la sécurité du pays sont souvent étroitement associés à leurs travaux.

Tensions avec la Silicon Valley

Une fois abandonné l'uniforme, les Israéliens peuvent tirer profit des années d'expérience acquises grâce à l'espionnage des Palestiniens en créant des sociétés développant des logiciels similaires pour des applications à plus grande échelle.

Les applications utilisant une technologie de surveillance sophistiquée d'origine israélienne sont de plus en plus courantes dans nos vies quotidiennes et numériques. Certaines ont été utilisées pour des usages relativement [et prétendument] bénins. Waze, qui surveille la congestion du trafic, permet aux conducteurs d'atteindre les destinations plus rapidement, tandis que Gett met les clients en liaison avec les taxis à proximité via leur téléphone.

Mais certaines des technologies les plus secrètes produites par les développeurs israéliens restent beaucoup plus proches de leur objectif militaire initial.

Ce logiciel agressif est vendu à la fois aux pays qui souhaitent espionner leurs propres citoyens ou des États rivaux, et à des sociétés privées qui espèrent gagner un avantage sur leurs concurrents ou mieux exploiter et manipuler commercialement leurs clients.

Une fois intégrés aux plateformes de médias sociaux comptant des milliards d'utilisateurs, ces logiciels espions offrent aux agences de sécurité des États une portée potentielle quasi mondiale. Cela explique la relation parfois difficile entre les sociétés de technologie israéliennes et la Silicon Valley, cette dernière luttant pour prendre le contrôle de ce malware [ensemble des logiciels sur le réseau considérés comme nocifs] – comme le montrent deux exemples récents et assez contrastés.

« Kit d'espionnage » pour téléphone portable

Signe des tensions, WhatsApp, une plate-forme de médias sociaux appartenant à Facebook, a engagé la semaine dernière un premier recours de ce type devant un tribunal californien contre NSO, la plus grande société de surveillance israélienne.

WhatsApp accuse NSO de cyberattaques. Au cours d'une courte période de deux semaines se terminant début mai et scrutée par WhatsApp, NSO aurait sponné les téléphones mobiles de plus de 1400 utilisateurs dans 20 pays.

Le logiciel espion de la NSO, appelé Pegasus, a été utilisé contre des défenseurs des droits de l'homme, des avocats, des responsables religieux, des journalistes et des travailleurs humanitaires. Reuters a révélé la semaine dernière que de hauts responsables de pays alliés des États-Unis avaient également été pris pour cibles par la NSO.

Après avoir pris le contrôle du téléphone de l'utilisateur à son insu, Pegasus copie les données et active le microphone pour enregistrer les conversations. Le magazine Forbes l'a décrit comme « le kit d'espionnage mobile le plus intrusif au monde ».

La NSO a octroyé une licence d'utilisation de ce logiciel à des dizaines de gouvernements, notamment à des régimes réputés pour violer les droits de l'homme, tels que l'Arabie Saoudite, Bahreïn, les Émirats arabes unis, le Kazakhstan, le Mexique et le Maroc.

Amnesty International s'est plaint de ce que son personnel figure parmi les personnes visées par les logiciels espions de la NSO. Il soutient actuellement une action en justice contre le gouvernement israélien pour avoir délivré une licence d'exportation à cette même société.

Liens avec les services du renseignement israélien

NSO a été fondée en 2010 par Omri Lavie et Shalev Hulio, tous deux censés être des diplômés de la fameuse unité de renseignement militaire 8200 d'Israël.

En 2014, des lanceurs d'alerte ont révélé que l'unité espionnait régulièrement les Palestiniens, cherchant des preuves d'inconduites sexuelles, de problèmes de santé ou de difficultés financières pouvant les obliger à collaborer avec les autorités militaires israéliennes d'occupation.

Ces lanceurs d'alerte [des soldats] écrivaient que les Palestiniens étaient « complètement soumis à l'espionnage et à la surveillance par les services du renseignement israélien, à des fins de persécution politique et pour créer des divisions au sein de la société palestinienne en recrutant des collaborateurs et en incitant des membres de la société palestinienne contre elle-même. »

Alors que ce sont les autorités qui ont délivré des licences d'exportation à la NSO, le ministre israélien Zeev Elkin a nié la semaine dernière « l'implication du gouvernement israélien » dans le piratage de WhatsApp. Il a prétendu à la radio israélienne : « Tout le monde comprend que cela n'a rien à voir avec l'État d'Israël. »

Un « Mossad privé à louer »

Deux exemples notoires de ce genre d'entreprise ont un court moment fait les manchettes.

La société Psy-Group, qui s'est présentée comme un « Mossad privé à louer », a été fermée l'année dernière après que le FBI a ouvert une enquête pour ingérence dans l'élection présidentielle américaine de 2016. Son « Project Butterfly » [projet papillon], selon le New Yorker, visait à « déstabiliser et perturber les mouvements anti-Israéliens de l'intérieur ».

Black Cube, quant à elle, a fait parler d'elle l'année dernière pour avoir exercé une surveillance hostile sur les principaux membres de la précédente administration américaine alors dirigée par Barack Obama. Cette entreprise semble étroitement liée aux services de sécurité israéliens et a été basée pour un temps sur une base militaire israélienne.

Un avenir cauchemardesque

L'élite de la sécurité israélienne tire profit de ce nouveau marché de la cyberguerre, exploitant – comme elle l'a fait pour le commerce des armes classiques – une population palestinienne totalement captive, sur laquelle il peut tester sa technologie.

Il n'est pas surprenant qu'Israël normalise progressivement dans les pays occidentaux des technologies intrusives et oppressives subies depuis longtemps par les Palestiniens.

Les logiciels de reconnaissance faciale permettent un profilage racial et politique toujours plus sophistiqué. La collecte et la surveillance secrètes de données effacent les frontières traditionnelles entre les espaces privés et publics. Et les campagnes de doxxing [divulgarion sur Internet de données privées avec la volonté de nuire] qui en résultent permettent d'intimider, de menacer et de fragiliser ceux qui sont dans l'opposition ou qui veulent – comme ceux qui défendent les droits de l'homme – que les puissants rendent des comptes.

Si cet avenir de cauchemar continue de se concrétiser, New York, Londres, Berlin et Paris ressembleront de plus en plus à Naplouse, Hébron, Jérusalem-Est et Gaza. Et nous comprendrons tout ce que cela signifie que vivre dans un État de surveillance, engagé dans une guerre cybernétique contre ceux qu'il a sous sa férule.

Jonathan Cook

La source originale de cet article est lexpressquotidien.dz

Copyright © [Jonathan Cook](http://JonathanCook.com), lexpressquotidien.dz, 2022

Articles Par : [Jonathan Cook](http://JonathanCook.com)

Avis de non-responsabilité : Les opinions exprimées dans cet article n'engagent que le ou les auteurs. Le Centre de recherche sur la mondialisation se dégage de toute responsabilité concernant le contenu de cet article et ne sera pas tenu responsable pour des erreurs ou informations incorrectes ou inexactes.

Le Centre de recherche sur la mondialisation (CRM) accorde la permission de reproduire la version intégrale ou des extraits d'articles du site Mondialisation.ca sur des sites de médias alternatifs. La source de l'article, l'adresse url ainsi qu'un hyperlien vers l'article original du CRM doivent être indiqués. Une note de droit d'auteur (copyright) doit également être indiquée.

Pour publier des articles de Mondialisation.ca en format papier ou autre, y compris les sites Internet commerciaux, contactez:

media@globalresearch.ca

[Mondialisation.ca](http://mondialisation.ca) contient du matériel protégé par le droit d'auteur, dont le détenteur n'a pas toujours autorisé l'utilisation. Nous mettons ce matériel à la disposition de nos lecteurs en vertu du principe "d'utilisation équitable", dans le but d'améliorer la compréhension des enjeux politiques, économiques et sociaux. Tout le matériel mis en ligne sur ce site est à but non lucratif. Il est mis à la disposition de tous ceux qui s'y intéressent dans le but de faire de la recherche ainsi qu'à des fins éducatives. Si vous désirez utiliser du matériel protégé par le droit d'auteur pour des raisons autres que "l'utilisation équitable", vous devez demander la permission au détenteur du droit d'auteur.

Contact média: media@globalresearch.ca