

Unissons-nous contre la cyber-surveillance et la répression!

10.01.2022

Categories: Apartheid et colonialisme

Un appel depuis la Palestine : unissons-nous contre la cyber-surveillance et la répression

Déclaration du Comité National palestinien de BDS (BNC) du 21/7/21

Le scandale international croissant autour du logiciel espion Pegasus du groupe israélien NSO, utilisé par des dictatures et des régimes autoritaires pour perpétrer de nombreux crimes et violations des droits humains, n'est que la partie émergée de l'iceberg. Depuis des années, Israël et ses entreprises de haute technologie exportent des logiciels espions et d'autres technologies de surveillance intrusives dans le monde entier, y compris vers certains des régimes les plus impitoyables.

Le commerce des technologies militaires, de sécurité et de surveillance constitue le socle des liens d'Israël avec le reste du monde.

Cette technologie est le résultat direct de la recherche et des pratiques qui soutiennent l'apartheid israélien dans sa répression du peuple palestinien. La surveillance massive et ciblée des Palestiniens indigènes - privés de leurs droits fondamentaux et de tout recours à la justice - est une caractéristique essentielle du système israélien de répression, d'oppression et de dépossession coloniale.

L'armée israélienne, en partenariat avec ses universités et ses centres de recherche, n'a pas seulement développé la technologie et la méthodologie utilisées pour assujettir et opprimer la population palestinienne. Elle a également mis en place un système élaboré qui canalise ses technologies militaires et de surveillance de masse "testées sur le terrain" vers le marché mondial lucratif de l'industrie de la surveillance. Il a transformé son unité de renseignement militaire 8200 en un incubateur de startups, faisant une promotion agressive de ses capacités, y compris le fait même que celles-ci sont enracinées dans l'oppression du peuple palestinien.

En 2020, les cyber-entreprises israéliennes ont reçu environ 31 % des investissements mondiaux dans le secteur. Les acquisitions d'entreprises de cyber-technologies israéliennes ont généré quelque 4,7 milliards de dollars US, et les exportations israéliennes de ce secteur se sont élevées à 6,85 milliards de dollars US. Israël est devenu un leader sur le marché des logiciels espions et de la surveillance, fournissant une expertise pour la collecte et le traitement des données, y compris les logiciels espions, la reconnaissance faciale, les "outils de suivi des utilisateurs" qui sont utilisés pour le maintien de l'ordre, la manipulation électorale, etc. Comme le confirment les révélations du projet Pegasus en cours, Israël vend cette technologie aussi bien à des gouvernements démocratiques, contribuant ainsi à l'érosion constante des droits civils, qu'à des régimes autoritaires, permettant et aggravant leurs violations des droits humains existantes,

Le régime despotique de l'Arabie saoudite avait utilisé le logiciel espion Pegasus pour traquer le dissident saoudien Jamal Kashoggi, qui a été brutalement assassiné dans l'ambassade saoudienne en Turquie en 2018. Les familles des 43 lycéens d'Ayotzinapa, au Mexique, assassinés et disparus en 2014, ont été la cible du logiciel espion israélien alors qu'elles se battaient pour obtenir justice. Pegasus a également été utilisé dans la persécution des militants et des avocats dans l'affaire Bhima Koregaon en Inde.

Les recherches sur le groupe NSO, son logiciel espion Pegasus et les Circles, moins connus, ont révélé l'étroite coopération entre l'armée, l'État et les entreprises au sein du régime d'apartheid israélien et ont mis à nu la porte tournante que le complexe militaro-industriel israélien a créée. Le ministre israélien de la défense régleme-tte étroitement le groupe NSO, en accordant des licences d'exportation individuelles, et NSO, à son tour, est prêt à vendre sa technologie lorsque le gouvernement israélien est intéressé à faire progresser les liens diplomatiques en soutenant des régimes répressifs et autoritaires dans le monde arabe, en Afrique, en Asie, en Amérique latine et au-delà. La communauté américaine du renseignement suppose qu'Israël a accès aux données collectées illégalement par Pegasus. Sans surprise, le gouvernement israélien serait en train de mettre en place une task force pour gérer la crise générée par les dernières révélations.

Il ne s'agit pas seulement du groupe NSO - il est temps d'arrêter les sociétés de cyber-surveillance dès maintenant.

Comme le dit Edward Snowden : "Leurs seuls produits sont des vecteurs d'infection. Ce ne sont pas des produits de sécurité. ...Ils ne font pas de vaccins - la seule chose qu'ils vendent, c'est le virus".

Depuis près de deux décennies, alors que la technologie numérique occupe une place centrale dans notre monde, la surveillance de masse et l'espionnage ciblé ont été exposés comme un moyen pour les États autoritaires et les entreprises de surveiller, contrôler, manipuler et réprimer les militants, les journalistes et les gens ordinaires. Cette répression mondiale, dont une grande partie provient de la matrice de surveillance militaire d'Israël, doit être remise en question par nous tous, ensemble.

Nous appelons les mouvements pour la justice, les organisations progressistes et les personnes de conscience du monde entier à :

- Nous rejoindre dans la campagne visant à interdire la cybersurveillance et à mettre fin à son rôle dans la violation et l'érosion des droits humains et civiques.
- Mettre fin au commerce sale - et mortel - du Groupe NSO à travers le monde.
- Demander la fin des relations militaires et de sécurité avec l'Israël de l'apartheid.

Source : <https://bdsmovement.net/news/call-from-palestine-unite-against-cyber-surveillance-repression>