

[Communiqué du BNC] Un appel de Palestine : unissons nous contre la cyber-surveillance et la répression

Par le Comité National BDS palestinien (BNC), le 22 juillet 2021

Le scandale international grandissant autour du logiciel espion israélien Pegasus de NSO Group, dont se servent des dictatures et des régimes autoritaires pour perpétrer quantité de crimes et de violations des droits de l'homme, n'est que le sommet de l'iceberg. Depuis des années, Israël et ses entreprises de technologie de pointe ont exporté des logiciels espions et autres technologies de surveillance intrusives à travers la planète, y compris pour certains des régimes les plus brutaux.

Le marché de la technologie militaire, sécuritaire et de surveillance constitue le socle des liens d'Israël avec le reste du monde.

Cette technologie est la conséquence directe de la recherche et des pratiques qui soutiennent l'apartheid israélien dans sa répression du peuple palestinien. La surveillance de masse aussi bien que ciblée des Palestiniens autochtones privés de leurs droits, à qui on dénie leurs droits fondamentaux et le recours à la justice, est une caractéristique essentielle du système israélien de répression, d'oppression et de dépossession coloniale.

L'armée d'Israël, en partenariat avec ses universités et ses centres de recherche, n'a pas seulement développé la technologie et la méthodologie qui ont servi à soumettre et à opprimer les Palestiniens. Elle a également mis en place un

système élaboré qui canalise sa technologie militaire et de surveillance de masse « testée sur le terrain » pour le marché mondial rentable de l'industrie de surveillance. Elle a transformé son service d'espionnage militaire Unit 8200 en un incubateur de start-ups, promouvant agressivement ses capacités, y compris le fait même qu'elles soient ancrées dans l'oppression du peuple palestinien.

En 2020, les cyber entreprises israéliennes ont reçu environ 31% de l'investissement mondial du secteur. Les acquisitions des cyber sociétés israéliennes ont généré quelque 4.7 milliards de dollars américains, et les cyber exportations israéliennes ont atteint 6.85 milliards de dollars américains. Israël est devenu un leader du marché des logiciels espions et de la surveillance, fournissant une expertise pour la collecte et le traitement des données, dont les logiciels espions, la reconnaissance faciale, 'les outils de suivi des utilisateurs' qui servent au maintien de l'ordre, à des manipulations électorales, et autres... Il vend cette technologie à des gouvernements démocratiques, contribuant à l'érosion continue des droits civiques, et à des régimes autoritaires, permettant et aggravant leurs violations existantes des droits de l'homme, comme le confirment les révélations du Projet Pegasus en cours.

Le régime despotique d'Arabie Saoudite s'était servi du logiciel espion pour traquer le dissident saoudien Jamal Kashoggi, qui a été sauvagement assassiné dans l'ambassade saoudienne de Turquie en 2018. Les familles des 43 lycéens d'Ayotzinapa, au Mexique, qui ont été assassinés et ont disparu en 2014 étaient des cibles du logiciel israélien tandis qu'ils luttait pour la justice. Pegasus a été utilisé pour persécuter militants et avocats dans l'affaire Bhima Koregaon en Inde.

L'enquête sur NSO Group, son logiciel espion Pegasus et les Cercles moins connus, a révélé l'étroite coopération qui existe entre l'armée, l'État et les affaires dans le régime

d'apartheid d'Israël, et laisse grande ouverte la porte pivotante que le complexe industriel de l'armée israélienne a créée. Le ministre israélien de la Défense contrôle étroitement NSO Group, accordant des permis d'importation individuels et NSO, en retour, est prêt à vendre sa technologie quand le gouvernement israélien souhaite développer des relations diplomatiques en aidant des régimes répressifs et autoritaires du monde arabe, d'Afrique, d'Asie, d'Amérique Latine et d'ailleurs. Le monde du renseignement américain présume qu'Israël a accès aux données illégalement collectées grâce à Pegasus. Sans surprise, on dit que le gouvernement israélien aurait mis en place un groupe de travail pour gérer la crise créée par les dernières révélations.

Cela ne concerne pas que NSO Group – il est temps maintenant de mettre fin aux sociétés de cyber surveillance.

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

Depuis presque 20 ans maintenant, alors que la technologie numérique occupe une place centrale dans notre monde, la surveillance de masse et l'espionnage ciblé ont été présentés comme un moyen pour les États autoritaires et les entreprises de surveiller, contrôler, manipuler et réprimer les militants, les journalistes et les gens ordinaires. Nous devons tous, ensemble, défier cette répression mondiale, dont une grande part trouve son origine dans la matrice de la surveillance militaire israélienne.

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

- **Nous rejoindre dans la campagne pour interdire la cyber-**

surveillance et mettre fin à son rôle dans la violation et l'érosion des droits de l'homme et des droits civiques.

- **Mettre fin à la sale – et mortelle – besogne de NSO Group dans le monde entier.**
- **Appeler à la fin des relations militaires et sécuritaires avec l'Israël d'apartheid.**

Source : BDS Movement

Traduction J. Ch. pour BDS France