Pegasus – la pointe de l'iceberg

03.09.2021

Categories: Apartheid et colonialisme, Embargo militaire

Depuis des années, Citizen's Lab de l'Université de Toronto enquête sur NSO, une compagnie israélienne spécialisée dans le cyber espionnage. En 2018, suite à l'assassinat brutal de l'opposant Jamal Khashoggi dans l'ambassade saoudiennne à Istanbul, le nom de NSO est apparu dans les journaux. Depuis quelques semaines, NSO, avec son produit phare Pegasus, un logiciel de cyber-espionnage israélien, est à la une de nombreux médias.

Le « projet Pegasus » est une enquête menée par des journalistes et des médias dans 10 pays et coordonnée par *Forbidden Stories* (1), une organisation médiatique à Paris « dont la mission est de protéger, poursuivre et publier le travail d'autres journalistes menacés, emprisonnés ou assassinés ». Le soutien technique d'Amnesty International a permis d'identifier les traces du logiciel sur 50'000 numéros de téléphones de cibles potentielles. Il s'est avéré que le logiciel espion de NSO Group a été utilisé pour faciliter les violations des droits humains à grande échelle dans le monde entier. Des chefs d'Etats, des journalistes, des opposant.e.s et des défenseurs.euses des droits humains ont été ou sont ciblé.e.s. Tout dernièrement, la RTS a révélé que le gouvernement suisse utilise des «gouvernement software » (GovWare) pour espionner des téléphones. D'après le journal NZZ il s'agirait de Pegasus.(2)

Les médias ont tous signalé que NSO était une compagnie israélienne, mais ils omettent d'expliquer sur quoi repose le développement fulgurant en Israël non seulement de l'industrie de l'armement traditionnel mais aussi des armes de surveillance et d'espionnage.

Beaucoup de technologies parmi les plus innovantes développées par l'industrie civile israélienne, notamment dans le domaine des télécommunications, émanent de la technologie militaire. Cet aspect fondamental est passé sous silence dans les récits médiatiques. Oui, Pegasus est un logiciel, mais il est surtout une nouvelle arme issue de la technologie militaire israélienne. L'industrie d'armement et sécuritaire développe et fournit des armes nécessaires à la politique d'occupation, de colonisation et d'apartheid en Israël/Palestine. Ces armes apportent les moyens techniques à l'oppression de la population palestinienne.

En Israël les secteurs de la haute technologie connaissent les taux de croissance les plus rapides, en moyenne 8% par an ces dernières années. Tout comme le secteur de l'armement, 80 % de la production « high tech » est destinée à l'exportation. Or ces secteurs nécessitent un niveau élevé de compétences ainsi que des capitaux importants. La recherche et le développement jouent aussi un rôle clef. Il n'est donc pas étonnant qu'Israël consacre 4,9 % de son PIB à ce secteur, le pourcentage le plus élevé parmi les pays de l'OCDE. Selon les experts de l'ONU, le secteur de la recherche et du développement israélienne est classé parmi les 10 meilleurs au monde. Les instituts de recherche universitaires fournissent une grande partie de la recherche et du développement de base.

Collaboration entre les universités et l'armée israélienne

Les forces de sécurité israéliennes, qu'elles soient publiques ou privées, sont devenues de plus en plus dépendantes des appareils de haute technologie issus des universités israéliennes. Les nouvelles technologies aident Israël à imposer son occupation avec moins de personnel militaire, tout en fournissant de nouveaux produits (armes) d'exportation pour l'industrie israélienne. Parmi les universités qui collaborent avec l'industrie de l'armement se trouvent le Technion de Haïfa, l'Institut Weizman de Rehovot, l'Université Ben Gourion, l'Université de Tel Aviv et l'Université hébraïque de Jérusalem (HUJ) (3). Sur son campus situé illégalement à Jérusalem-Est, cette dernière offre un programme de formation de 3 ans, Havatalot, destinée aux futurs officiers de renseignement, dans le cadre de leur service militaire obligatoire. Ces militaires vivent sur le campus dans un zone spéciale et portent leurs habits militaires pendant les cours(4). Il y a peu de pays au monde où l'établissement militaire travaille aussi étroitement avec le monde académique et des entreprises aux profit de ces trois secteurs. Cela n'empêche pas l'HUJ de participer au programme Horizon2020 de l'Union Européene !

Au sein de l'armee israélienne (IDF), l'Unité 8200 joue un rôle central dans la création de nouvelles armes estimées essentielles à la défense extérieure et intérieure du pays. L'Unité 8200 recrute les jeunes les plus brilliant.e.s qui seront formés pour créer des armes – offensives et défensives – de cyber-espionnage et de « hacking » . Plus tard, ils seront nombreux à quitter l'armée soit pour fonder leurs propres « start-ups » soit pour rejoindre des compagnies telles NSO, Quadri, Cyberx, etc. Grâce aux liens professionnels et personnels noués pendant leur service militaire, les soldat.e.s de l'Unité 8200 sont bien placé.e.s pour obtenir des investissement nécessaires à créer des « start-ups » dans le domaine du cyber-espionnage. Une étude de 2018 citée par Haaretz estime que 80 % des 2300 personnes qui ont fondé les 700 entreprises israéliennes de cyber-sécurité étaient issues du renseignement de l'armée israélienne(7). Et parmi les différents secteurs de haute technologie, la cyber-sécurité connait une expansion fulgurante. L'investissement dans le secteur sécuritaire a augmenté de 70% dans l'année 2020 (2.9 milliards de dollars).(5)

Le cyber-espionnage, arme essentielle de la politique israélienne

Mais l'industrie de cyber-espionnage n'est pas seulement un atout majeur pour l'armée et l'économie israéliennes, elle est aussi un outil essentiel pour la politique gouvernementale. « The Israël National Cyber Directorat », une agence gouvernementale, est responsable de la promotion des capacités du secteur cyber-sécuritaire du pays et de la défense intérieure du pays. Pour chaque contrat de vente à l'étranger, cette agence exerce son contrôle lors de l'offre, lors de la signature du contrat et enfin lors de la vente. Et la vente de Pegasus, une arme au même titre que des drones, des avions, etc… est également soumise à ces vérifications. Dans le contrat que Pegasus établit avec ses clients, le client promet d'observer certaines règles mais cela dépend du bon vouloir du client de s'y conformer. Dans les faits, le gouvernement n'a aucun intérêt à contrôler les ventes. En échange des exportations, approuvés par l'agence gouvernementale, Israël obtient des avantages politiques qui se répercutent sur la politique du gouvernement.

DarkMatters, établi en 2015 aux Emirats arabes unis (EAU), se limite officiellement à la cyber-défense. Mais selon une enquête de Reuters, DarkMatter fournit des services de piratage à l'agence de renseignement de ce pays contre des cibles occidentales, des journalistes et des militant.e.s des droits humains. Pour ce faire, DarkMatter utilise des logiciels israéliens et emploie d'anciens membres de l'Unité 8200. En 2020, grâce aux bons offices de Trump, Israël et les EAU ont signé un accord qui établit les relations diplomatiques entre les deux pays(6).

L'Arabie saoudite est sur la liste des pays ennemis d'Israël. Cela n'empêche pas Israël de permettre la vente des armes lourdes et de cyber-armes aux compagnies saoudiennes. Israël a tout intérêt d'avoir des contacts non officiels avec certains pays arabes. Car les pays ennemis peuvent aussi avoir un ennemi commun, l'Iran.

Vu l'importance de l'exportation d'armes de surveillance, de télécommunication et de cyber-espionnage (entre 7 et 9% des exportations de défense israéliennes), le gouvernement cherche à augmenter ces exportations. L'Iran, le Liban et la Syrie étant les seuls pays qui en sont exclus.

Et la Suisse ?

En 2013 le DFJP (Département fédéral de Police et Justice) a signé un contrat pour le nouveau système d'écoute téléphonique de la Suisse à Verint, entreprise israélienne spécialisée dans l'écoute téléphonique et l'espionnage. Ceci malgré le fait que le partenaire privilégié de Verint soit la NSA (National Security Agency) des États-Unis.

En 2015 l'armée suisse a acheté 6 drones Hermès à l'entreprise israélien Elbit, qui était, selon les autorités, devenu incontournable dans la production de drones « testés sur le terrain ». En 2021, le gouvernement a une fois de plus fait appel à Elbit pour un contrat concernant les moyens de télécommunication de l'armée. Plusieurs voix se sont levées contre ce choix, notamment à cause du risque d'un back box dans les logiciels, dispositif qui pourrait permettre à un pays tiers d'avoir accès aux informations sensibles. Les autorités ont à nouveau estimé que le choix était approprié puisqu' Elbit était l'entreprise la plus performante dans le domaine des télécommunications. Le 11 août, la RTS a rélévé que la Confédération utilisait des logiciels dits « gouvernement software » et des des antennes cachées permettant d'espionner ou de localiser des téléphones portables (IMSI-catchers) lors d'« infractions extrêmement graves comme les meurtres, viols et le soutien à des organisations terroristes ». Le NZZ a affirmé qu'il s'agissait du logiciel Pegasus(8). Décidément NSO est incontournable dans le domaine de la cyber-surveillence et le cyber-espionnage.

Or, l'histoire en Suisse nous a appris que le terme d' « organisation terroriste » est un sujet à de multiples interprétations. Ainsi, en 1989, une enquête parlementaire révèlait « l'affaire des fiches » : 900'000 personnes, dont des militant.e.s d'extrême gauche, des élu.e.s politiques, etc… avaient été surveillé.e.s et fiché.e.s en toute impunité par la police fédérale. Aujourd'hui, BDS, mouvement qui défend les droits légitimes de la population palestinienne par des moyens non-violents, est accusé par des parlementaires UDC de soutenir des mouvements terroristes. Des militant.e.s d'Extinction rébellion, qui préconisent l'utilisation de moyens non-violents pour stimuler la prise de conscience de la catastrophe climatique, sont-ils/elles également des extrêmistes aux yeux des tribunaux ?

L'utilisation à grande échelle des logiciels de surveillance et d'espionnage par des gouvernements voyous, mais aussi par des gouvernements des pays dits démocratiques, représente un immense danger. Les opposant.e.s deviennent, aux yeux de ceux et celles au pouvoir, des terroristes présum.e.s. Les droits démocratiques, la liberté d'expression, la liberté de manifester – sont de plus en plus soumis à de restrictions.

Certes Israël n'est pas le seul pays à produire et à exporter des armes, du matériel de surveillance et des logiciels de cyber-sécurité et d'espionnage. Mais il est le seul aux XXI siècle à être reconnu comme pratiquant une politique d'apartheid. Pour le droit international humanitaire, l'apartheid constitue un crime contre l'humanité. Au 20ème siècle, l'apartheid a été jugé intolérable en Afrique du Sud. L'apartheid est tout aussi intolérable en Israël/Palestine au 21ème siècle. Les armes lourdes, les armes de surveillance et de cyber-espionnage israéliennes sont conçues d'abord et avant contre la population palestinienne : elles servent à l'expulser de ses terres, à la soumettre et à la contrôler. En vendant ces armes à travers le monde, l'Etat d'Israël exporte aussi ses modèles d'oppression, son racisme, ses stratégies de surveillance et de contrôle qui sont ensuite utilisées pour traquer toutes celles et ceux qui luttent contre le colonialisme, le racisme, la militarisation de la société et l'exploitation des personnes les plus fragiles dans nos sociétés. Les drones Elbit, avec Frontex, traquent les réfugié.e.s sur la Meditérranée. Les stratégies de l'armée israélienne pour controller les palestinien.ne.s sont reprises par certaines des forces de police américaines. En Indonesie les logiciels de NSO traquent les LGBTQI+.

C’est pour toutes ces raisons que BDS appelle à un embargo militaire d’Israël. Il s’agit non seulement de contribuer à la lutte pour la mise à ban de cet Etat voyou, mais également de rejoindre et de renforcer les luttes globales pour la liberté, l’égalité et la justice.

1. https://forbiddenstories.org

2. https://www.nzz.ch/technologie/pegasus-die-schweiz-hat-umstrittene-spionagesoftware-eingesetzt-ld.1640310?reduced=true

3. https://bds-info.ch/index.php/fr/articles/la-cooperation-de-grandes-universites-israeliennes-avec-les-organes-securitaires

4. https://www.haaretz.com/israel-news/.premium-hebrew-university-to-host-israeli-army-base-on-campus-1.7113981

5. https://www.bankinfosecurity.cm/investments-i-israels-cybersecurity-sector-grow-a-15956

6. https://www.haaretz.com/israel-news/.premium-mysterious-uae-cyber-firm-luring-ex-israeli-intel-officers-with-astronomical-salaries-1.7991274?v=1629128028083

7. https://www.rts.ch/info/suisse/12411718-la-suisse-utilise-aussi-un-logiciel-espion-israelien-du-type-pegasus.html

8. https://www.nzz.ch/technologie/pegasus-die-schweiz-hat-umstrittene-spionagesoftware-eingesetzt-ld.1640310?reduced=true