



Israël perfectionne sa technologie de surveillance.

Laissez l'opportunité au Mossad et au Shin Bet de profiter militairement et financièrement du virus.

Par [Philip Girdali](#)

Mondialisation.ca, 16 mai 2020

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

Thème: [Droits humains et État policier](#),
[Services de renseignements](#)

Analyses: [COVID-19](#)

L'organisation d'espionnage externe d'Israël, le Mossad, et son équivalent d'espionnage interne, le Shin Bet, ont une réputation bien plus grande que leurs succès réels, mais le seul domaine dans lequel ils ont excellé est la collecte de renseignements électroniques. L'espionnage électronique récent autour de la Maison Blanche et d'autres bâtiments fédéraux à Washington, effectué par l'ambassade israélienne, démontre qu'Israël ne fait pas beaucoup de différence entre amis et ennemis lorsqu'il mène des activités d'espionnage. En fait, l'espionnage visant les États-Unis est probablement sa priorité numéro un, car l'État juif est si fortement dépendant du soutien étasunien qu'il se sent obligé de savoir quelles discussions le concernant se déroulent à huis clos.

La pénétration israélienne dans les télécommunications étasuniennes a commencé dans les années 1990, lorsque des sociétés étasuniennes comme AT&T et Verizon, les principaux relais de l'Agence de sécurité nationale (NSA) pour la surveillance des communications, ont commencé à utiliser du matériel produit en Israël, en particulier pour la surveillance liée à l'application de la loi et les enregistrements clandestins. Ces appareils étaient dotés d'une « porte dérobée », ce qui signifie que tout ce qu'ils faisaient était partagé avec Israël. Les cyber-spécialistes israéliens se sont même introduits dans des réseaux classifiés, la NSA et le FBI étant au courant de ce qui se passait mais peu disposés à affronter « le meilleur allié de l'Amérique ». Le président Bill Clinton a un jour dit à Monica Lewinski qu'ils devaient éviter d'utiliser le téléphone du Bureau ovale parce que quelqu'un pourrait l'écouter. Il faisait référence à Israël.

Il est certain que le secteur de la haute technologie de l'État juif a été grandement aidé dans son effort par les « propres objectifs » fournis par les États-Unis, ce qui permet à Israël de soumissionner à des contrats gouvernementaux relatifs à la sécurité nationale, garantissant virtuellement que toute innovation technique sera volée et réexportée par les entreprises de haute technologie israéliennes. Les grands innovateurs technologiques comme Intel, qui travaille avec la NSA, se sont installés en Israël et ont déclaré publiquement : « Nous nous considérons comme une entreprise israélienne autant que comme une entreprise américaine ». Le milliardaire sioniste Paul Singer a récemment été accusé de diriger vers Israël des emplois hautement rémunérés du secteur technologique étasunien, des emplois qui sont perdus à jamais pour l'économie étasunienne.

Ainsi, Israël est un leader dans l'utilisation des ressources électroniques pour effectuer de

l'espionnage et collecter des informations sur diverses cibles d'intérêt. Israël est également un innovateur, et sa relation étroite avec la communauté du renseignement étasunien (IC), plus particulièrement la NSA, signifie que les technologies et les procédures développées par l'État juif apparaîtront inévitablement aux États-Unis.

En tout état de cause, les États-Unis travaillent d'arrache-pied sur leurs propres outils de gestion des personnes, sous l'impulsion de l'hystérie de Covid-19. Des cartes d'identité spéciales pourraient permettre de suivre l'état de santé des individus. Cet état serait enregistré et mis à jour sur une puce lisible par les scanners du gouvernement qui, selon certains témoignages, pourrait être portée ou même intégrée de façon permanente dans le corps de chacun. Un autre plan promu par une entreprise commune d'Apple et de Google qui semble avoir le soutien de la Maison Blanche consiste à « ajouter à leurs plateformes de téléphones intelligents une technologie qui alertera les utilisateurs s'ils sont entrés en contact avec une personne atteinte de Covid-19 ». Les gens doivent adhérer au système, mais celui-ci a le potentiel de surveiller environ un tiers de la population mondiale », la surveillance étant assurée par des ordinateurs centraux. Une fois établi le principe juridique selon lequel les téléphones peuvent être manipulés pour effectuer ce qui est maintenant une « recherche illégale », il n'y a pas de limites techniques ou pratiques aux autres tâches qui pourraient également être effectuées.

Développements en Israël

Compte tenu des mesures prises pour contrôler les mouvements des citoyens susceptibles d'être infectés, certains développements récents en Israël sont, pour ne pas dire plus, inquiétants. **L'État juif procède actuellement à une surveillance multi-niveaux en temps réel, 24 heures sur 24 et 7 jours sur 7, de toutes les personnes résidant dans le pays.** Le journaliste d'investigation et militant pour la paix **Richard Silverstein** décrit en détail pourquoi cela se produit maintenant, ce que cela signifie et comment cela fonctionne.

Per Silverstein, Israël, comme tous les autres États autoritaires, profite actuellement de la distraction causée par la pandémie de coronavirus. Le Premier ministre **Benjamin Netanyahu**, dont la fortune politique semblait être sur le déclin en raison de trois élections en suspens, a exploité la peur du virus pour assumer les pouvoirs d'urgence et obtenir l'approbation de la Knesset pour utiliser une base de données nationale hautement classifiée « compilée par le Shin Bet et comprenant des données personnelles privées sur chaque citoyen israélien, tant juif que palestinien. Au lendemain du 11 septembre, la Knesset israélienne a secrètement confié à son service de renseignement national la tâche de créer la base de données, qui était prétendument destinée à la lutte contre le terrorisme ».

La base de données, surnommée « The Tool », comprend des noms, des adresses, des numéros de téléphone, des informations sur l'emploi et l'éducation, mais elle va bien au-delà en utilisant des données de suivi téléphonique pour enregistrer chaque appel téléphonique passé par l'individu afin d'inclure les noms et numéros des personnes appelées et la localisation géographique de l'endroit d'où l'appel a été passé. Le suivi des appels téléphoniques a également permis à Shin Bet de créer un registre des déplacements de l'appelant en Israël et dans les territoires occupés. L'utilisation d'Internet, si elle était active au téléphone, a également été enregistrée. Il s'agit d'une surveillance aussi complète et totale qu'il est possible d'obtenir d'un individu et elle n'implique aucune participation humaine, chaque élément étant réalisé par ordinateur.

Netanyahu a publiquement proclamé son intention d'utiliser la base de données, déclarant qu'elle serait utilisée pour combattre le coronavirus, qu'il a décrit comme une menace pour la survie nationale. Suite à la crise annoncée, lui et son principal adversaire, le leader du parti Bleu et Blanc **Benny Gantz**, ont pu s'entendre le 20 avril pour former un « gouvernement d'unité nationale d'urgence » avec Netanyahu comme premier ministre.

L'exploitation de la peur du virus et la révélation du puissant outil technique dont dispose Israël pour le contrecarrer ont permis à Nétanyahou de remporter une victoire, lui qui s'est effectivement présenté comme un leader fort et indispensable, effaçant ainsi les stigmates résultant de son procès en cours pour corruption massive pendant son mandat. L'une des premières mesures que Nétanyahou va apparemment prendre est de remplacer le procureur général et le procureur de l'État qui cherchaient à l'envoyer en prison, supprimant ainsi la menace qu'il puisse être emprisonné.

La révélation de l'existence de la base de données a inévitablement conduit à des accusations selon lesquelles Nétanyahou aurait, pour son profit personnel, révélé la plus puissante arme antiterroriste d'Israël. L'importance de l'énorme quantité d'informations personnelles collectées par le Shin Bet a également suscité des inquiétudes, notamment en ce qui concerne la suggestion qu'elle constituait une violation flagrante des libertés civiles. Mais la crainte du virus soigneusement maintenue, combinée à certains accords et manœuvres politiques, a fait que l'utilisation de ces données a finalement été approuvée par le comité de sécurité de la Knesset à la fin du mois de mars.

Israël, qui a fermé ses frontières et qui a encore un niveau relativement faible d'infections et de décès dus au coronavirus, a déjà commencé à utiliser la base de données du Shin Bet tout en transformant les tentatives de lutte contre la maladie en une sorte de guerre du renseignement. Les informations obtenues grâce à « The Tool » permettent à la police et à l'armée de déterminer si une personne se tenait près d'une autre personne pendant plus de quelques minutes. Si le contact incluait une personne déjà infectée, tous les autres individus sont placés en quarantaine. Toute tentative de se soustraire aux contrôles entraîne l'arrestation et la sanction d'une peine de six mois de prison, plus une amende de 1 500 dollars. Les soldats armés qui patrouillent dans les rues sont habilités à interroger toute personne en déplacement.

Le Mossad est également impliqué dans la lutte contre le virus, se vantant d'avoir « volé » 100 000 masques faciaux et également des respirateurs à un pays voisin présumé être les Émirats arabes unis. Silverstein observe que « le gouvernement d'extrême droite d'Israël a militarisé la contagion. Tout comme un marteau n'a jamais rencontré un clou qu'il ne voulait pas enfoncer, il est tout à fait naturel pour un État de sécurité nationale comme Israël de considérer Covid-19 comme une menace pour la sécurité tout autant, voire plus, qu'une menace pour la santé ». En ce qui concerne les armes biologiques, Israël n'y est pas parvenu. Ironiquement, l'histoire cachée derrière la « guerre contre le coronavirus » est qu'Israël est lui-même l'un des États les plus avancés dans le développement et les tests d'armes biologiques dans son laboratoire de Nes Tziona.

Revenant sur l'émergence de « l'outil », le ministre de la défense, **Naftali Bennett**, a également suggéré de monétiser le produit en vendant une « version civile », qui comprendrait le système d'exploitation, les capacités analytiques et les détails de configuration à des pays étrangers, dont les États-Unis. Israël a déjà commercialisé avec succès aux agences de sécurité et aux gouvernements un produit similaire appelé Pegasus, qui a été décrit comme le malware le plus sophistiqué du marché.

Comme The Tool, Pegasus fait de l'exploration de données et de l'analyse en temps réel des individus en se basant sur une série de techniques de collecte. La cyberentreprise israélienne NSO Group, qui commercialise Pegasus, a récemment été impliquée dans une tentative de piratage du système de communication sécurisé Whats-App, propriété de Facebook-, ciblant des journalistes et des militants politiques, pour le compte d'un client inconnu. Ironiquement, on pense que Facebook avait auparavant utilisé les services quelque peu obscurs de NSO Group. Peut-être plus notoirement, Pegasus a également été utilisé pour surveiller les contacts et établir la localisation physique dans le cas du journaliste Jamal Khashoggi, qui a été assassiné par des agents des services de renseignement saoudiens à Istanbul.

Les États-Uniens devraient donc être prudents lorsqu'ils sont confrontés au nouveau logiciel de cybersécurité promu par Israël, car l'État juif exporte également sa propre vision d'un État militarisé contrôlé centralement où tous les droits sont potentiellement sacrifiés pour la sécurité. Comme l'a déjà révélé le dénonciateur Edward Snowden, la NSA a la capacité de collecter de vastes quantités d'informations sur les citoyens. Si le gouvernement étasunien tombe dans le piège et se dirige vers Israël, en utilisant ces données pour permettre la surveillance et la gestion de tous les citoyens en permanence, la tentation sera grande d'utiliser cette nouvelle technologie même si son utilisation n'est pas justifiée à proprement parler.

Et il n'y aura personne pour dire non aux nouveaux pouvoirs, ni au Congrès, ni à la Cour suprême, ni à la Maison Blanche. Et les médias seront également de la partie, arguant que la sécurité contre les menaces externes et internes nécessite certaines violations des droits de la personne. C'est l'une des ironies de l'histoire que les États-Unis d'Amérique, avec leurs vastes ressources, leur importante population et leur héritage de liberté individuelle, soient devenus plus semblables à leur petit État client militarisé, Israël. C'est une tendance à laquelle tout Étasunien soucieux des libertés fondamentales doit à tout prix s'opposer.

Philip Giraldi

*

Note aux lecteurs : veuillez cliquer sur les boutons de partage ci-dessus ou ci-dessous. Faites suivre cet article à vos listes de diffusion. Publiez cet article sur votre site de blog, vos forums Internet, etc.



Article original en anglais :

[**Israel Perfecting Surveillance Tech**](#)

Cet article a été publié à l'origine sur [American Free Press](#).

Traduit par Maya pour [Mondialisation](#).

L'image en vedette est celle de l'American Free Press

Philip Girdali est un ancien spécialiste de la lutte contre le terrorisme de la CIA et un officier du renseignement militaire. Il est également chroniqueur et commentateur de télévision. Il est également le directeur exécutif du Conseil pour l'intérêt national. Ses autres articles sont publiés sur le site web de « The Unz Review ».

La source originale de cet article est Mondialisation.ca
Copyright © [Philip Girdali](#), Mondialisation.ca, 2020

Articles Par : [Philip Girdali](#)

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 inexacts.

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](#) 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