UQÀM
CHAIRE RAOUL-DANDURAND
EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

CHRONIQUES DES NOUVELLES CONFLICTUALITÉS

Hacktivisme Hamas-Israël : entre cyberguerre et opportunisme

Par Fanny Tan

La guerre entre Israël et le Hamas a mobilisé un grand nombre de groupes hacktivistes, qui ont pris fait et cause pour l'une des deux parties dans le cyberespace. Toutefois, sous couvert de motivations idéologiques, ces attaques revêtent parfois d'autres motifs pour les pirates qui les initient.

Depuis l'attaque-surprise du Hamas en Israël le 7 octobre dernier, plus d'une centaine d'anciens et de nouveaux groupes cybermilitants aux origines variées ont publiquement prêté allégeance à l'un des deux camps. Comme observé dans le contexte de la guerre en Ukraine, cette vaste mobilisation cause beaucoup de remous dans l'espace numérique, dont les vrais signaux sont souvent difficiles à distinguer.

En effet, malgré l'abondance des revendications diffusées par les hacktivistes sur des plateformes comme Telegram, seule une poignée de cyberattaques s'est réellement produite jusqu'ici, et la plupart se sont avérées bénignes. Si des attaques par déni de service distribué (DDoS) et des « défacements » de sites web ont effectivement été menés des deux côtés, la majorité de ces interventions n'a causé que des perturbations mineures, affectant l'accès aux sites web ciblés pendant quelques minutes, voire quelques secondes seulement.

Israël a été particulièrement visé par ces attaques plus symboliques que dommageables. Selon la firme de cybersécurité israélienne CheckPoint, plus de quarante groupes hacktivistes auraient ciblé des sites gouvernementaux et médiatiques israéliens, en plus d'importantes organisations comme la Banque d'Israël et la société de télécommunication Cellcom, lors de la première semaine du conflit. Parmi les rares attaques symboliques notables, il y a celle ayant visé le Jerusalem Post, dont le site web a été rendu indisponible pendant près de deux jours. Elle a été revendiquée à la fois par le groupe islamique Team insane Pakistan et Anonymous Sudan — un groupe aligné sur les intérêts de la Russie qui ne serait lié ni au Soudan ni au collectif Anonymous. Dans le même registre, on note le piratage de deux panneaux d'affichage intelligents à Tel-Aviv et ses environs, qui ont diffusé des messages pro-Hamas pendant quelques minutes.

La seule attaque hacktiviste ayant véritablement inquiété les autorités israéliennes, revendiquée à la fois par Anonymous Sudan et le groupe islamique AnonGhost, est celle ayant affecté l'application mobile Red Alert, qui sert à prévenir les civils israéliens de frappes de roquettes imminentes. Celle-ci a été piratée de manière à envoyer des notifications menaçantes à ses usagers. Plus récemment, la découverte de BiBi-Linux, un nouveau maliciel de type *wiper*[1] qui s'en est pris aux systèmes Linux d'entreprises israéliennes, témoigne d'une possible sophistication des cyberattaques à venir.

Un autre type d'attaque que les groupes hacktivistes prétendent fréquemment mener dans le cadre de la guerre Israël-Hamas consiste en des opérations de type *hack and leak*, soit le vol et la dissémination de données sensibles. Bien que la plupart des fuites se soient révélées fausses — les pirates rediffusant abondamment des données issues d'anciennes fuites —, le risque pour les populations visées demeure réel. Le récent piratage de la compagnie de test génétique 23andMe, suivant lequel des données sensibles de plus d'un million de personnes juives ashkénazes ont été mises en vente sur BreachForums, suscite de l'inquiétude chez les communautés juives, qui, comme les communautés palestiniennes, sont visées par des incidents haineux bien au-delà du Proche-Orient.

Notoriété et gain financier

Ce qui ressort de cette envolée de l'hacktivisme dans le conflit Israël-Hamas, c'est surtout l'afflux d'allégations exagérées, voire complètement fausses, de cyberattaques revendiquées par certains groupes. Le jeu des prétentions se révèle parfois particulièrement complexe. En témoigne le cas de la cyberattaque prétendument perpétrée

[1] Un *wiper* est un maliciel (logiciel malveillant) dont l'objectif est d'effacer les données du disque dur d'un ordinateur infecté.

contre la centrale électrique israélienne de Dorad et revendiquée par Cyber Av3ngers, un compte Telegram paraissant vouloir usurper l'identité du groupe pro-Iran Cyber Avengers.

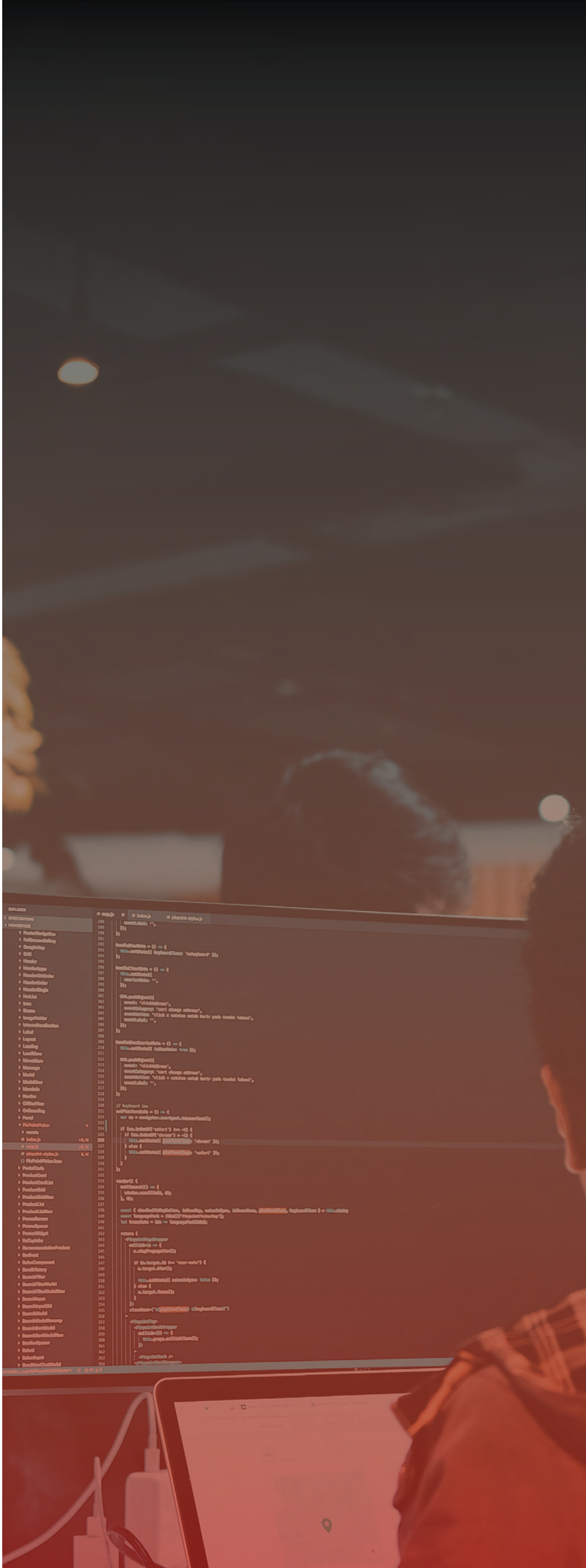
Outre la course à la notoriété, c'est l'appât du gain financier qui semble motiver certains regroupements d'hacktivistes à prendre part (ou à prétendre prendre part) aux cyberhostilités. En effet, la visibilité générée par le conflit représenterait un moyen pour les pirates d'attirer l'attention sur les services cybercriminels qu'ils commercialisent parallèlement sur le dark web.

Selon un chercheur en renseignement sur les cybermenaces chez Equinix, plusieurs acteurs profiteraient de la situation au Proche-Orient pour promouvoir leurs services de courtiers d'accès initial et de *DDoS-for-hire*. C'est le cas de Killnet, un collectif de cybermilitants prorusse très actif en Ukraine, qui a passé une bonne partie de l'année 2023 à travailler sur sa stratégie marketing. Les conflits armés contemporains tendent à démontrer que la frontière entre l'hacktivisme et la cybercriminalité, voire dans certains cas le cybermercenariat, est plus mince qu'il n'y paraît.

Résurgence de groupes commandités par des États

De fait, la participation de groupes étrangers (notamment indiens, russes et iraniens) aux cyberhostilités ajoute une couche de complexité à l'arène virtuelle de la guerre Israël-Hamas.

Les actions des groupes prétendument hacktivistes, mais en fait soupçonnés d'être commandités par des États, inquiètent particulièrement. En effet, contrairement à ceux cybermilitants, les groupes parrainés par des États sont plus sophistiqués et causent des dommages beaucoup plus



importants sur des cibles de haut niveau, telles les infrastructures critiques.

L'amélioration des capacités cyber des groupes de pirates informatiques commandités par l'Iran ainsi que le retour de Predatory Sparrow, que certains croient lié au gouvernement israélien, font craindre une escalade des tensions Iran-Israël dans le cyberespace. Alors que Predatory Sparrow avait déjà fait les manchettes pour avoir ciblé des installations sidérurgiques au printemps 2022 et des systèmes de paiements de stations-service iraniennes à l'automne 2021, les pirates iraniens se sont montrés particulièrement agressifs envers Israël dans la dernière année.

Malgré ces inquiétudes, l'intensité de la cyberguerre Israël-Hamas est, pour l'heure, bien moindre que celle ayant sévi lors des premiers jours de l'invasion russe en Ukraine en février 2022. Plusieurs experts interrogés sur le sujet estiment que l'hacktivisme Israël-Hamas n'aura pas d'impact significatif sur le terrain, ni même en ligne, vu le caractère rudimentaire de la majorité des attaques perpétrées à ce jour. Selon Alexander Leslie, analyste en renseignement sur les menaces pour la firme Recorded Future, l'écrasante majorité des cyberattaques revendiquées par les groupes cybermilitants sont « opportunistes et réactives ». Toutefois, l'abondance des attaques, bien que mineures, demeure un sujet de préoccupation chez certains, qui craignent une amplification des hostilités dans les semaines à venir.

Impact au Canada

L'essor de l'hacktivisme dans le cadre de la guerre Israël-Hamas pourrait-il affecter le Canada ? Comme observé lors des attaques par déni de service distribué perpétrées par des groupes pro-russes cette année au Québec et au Canada, les pirates informatiques étrangers n'hésitent pas à cibler des États soutenant la cause de pays ennemis. Plusieurs groupes pro-Palestine ont d'ores et déjà attaqué des entités en Inde, en France, aux États-Unis et en Ukraine, en réponse au soutien de ces pays à Israël. Il est donc probable que des actions similaires soient éventuellement observées au Canada si Ottawa devait par exemple adopter des mesures significatives ou très médiatisées par rapport au conflit.

Des personnalités qui s'exprimeraient publiquement sur la situation pourraient également être visées par des cyberattaques, comme l'illustre le coûteux piratage du casino du milliardaire israélo-américain Sheldon Adelson perpétré en 2014 à la suite de ses propos incendiaires sur l'Iran. Dans le cyberespace, les frontières nationales sont rapidement franchies, en particulier lors de conflits qui ne laissent personne indifférent.

Fanny Tan est chercheure à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux : https://dandurand.uqam.ca/