LE RUBICON

Retour en asymétrie : Que nous apprend le combat cyber-électronique entre Israël et le Hamas ?

Anthony Namor | 1 août 2024

Le 7 octobre 2023, alors que le regard des analystes était tourné vers l'Ukraine, prenant la mesure du retour d'une conflictualité inter-étatique de grande ampleur dite de haute intensité, l'attaque du Hamas en territoire israélien a brusquement rappelé au monde que l'asymétrie et le terrorisme étaient loin d'avoir disparu du contexte stratégique contemporain. Les combats qui se déroulent désormais sur ces deux théâtres ont pourtant quelques points communs, parmi lesquels figure l'incontournable confrontation cyber-électronique, considérée dans cet article comme l'ensemble des actions sur les réseaux informatiques et de guerre électronique, dont la convergence de plus en plus marquée a amené la doctrine américaine à les concevoir de pair sous la notion de *cyber electromagnetic activities*. Dans ce domaine, l'analyse plus spécifique d'un conflit entre une force étatique réputée pour sa supériorité numérique et technologique et d'une structure militaire pratiquant essentiellement le combat irrégulier offre un précieux éclairage sur les possibilités et limites des effets dans les champs immatériels. Elle est d'autant plus nécessaire qu'elle préfigure sans doute une forme de combat qui pourrait se généraliser.

Comment le conflit israélo-palestinien se traduit-il dans le domaine cyber-électronique depuis 2023 ? Les actions aéroterrestres du Hamas et d'Israël ont-elles bénéficié d'un appui innovant dans ce domaine ? Quels enseignements peut-on en tirer ?

Les modes d'actions et effets produits par les deux camps dans les trois couches du cyberespace (physique, assurant le transport et stockage de l'information ; logique, permettant son partage et son traitement par des logiciels ; et sémantique désignant son sens et son interprétation par les humains) sont révélateurs de la manière dont l'affrontement asymétrique (du faible au fort, via des moyens irréguliers) s'y manifeste. À Gaza, ils relèvent d'une recherche d'égalisation des rapports de forces par le camp le plus faible (dans une logique de techno-guérilla), d'une lutte autour du siège informationnel imposé par le camp fort et de l'exploitation du cyberespace pour semer la terreur. S'ils ne sont pas à même de faire basculer le cours des combats, ils nous rappellent surtout, à l'heure des tranchées ukrainiennes, que chaque conflit contemporain comporte désormais un affrontement dans cet espace.

Un théâtre d'opérations très tactique à forts enjeux géopolitiques

Afin de comprendre le combat qui se joue dans le cyberespace du conflit, il convient tout d'abord d'en appréhender la géographie physique – qui rend l'échelon tactique particulièrement important et sensible – et cyber, qui augure d'une lutte pour l'accès d'un territoire enclavé aux opinions internationales attentives à son sort.

La spécificité du conflit israélo-palestinien tient d'abord à la géographie, qui en fait un théâtre éminemment tactique de par les dimensions de sa principale zone de combats (41 km par 6 à 12 km pour Gaza) et la densité de ses zones urbaines, dont la forte intrication entre combattants et population civile est un corollaire. Cette configuration implique, pour les *Israel Defense Forces* (IDF), de déployer un grand volume de troupes, essentiellement débarquées, dans de petits compartiments de terrain cloisonnés et des souterrains (quatre divisions sont engagées). Les communications radio et la coordination sont alors cruciales pour éviter les tirs fratricides, en particulier dans le cadre d'opérations complexes combinant différents domaines (feux dans la profondeur, actions au sol, aviation, drones, etc.).

En couche physique du cyberespace, dans un territoire aussi petit et enclavé, la connectivité présente une forte dépendance aux pays voisins, tant du point de vue des infrastructures que de l'énergie. Le principal opérateur mobile y est *PalTel* et n'a été autorisé par Israël à y déployer un réseau 3G qu'en 2018. Le passage à la 4G était envisagé pour 2023, avant que le conflit actuel n'éclate, et n'a donc pas abouti. Ainsi le réseau mobile gazaoui offre des débits relativement faibles et une moindre sécurité. À l'inverse, l'ouverture et le niveau de développement économique d'Israël amène le pays à disposer d'un excellent maillage télécom et d'accords de *roaming* (entente entre opérateurs partageant leurs infrastructures) qui vont paradoxalement jouer un rôle important pour l'accès des Palestiniens à Internet.

Bien que les opérations dans Gaza aient ainsi une dimension tactique très importante – impliquant des combats urbains du niveau de la section voire du groupe, leurs enjeux ont un retentissement géopolitique très fort. Au niveau régional, par l'implication de l'Iran et des Houthis attaquant notamment les flux commerciaux en mer Rouge. Dans le monde, le conflit est très observé et a des répercussions sur le positionnement de plusieurs États vis-à-vis des belligérants. Il suscite également l'engagement de plusieurs groupes d'hacktivistes (pirates menant des actions pour des motifs idéologiques) de diverses régions du monde telles que la Russie, l'Iran, l'Inde ou le Bangladesh. Dans ce contexte, l'accès à l'opinion publique internationale pour lui présenter un narratif à même de la faire peser sur le soutien ou la condamnation d'un camp revêt une importance majeure.

Forces en présence : la puissance face à l'hybridité

Une seconde clef de compréhension de l'affrontement dans le cyberespace réside dans l'analyse des forces qui s'opposent sur le terrain.

Ainsi pour relever le défi d'une telle opération, Israël s'appuie sur une structure de commandement repensée au travers du *Momentum Multiyear Plan* de 2019 pour favoriser l'intégration multi-domaines (terre, air, mer, renseignement, cyber, guerre électronique…) dans la planification et la conduite des opérations. Le système de commandement et contrôle (C2) est alors essentiel dans la performance de Tsahal. Il repose par ailleurs sur l'idée de l'*intelligence-based warfare* : le positionnement du renseignement au centre des opérations, son partage étant facilité par l'intégration d'agents de l'unité 8200 (centre national de collecte et traitement du renseignement d'origine électromagnétique, dont la mission peut être comparée à celle de la NSA) dans les états-majors jusqu'au niveau brigade et par l'utilisation de systèmes d'intégration de sources de renseignement, tels que le TORCH-X d'Elbit. Plus largement, Tsahal est réputée pour son haut niveau technique porté par son tissu industriel : en cyberdéfense, *NSO Group* en est le plus célèbre exemple. En guerre électronique, on pourra citer *Netline* et ses brouilleurs de drone et d'IED portatifs sans doute pertinents en zone urbaine.

De leur côté, les brigades Al Qassem (branche armée du Hamas) opèrent sur un mode irrégulier, employant principalement des modes d'actions terroristes, tout en présentant une organisation et une hiérarchisation proches d'une armée régulière, ainsi qu'un arsenal leur permettant de se confronter à une puissance comme Israël. Depuis une dizaine d'années, malgré la pression constante d'Israël, le Hamas semble avoir développé des capacités de cyberespionnage notamment par *phishing* via des mails piégés, visant essentiellement à collecter du renseignement sur les forces israéliennes. Il serait par exemple capable de développer et déployer des applications mobiles malicieuses à fin d'espionnage. Également soutenu par l'Iran dans ce domaine, il bénéficie de l'appui de groupes d'hacktivistes tels que *Molerats*, *AnonGhost* et *Dark Storm*. D'un point de vue plus offensif, ce soutien lui permet de mener des dénis de service ainsi que des défigurations de sites web (modification d'une page à l'insu de son administrateur). De plus, le groupe semble s'être doté d'une capacité de guerre électronique, au moins de brouillage GPS (technologie peu coûteuse et relativement facile d'accès), voire d'outils plus performants qui auraient pu être fournis par l'Iran.

Enfin, il aurait disposé d'un véritable *datacenter* découvert par les IDF lors de leur opération dans Gaza, tendant à montrer la faculté du groupe à exploiter la donnée pour optimiser son efficacité opérationnelle.

À l'aune de ce contexte, l'analyse des actions cyber-électroniques de chaque camp offre au moins trois principaux enseignements.

La recherche de l'égalisation par l'appui cyber-électronique

Tout d'abord, on observe que le Hamas exploite cet appui pour réduire l'avantage comparatif de son adversaire. Ce type de tactique est caractéristique du combat asymétrique et de l'hybridation. Au plan offensif, il tire le meilleur parti possible des capacités qu'il a récemment développées. Pour se défendre, il présente une faible surface d'attaque et utilise le couvert naturel d'un milieu urbain qu'il connait bien.

Ainsi dans la couche physique du cyberespace, le brouillage et l'attaque par drones des infrastructures télécoms le long des défenses israéliennes auraient favorisé l'effet de surprise de ses commandos le 7 octobre 2023. Ils auraient tout du moins entravé et retardé la mise en alerte de troupes à même de repousser l'attaque. Plus tard dans le conflit, la capacité du Hamas à perturber le GPS sur de grandes distances aurait également fait peser une menace sur l'efficacité de certaines bombes israéliennes guidées par ces signaux telle que la GBU 39.

Dans la couche logique, si les attaques informatiques propalestiniennes sont jugées peu complexes et dénotent du faible niveau de sophistication des groupes qui les exécutent, leur rapport coût-efficacité semble avantageux. Dans la phase de préparation de ses opérations, le Hamas a pu bénéficier de renseignement via des actions simples sur les réseaux sociaux et en utilisant des applications piégées telles qu'évoquées plus haut. Le détournement de l'application *Red Alert* – utilisée par Israël pour prévenir ses habitants des frappes palestiniennes – afin de diffuser de fausses alertes est un bon exemple d'action à faible coût et fort retentissement. Les dénis de service observés dès l'attaque du 7 octobre sont également peu coûteux et peuvent *a minima* perturber la réactivité de l'État. Sans pouvoir faire basculer le rapport de force, ces outils sont incontestablement un appui précieux dans la faculté du groupe à obtenir du renseignement sur les forces israéliennes, propager ses « narratifs » et mener des actions de terreur visant les infrastructures civiles.

En défense, la perturbation du C2 adverse est facilitée par les nombreux masques de la zone urbaine et la proximité entre différentes unités de l'attaquant, qui lui imposent une parfaite gestion du spectre électro-magnétique (coordination des communications, capteurs, brouilleurs) pour ne pas se gêner lui-même (l'armée américaine l'a notamment constaté lors de la bataille de Mossoul). Plus largement, le groupe présente une faible surface d'attaque et de renseignement dans le cyberespace. Il privilégie les télécommunications filaires pour se soustraire aux capteurs israéliens, et est moins présent sur Internet – en tant que groupe régional – qu'une internationale terroriste telle que Daesh. De plus, ses opérations y semblent menées par des proxys ou des soutiens. En 2019, les IDF avaient toutefois ciblé un bâtiment jugé abriter un groupe de hackers à Gaza, constituant une première historique en répliquant immédiatement à une attaque informatique par une frappe cinétique.

La poliorcétique dans le cyberespace

Un second enseignement peut être tiré de la manière dont les belligérants se disputent l'accès à l'opinion publique internationale. Le siège de Gaza se joue ainsi également dans le cyberespace, où la poliorcétique (art d'assiéger les villes) présente des spécificités. Pour le Hamas et les Palestiniens, la diffusion de contenus et la recherche de soutiens dans le monde sont un levier stratégique. Or, la configuration de Gaza évoquée plus haut permet à Israël de couper l'ensemble du territoire d'Internet en ciblant l'approvisionnement en électricité ou les infrastructures télécoms qui passent par son territoire. Les coupures sont donc régulières, en particulier dès les premières heures de l'attaque du 7 octobre ou lors des phases sensibles de l'opération aéroterrestre israélienne comme le début de l'incursion dans la bande de Gaza du 27 au 29 octobre.

Pour contourner ce siège depuis Gaza, les Palestiniens pourraient avoir deux principaux recours. Le premier consiste à employer une infrastructure alternative, notamment via des accords de *roaming* avec un opérateur égyptien (permettant par exemple à des mobiles de se raccorder aux antennes situées à l'ouest de Rafah, solution limitée géographiquement au sud-ouest de Bani Suheila et à un petit nombre d'abonnés simultanément). L'Égypte n'a cependant pas acté un tel accord, ni même l'extension du rayon de desserte de ses antennes limitrophes un temps envisagée. À l'instar de l'Ukraine, la bande de Gaza aurait également pu s'appuyer sur des satellites basse orbite. Cela nécessite cependant l'importation et la mise en place d'équipements au sol qui ne peuvent actuellement passer l'embargo. Le second recours, plus efficace, consiste à utiliser des *e-SIM* (cartes SIM virtuelles) d'opérateurs de pays alliés d'Israël afin de se raccrocher aux stations émettrices-réceptrices frontalières de Gaza et d'exploiter le

réseau mobile israélien disposant d'accords de *roaming* avec ceux-ci. Les sympathisants étrangers de la cause palestinienne, comme les humanitaires, ont ainsi été appelés à fournir des e-SIM occidentales aux Gazaouis pour leur permettre de communiquer à nouveau. Depuis l'extérieur, les Palestiniens bénéficient également d'appuis cherchant à capter l'attention malgré la tentative de maîtrise israélienne. Un groupe hacktiviste iranien est ainsi parvenu à interrompre une chaîne de *streaming* émiratie pour diffuser un faux bulletin d'information sur Gaza dont le présentateur était un *deepfake*. À l'inverse, on notera également qu'une part importante des dénis de service propalestiniens visent des sites de médias et d'actualités israéliens. Si elles ne semblent pas avoir d'effets notables sur la capacité opérationnelle de Tsahal, ces attaques contribuent à en perturber la communication et à augmenter la pression psychologique que le groupe terroriste cherche à mettre sur la population civile.

Enfin, l'accès à l'information de la population assiégée peut quant à lui passer par des moyens plus rustiques : la BBC a mis en place une diffusion radio d'urgence en modulation d'amplitude sur ondes courtes (639 KHz), offrant la possibilité d'émettre sur plusieurs centaines à milliers de kilomètres.

Quand le terrorisme s'arme des moyens cyber

L'observation des modes d'action et des cibles des groupes propalestiniens – dans un cadre temporel dépassant le conflit en cours – révèle un troisième enseignement sur l'emploi terroriste de l'arme cyber-électronique. Dans la logique du mode d'action visant à propager la peur dans la population, ils ciblent délibérément des infrastructures civiles stratégiques : approvisionnement en eau en 2021, attaques par déni de service sur des sites gouvernementaux, médias, banques, municipalités etc. dont certaines relèvent de l'opportunisme anti-occidental de groupes pro-russes (notamment *Anonymous Soudan* et *KillNet*), utilisation de *wipers* (logiciel malveillant détruisant les données présentes sur des supports informatiques) contre diverses sociétés israéliennes depuis novembre 2023. En représailles de ces attaques pour la plupart appuyées, voire menées par des groupes iraniens, des groupes anti-iraniens répliquent en visant également des cibles civiles telles que les transports ferroviaires iraniens par le groupe Indra ou la distribution d'essence par le groupe *Gonjeshke Darande* (« Moineau prédateur » en persan). Ce schéma pourrait conduire à une forme d'escalade dont la limitation pourrait être d'autant plus difficile selon la capacité réelle des États à contrôler leurs instigateurs.

Des effets psychologiques sur la population civile sont aussi recherchés par une forme très agressive de propagande, passant par exemple par le piratage d'annonces publicitaires dans les cinémas israéliens, l'envoi massifs de SMS prétendant que les systèmes radars avaient été piratés, la divulgation de données électorales ou médicales sensibles. Les plus retentissants relèvent de l'exploitation des otages capturés par le Hamas et du détournement de leurs propres comptes sur les réseaux sociaux pour diffuser des messages. Le détournement de l'application *Red Alert* cité plus haut concourt également à ces effets psychologiques en attaquant la confiance de la population dans son système de prévention, voire de protection face aux tirs de roquettes du Hamas.

L'étendue des cibles possibles, essentiellement du ressort du secteur privé, rend la défense d'autant plus difficile pour le pays ainsi attaqué. S'il est en effet envisageable de durcir la protection des systèmes d'arme, l'informatique des municipalités ou des industries sont autant de cibles opportunistes souffrant souvent d'une moindre sécurité. Bien qu'elles se soient intensifiées depuis octobre 2023, on notera que ces attaques d'ampleur stratégique ne suivent pas exactement le rythme tactique des opérations en cours (les données fuitées datent pour la plupart de 2022 et plus tôt). Leur conception et mise en œuvre nécessitent en effet une préparation et un tempo qui s'étale sur plusieurs mois.

Conclusion

Comme dans la plupart des conflits contemporains, les combats entre Israël et le Hamas se déroulent pour partie dans le cyberespace. Dans le cas de cet affrontement du faible au fort, ce nouveau champ de bataille ouvre à une structure subétatique l'accès à des outils lui permettant de compenser en partie son infériorité capacitaire avec un ratio coût-efficacité particulièrement avantageux, bien que les effets ne demeurent pas à même de changer le cours des combats. En cela, ils en complètent l'arsenal de la techno-guérilla.

La non-discrimination des cibles d'attaques numériques, si elle est un marqueur du mode d'action terroriste, est loin de se cantonner à ce mode de combat. Le cas de l'Ukraine, qui a subi plusieurs cyber-attaques visant ses centrales électriques, en est un bon exemple. Face à la quasi-impossibilité d'ériger une cyber ligne Maginot autour de ses infrastructures, Israël a peut-être créé un précédent, en 2019, en frappant un immeuble immédiatement après y avoir localisé des *hackers* en action. Cette boucle de ciblage est rarissime, voire peut-être unique à ce jour. Car, au-delà des questions de droit qu'elle pose (un pirate informatique est-il un combattant ? Une frappe balistique est-elle une riposte proportionnée à un déni de service ?), elle nécessite une

capacité d'attribution d'une grande fiabilité, reposant sur une caractérisation de l'attaque à même de la lier à une localisation précise. Celle-ci implique sans doute une coopération très étroite entre les équipes de lutte informatique défensive (chargées de détecter et caractériser l'attaque) et de renseignement informatique et électronique (à même d'associer des éléments techniques de la couche logique à des indices de la couche physique). Le développement d'une telle coordination pourrait être un axe intéressant en contexte d'affrontement de haute intensité.

Bien pris en compte par l'armée israélienne, l'appui cyber-électronique y semble intégré à la planification jusqu'au niveau brigade, au moins dans les domaines du renseignement et de l'influence. Pour autant, les attaques numériques posent un véritable défi aux armées modernes par l'étendue de leurs cibles – essentiellement civiles et privées dont elles dépendent sans pour autant en avoir la responsabilité – et par leurs moyens de contournement de tout blocus informationnel et d'accès à l'opinion à travers le monde.

Appuyées par des puissances telles que l'Iran, ces actions cyber asymétriques ne doivent pas être éclipsées par le retour de la conflictualité inter-étatique en Ukraine. Elles pourraient bien inspirer, demain, des forces peu scrupuleuses du droit international cherchant à produire des effets à peu de frais.

Crédit photo : gorodenkoff

•— ••— — • ••— •—• •••

Anthony Namor

Anthony Namor (@anthony_namor) est chercheur associé au centre de recherche des écoles de Coëtquidan (CREC). Officier saint-cyrien, il a essentiellement servi et commandé en unités de guerre électronique et de cyberdéfense militaire. Il réalise une thèse sur le combat numérique et la théorie des jeux.

Vous pouvez retrouver son analyse sur « Le combat cyberélectronique russe en Ukraine » sur le site du Rubicon, ainsi que l'épisode du Collimateur auquel il a participé : « Guerre électronique, mode d'emploi« .

Comment citer cette publication

Anthony Namor, « Retour en asymétrie : Que nous apprend le combat cyber-électronique entre Israël et le Hamas ? », *Le Rubicon*, 1 août 2024 [https://lerubicon.org/retour-en-asymetrie-que-nous-apprend-le-combat-cyber-electronique-entre-israel-et-le-hamas/].