LE RUBICON

Cyber-Hezbollah : le « Parti de Dieu » dans les pas du grand frère iranien

Pierre Pahlavi | 24 novembre 2022

Depuis sa création en 1982 sous le patronage du Corps des Gardiens de la Révolution islamique (CGRI), le Hezbollah libanais n'a jamais cessé d'œuvrer comme un relais de la République iranienne au Proche-Orient permettant à Téhéran de rompre son isolement diplomatique et diffuser – par procuration – son influence dans le monde arabe. D'abord limité à un rôle d'auxiliaire de guérilla, la milice de Dieu s'est progressivement métamorphosée en un cyberproxy reproduisant le mode opératoire du grand frère iranien pour mieux étendre la portée du discours idéologique *panchiite* : « Inspiré et affiné avec l'aide de l'Iran, note Ben Schaefer, le Hezbollah a progressivement adapté ses tactiques pour transférer ses activités des théâtres urbains et des champs de bataille traditionnels vers les réseaux informatiques des adversaires régionaux et occidentaux ». À travers l'analyse de ce partenariat irano-libanais et de l'évolution des capacités technologiques du Hezbollah, cet article montre comment une milice locale s'est muée en l'espace de deux décennies en protagoniste influent et sophistiqué du cyberespace.

L'apprentissage de la guerre médiatique (2003 – 2012)

Les parrains iraniens de la milice de Dieu ont très tôt pris conscience de son potentiel en matière d'influence idéologique et de l'opportunité qu'elle pouvait leur offrir pour rejoindre indirectement, mais plus efficacement l'audience proche-orientale. Fondée en 1991 avec des subsides du régime islamique, la chaine TV Al-Manar [en arabe : Le Phare ou Minaret] se positionne rapidement comme « la plus grande et la plus importante société de radiodiffusion au Liban ». La mission que lui confient ses sponsors iraniens est clairement affichée sur le site Web de la chaîne de télévision libanaise : « Al-Manar est la première organisation arabe à coordonner une guerre psychologique efficace contre l'ennemi sioniste [Israël] ». Depuis son lancement, Le Phare n'a jamais déçu les attentes des stratèges iraniens puisque, en plus de servir l'agenda local du Hezbollah, il a permis de relayer efficacement la propagande de Téhéran sans que celle-ci puisse être directement attribuable à la République islamique.

Outre la victoire par procuration sur les forces israéliennes, la guerre des 33 jours a offert aux Pasdarans un banc d'essai pour tester leur doctrine de guerre mosaïque adoptée en 2005. Celle-ci est une approche multifacette et indirecte qui consiste à annuler la supériorité militaire de l'adversaire en évitant le combat frontal et en le menant là où il peut être mis en difficulté incluant le champ médiatique. Hassan Nasrallah et ses lieutenants ont en effet très largement adopté et mis en œuvre les préceptes développés par le Brigadier-Général Mohammad Ali Djafari, commandant du CGRI, qui, quelques semaines après la fin des hostilités, déclare que : « compte tenu de la supériorité technologique de l'adversaire, nous avons utilisé ce qu'on appelle des méthodes de 'guerre asymétrique'. Nous avons effectué les opérations nécessaires et nos forces sont maintenant bien préparées pour cela. C'est ainsi que nous agirons désormais ». À plusieurs égards, la « Deuxième Guerre libanaise » s'est donc avérée moment pivot dans la mutation des conflits contemporains : c'est d'ailleurs à ce moment que les spécialistes comme F. G. Hoffman datent l'émergence de ce qu'ils ont appelé les « guerres hybrides », c'est-à-dire des conflits impliquant l'utilisation coordonnée de moyens militaires et irréguliers/non-conventionnels pour obtenir des gains autant psychologiques que cinétiques ou territoriaux.

À l'assaut du champ de bataille digitale (2011 – 2022)

La guerre Israël-Hezbollah des 33 jours a également marqué le début de l'intense collaboration entre l'Iran et le Hezbollah dans le cyberespace et, en particulier, la réalisation par la milice chiite des avantages stratégiques considérables offerts par la cyberinfluence – un aspect qui est passé largement inaperçu à l'époque. C'est en effet au cours de l'été 2006 que le mouvement libanais lance ses premières cyberattaques – pour l'heure encore très rudimentaires – contre les sites web israéliens et américains. Dès cette époque, les attaques conduites par les cyberactivistes libanais se sont cependant démarquées en ne se limitant pas à de simples actes de sabotage et en étant exploitées comme des opérations d'influence à part entière – c'est-à-dire très largement « concentrées sur la diffusion de la propagande du Hezbollah ». C'est également l'occasion pour la future Cyber-Armée iranienne de tester un mode opératoire qui deviendra sa marque de commerce au cours de la décennie suivante.

Au début des années 2010, plusieurs événements se conjuguent pour favoriser une maturation du système de cyberguerre du Hezbollah sur le modèle de celui des Iraniens. En 2010, la découverte de l'opération Stuxnet, qui neutralise momentanément le programme nucléaire de la République islamique, encourage le CGRI à accélérer le recrutement et la formation d'experts du cyberespace. À son tour, illustrant une logique isomorphique entre partenaires chiites, le développement de la cyberarmée iranienne entraîne, quasi simultanément, la mise sur pied d'une unité d'action électronique au sein du système opérationnel du Hezbollah. Bien que ladite *Hezbollah Cyber-Army* (HCA) commence à opérer activement durant le « Printemps arabe » de 2011, il faut attendre 2015 et les révélations concernant sa campagne Volatile Cedar (ciblant des centaines de serveurs abrités par des organisations israéliennes et américaines) pour que le Mossad et les services de renseignements occidentaux constatent l'apparition d'une entité libanaise distincte et opérationnelle. Comme les activités de cyberespionnage et de cybersabotage, dont elles se distinguent cependant, les opérations de désinformation et de cyberinfluence du Hezbollah visant à modifier la perception d'audiences cibles sont placées sous l'autorité directe de la chaîne de commandement paramilitaire et obéissent à ce titre à la même logique offensive guidant l'ensemble des initiatives de cyberattaque de la milice libanaise. Là aussi, la Hezbollah Cyber-Army reproduit le modèle de la cyberarmée du CGRI.

Dans la seconde moitié des années 2010, la milice de Dieu s'engage plus systématiquement encore dans l'utilisation des médias sociaux à des fins de cyberinfluence, tout en poursuivant en parallèle ses actions plus « classiques » de cyberespionnage et de cybersabotage. Banni par des plateformes comme Facebook, YouTube et Twitter, la HCA développe alors l'habitude d'agir à travers des comptes fantômes ou des comptes par proxy permettant de rejoindre une audience considérablement élargie. Reprenant à son compte une technique du mode opératoire iranien, l'unité de cyberinfluence du Hezbollah diffuse également son message à travers une myriade de cellules basées à l'étranger : le recours à ses complices difficilement traçables et sans liens institutionnels avec l'organisation centrale atteste d'une maîtrise réelle de l'art du « blanchiment d'influence » permettant de se prémunir plus aisément contre les contre-mesures adverses.

Acteur du cyberespace (2022)

Après avoir essentiellement opéré dans l'ombre du grand frère iranien, la HCA jouit aujourd'hui d'un incontestable degré de maturation faisant d'elle une force à part entière du cyberespace. Cela ne l'empêche pas de continuer à être massivement soutenue par la cyberarmée des Gardiens iraniens – ce qui lui a notamment valu d'être qualifiée par le Major-Général Yaakov, ancien conseiller national de sécurité israélien, de « sous-traitant » [« sub-contractor »] du régime iranien. Désormais, la HCA n'en est pas moins considérée par les experts comme une unité « autosuffisante » capable d'opérer de manière autonome. Lui permettant d'agir comme un allié incontournable de l'Iran en matière de cyberinfluence, cette autonomie repose sur un système de désinformation, de manipulation et de recrutement n'ayant rien à envier à celui des acteurs du cyberespace : en plus de ses

stations de télévision et de radio, le Hezbollah gère maintenant plus de 20 sites Web en sept langues (arabe, azéri, anglais, français, hébreu, persan et espagnol) ainsi qu'un vaste réseau composé d'une multitude d'unités proxy agissant sur les médias sociaux à travers lesquelles la milice d'Hassan Nasrallah peut diffuser sa propagande anti-israélienne et anti-occidentale à l'échelle régionale et internationale.

En plus de s'être dotée d'un système de plates-formes cryptées permettant de recruter des cyberactivistes dans tout le Moyen-Orient, mais aussi en Europe et en Amérique du Nord, la HCA met un soin particulier à la formation de ses futurs propagandistes : à cette fin, la cyberarmée du Hezbollah organise régulièrement des camps d'entraînement au cours desquels les stagiaires étrangers sont rompus aux principes fondamentaux de la désinformation – dans le but, à plus long terme, de constituer des « fermes de trolls » et des « armées électroniques » susceptibles de rejoindre les rangs de la coalition numérique combattant aux côtés du Hezbollah et de l'Iran. Une fois formés, les militants sont envoyés dans d'autres pays pour transmettre leurs compétences aux cyberunités locales essaimant ainsi le modèle iranien à travers tout le Moyen-Orient. Parmi les principaux bénéficiaires de ce transfert de savoir-faire figurent les Houthis au Yémen et le Kata'ib Hezbollah irakien. Composée, selon les renseignements américains, de 400 agents, l'unité de propagande numérique du Kata'ib Hezbollah est désormais pleinement opérationnelle et « inonde Facebook de faux comptes et fait la promotion de fausses informations ».

Au-delà du Moyen-Orient, la cyberarmée du Hezbollah collabore de plus en plus avec sa matrice du CGRI pour influencer la vie politique et le processus électoral de plusieurs démocraties libérales aussi bien neutres qu'adverses. Selon la communauté du renseignement américain, les deux acteurs chiites du cyberespace auraient ainsi combiné leurs efforts à ceux de pays alliés (Russie, Chine, Cuba, Venezuela) pour saper les perspectives de réélection du candidat républicain lors du dernier scrutin présidentiel de 2020. La HCA et ses partenaires iraniens sont également soupçonnés de mener des opérations d'information analogues dans plusieurs pays d'Afrique de l'Ouest : comme le souligne Toulu Akerele, consultant en cybersécurité à l'Institut Hudson, ces initiatives ciblant les populations d'origine libanaise vivant dans ces pays constituent une réelle menace et montrent l'étendue de la cyberinfluence acquise par le Parti de Dieu.

Conclusion

Depuis plus de quatre décennies, la République islamique d'Iran et le Hezbollah ont mis en œuvre un partenariat fondé sur la recherche d'avantages mutuels qui trouve aujourd'hui son expression la plus aboutie dans le domaine du cyberespace : Téhéran fournit au Parti de Dieu un soutien financier et une expertise technologique ; tandis que ce dernier apporte sa légitimité locale, sa connaissance du terrain et ses précieux réseaux d'influence pour mieux diffuser leur idéologie commune basée sur le rejet de l'impérialisme occidental. S'inspirant de ses adversaires comme de ses alliés, le cyber-Hezbollah s'est imposé au cours des 20 dernières années comme un acteur autonome du cyberespace capable de planifier et de mettre en œuvre des opérations d'influence sophistiquées tant au Moyen-Orient et dans d'autres régions clefs. La capacité de ce type d'acteurs à travailler en synergie avec ses partenaires et à engendrer à son tour d'autres cyberarmées capables d'émuler ses méthodes d'influence subversives fait craindre que le plus grand défi à l'ordre mondial libéral soit peut-être encore à venir.

Crédits photo : Richard Patterson

•— ••— — • ••— •—• •••

Pierre Pahlavi

Professeur titulaire au Collège des forces canadiennes de Toronto (@College_FAC), Pierre Pahlavi est actuellement directeur adjoint du département des études de la défense. Ses principaux domaines d'expertise et ses publications portent sur les stratégies d'influence, la politique étrangère de l'Iran et les défis hybrides. Son dernier livre sur la révolution iranienne publié aux éditions Perrin en 2017 a reçu le prix Diane Potter-Boès décerné chaque année par l'Académie française pour le meilleur livre sur le Moyen-Orient. Il est un membre actif de l'Observatoire sur le Moyen-Orient et l'Afrique du Nord de la Chaire Raoul-Dandurand, UQAM (Québec).

Comment citer cette publication

Pierre Pahlavi, « Cyber-Hezbollah : le « Parti de Dieu » dans les pas du grand frère iranien », *Le Rubicon*, 24 novembre 2022 [https://lerubicon.org/cyber-hezbollah-dans-les-pas-du-grand-frere-iranien/].