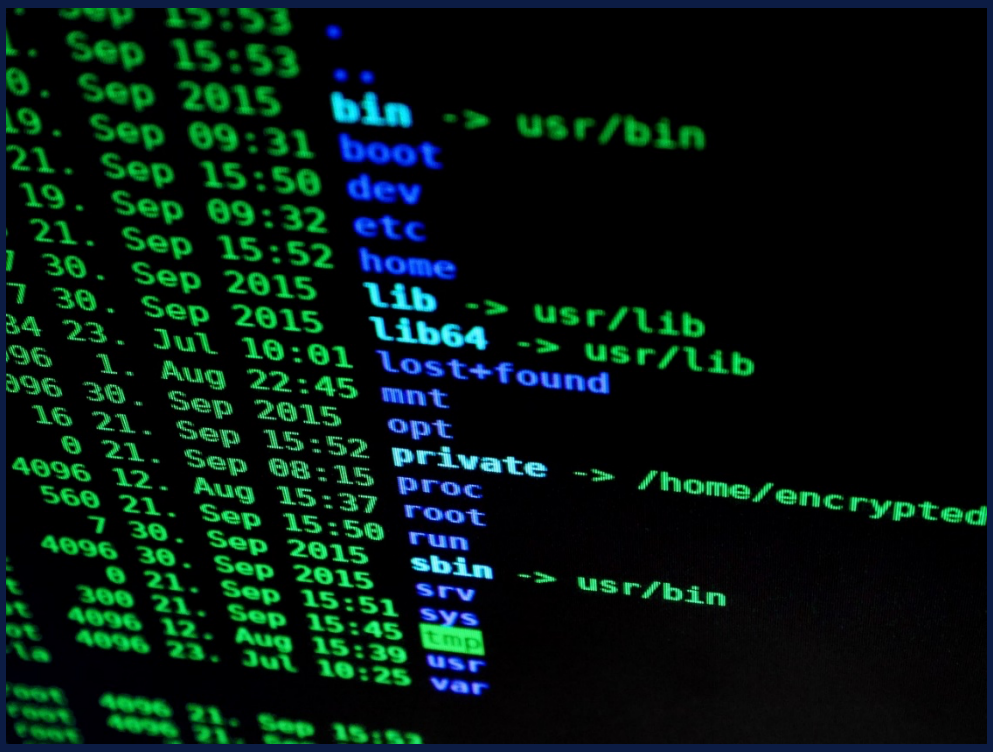
LES PUBLICATIONS

[EN CLAIR]

L'ECOSYSTÈME CYBER AU MOYEN-ORIENT



Par Florian L'écu Leal

LES JEUNES IHEDN

À PROPOS DE L'ARTICLE

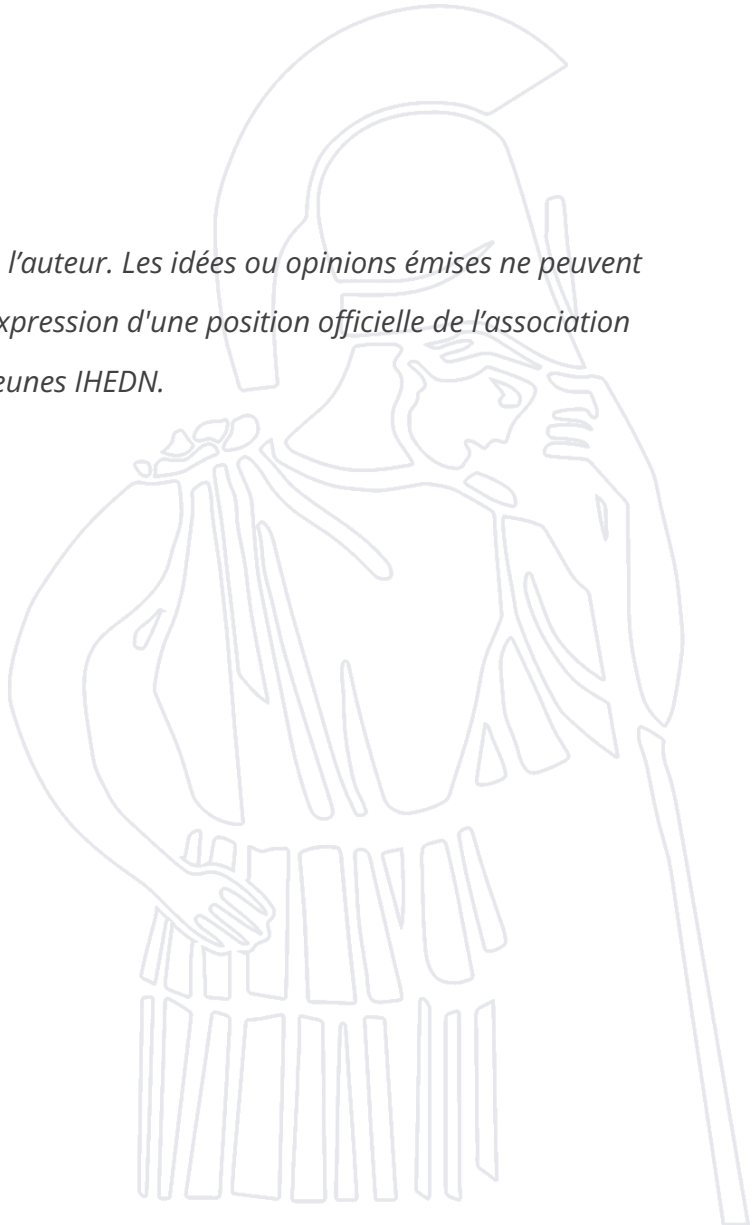
Le cyber [1] est devenu un outil incontournable pour les acteurs des relations internationales. En évolution constante et rapide, il est au cœur de nombreux enjeux de puissance. Cet article propose donc de se focaliser sur l'articulation du cyber au Moyen-Orient, région qui n'échappe pas à la dynamique cyber mondiale.

À PROPOS DE L'AUTEUR

Florian L'écu Leal est étudiant en Master de cryptologie et sécurité informatique à l'Université de Bordeaux. Il a rejoint le comité Moyen-Orient et Monde Arabe des Jeunes IHEDN en 2025.

[1] Le terme cyber représente ici l'ensemble des activités humaines dans le domaine de l'informatique et des réseaux de communications. Il peut s'agir d'activités de recherche et de développement, d'activités liées aux enjeux de défense ou bien encore d'activités à but économique ou politique.

Ce texte n'engage que la responsabilité de l'auteur. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.



La variété des acteurs du monde cyber au Moyen-Orient est à l'image de la multitude d'entités étatiques et non-étatiques qui ont de l'influence dans la région. En raison de leurs moyens plus importants, les États sont les principaux protagonistes de la scène cyber moyen-orientale. Une certaine disparité parmi eux en termes de capacités est tout de même à signaler. Enfin, certains acteurs non-étatiques occupent également une place dans cet écosystème, ce qui leur offre une opportunité de maintenir leur rang de puissance régionale.

Deux acteurs principaux

L'État le mieux doté de la région en matière cyber est Israël[2]. Cette puissance est le fruit de l'application à grand échelle des recommandations de la *National Cyber Initiative*[3], réflexion stratégique sur le cyber conduite par un groupe d'experts israéliens à la demande Benyamin Netanyahou en 2010, pendant de son deuxième mandat. Tant militaire que civile, l'ambition cyber d'Israël s'est construite dans un but large de recherche de sécurité mais également de *leadership* économique dans le domaine. L'*Israel National Cyber Directorate* (INCD)[4], dont la création en 2011 était la principale recommandation de la *National Cyber Initiative*, est l'organisme chargé de la coordination de la politique cyber du pays en lien avec les différents secteurs concernés. Placé sous l'autorité directe du premier ministre, il montre l'importance accordée à ce sujet par le gouvernement israélien. Du côté militaire, la figure de proue des forces armées israéliennes en matière d'opérations cyber est l'Unité 8200[5]. Cette entité est chargée des actions offensives dans le domaine cyber et est capable de collaborer avec des services cybers de très haut

[2] TENEZE, Nicolas. « Israël : la « supériorité numérique » du Moyen-Orient ». *Revue de Défense Nationale* [en ligne], n°784, Novembre 2015 [consulté le 08/02/2025]. Disponible sur : https://www.defnat.com/e-RDN/vue-article.php?carticle=20925.
[3] TABANSKY, Lior et BEN ISRAEL, Isaac. « Seeking Cyberpower : The National Cyber Initiative, 2010. ». Cybersecurity in Israel, p. 43-48, Springer [en ligne], 2015 [consulté le 08/02/2025]. Disponible sur : https://link.springer.com/chapter/10.1007/978-3-319-18986-4_6.
[4] *Israel National Cyber Directorate* [en ligne]. 2025 [08/02/2025]. Disponible sur : https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page.
[5] JOLY, Vinciane. « Israël : qu'est-ce que l'unité 8200, que le Hezbollah dit avoir visée lors de sa riposte ». *La Croix* [en ligne], 26 août 2024 [consulté le 08/02/2025]. Disponible sur : https://www.la-croix.com/international/israel-qu-est-ce-que-lunite-delite-8200-que-le-hezbollah-dit-avoir-visee-lors-de-sa-riposte-20240826.

niveau, comme par exemple la NSA[6] américaine. En effet, ces deux agences sont soupçonnées d'être à l'origine de l'attaque de grande ampleur portée par le virus Stuxnet[7] qui a ciblé le site iranien d'enrichissement d'uranium de Natanz en 2010. D'autres services des forces armées israéliennes complètent le dispositif de l'État hébreux en assurant les missions relevant du spectre défensif. De plus, ces unités, composées à la fois de militaires de carrière et de citoyens israéliens en période de service militaire, permettent un ruissellement des compétences cyber vers le monde civil. Tout d'abord, le domaine cyber y est considéré comme une discipline universitaire à part entière et des formations diplômantes y ont été créées en lien avec l'armée[8]. Israël œuvre également dans la recherche et le développement en la matière, à la fois dans les domaines publics et privés, bénéficiant des connexions déjà existantes entre les deux. Ces connexions sont en effet fortes ; à titre d'exemple, l'acquisition du logiciel espion Pegasus développé par l'entreprise privée israélienne NSO Group[9] fait l'objet d'une approbation par le ministère de la défense d'Israël. Ces efforts sont récompensés, puisque l'État hébreux se classait dès 2014 comme deuxième exportateur mondial de solutions cyber[10] avec un montant de 3 milliards de dollars, derrière les États-Unis. Cette réussite incite ses voisins et compétiteurs régionaux à faire eux aussi des efforts en la matière.

Parmi les autres acteurs régionaux, l'Iran fait également preuve d'ambition en matière de cyber. Un marqueur de cette ambition est la création en 2012 par l'ayatollah Khamenei du *Conseil Suprême du Cyberespace*[11]. Cet organe rassemblant des hauts responsables

[6] La NSA, pour National Security Agency, est l'agence de renseignement technique des États-Unis. Forte d'environ 35 000 employés, son budget annuel est d'environ 10 milliards de dollars.

[7] SANGER, David. « Obama Order Sped Up Wave of Cyberattacks Against Iran ». *The New-York Times* [en ligne], 1 juin 2012 [consulté le 08/02/2025]. Disponible sur : https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[8] DANINO, Olivier. « L'utilisation stratégique du cyber au Moyen-Orient ». *Délégation aux affaires stratégiques, Ministère des Armées* [en ligne], 2013 [consulté le 08/02/2025]. Disponible sur : https://archives.defense.gouv.fr/content/download/205767/2281231/file/EPS2013-Utilisation%20strat%20cyber%20MoyenOrient.pdf.

[9] L'entreprise israélienne NSO Group a été fondée par 3 anciens membres de l'unité 8200. Son logiciel espion Pegasus est conçu pour faire de la collecte de données sur les smartphones en contournant les sécurités des appareils.

[10] MARTIN, Kévin. « Cybersécurité : ambitions israéliennes et positionnement des acteurs de défense ». *Fondation pour la recherche stratégique* [en ligne], 1 février 2016 [consulté le 08/02/2025]. Disponible sur : https://www.frstrategie.org/publications/defense-et-industries/cybersecurite-ambitions-israeliennes-positionnement-acteurs-defense-2016.

[11] PATOT, Jérémie. « Le cyberespace iranien : forteresse technologique à meurtrière interne - 1/3 : La genèse d'internet en Iran ». *Eurasiaspace* [en ligne], 28 novembre 2022 [consulté le 14/02/2025]. Disponible sur : https://eurasiapeace.org/cyberespace-iranien-forteresse-technologique-genese-1-3/.

techniques et politiques de la république islamique a pour vocation de concevoir la politique de l'Iran dans le domaine cyber. Cette politique repose principalement autour de deux axes pour lesquels les doctrines employées sont différentes. Le premier axe de cette politique est la défense contre les menaces cyber venant de l'intérieur et de l'extérieur du pays. Les acteurs de cette politique intérieure sont clairement identifiés et sous les ordres du *Conseil Suprême du Cyberespace.* Pour assurer la défense de ses infrastructures face aux attaques cyber, l'Iran emploie principalement la branche cyber de la *National Organization for Passive Defense*[12] et de quelques unités des forces armées[13]. Le régime iranien exerce également un fort contrôle d'Internet. Il est en effet capable d'opérer des coupures de grandes ampleurs et de restreindre drastiquement les flux de données venant de l'extérieur du pays, capacité dont il a fait la démonstration à plusieurs reprises en 2019 en 2022 lors des grandes vagues de manifestations[14]. Ce contrôle lui est possible car « le réseau iranien est connecté à l'Internet mondial par seulement trois points d'entrée »[15] sous son contrôle. Le second axe de la politique iranienne en matière de cyber concerne des opérations offensives tournées vers l'extérieur et à caractère moins revendiquées. En effet, le régime iranien est soupçonné d'être en lien avec des groupes[16] menants des actions cyber offensives contre des entités concurrentes de l'Iran, à l'image du groupe *CyberAv3ngers*[17] et de son attaque en 2023 contre des composants électroniques israéliens et américains. Cependant, aucune déclaration officielle n'est venue prouver formellement ces accusations. Les groupes en question, catégorisés

[12] La National Organization for Passive Defense est un organisme gouvernemental iranien chargé de la défense civile du territoire et des infrastructures sensibles.

[13] « Cyber Capabilities and National Power : A Net Assessment ». *International Institute for Strategic Studies* [en ligne], 28 juin 2021 [consulté le 14/02/2025]. Disponible sur : https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---iran.pdf.

[14] GOLSHIRI, Ghazal. « Le régime iranien cible les VPN pour limiter l'accès à Internet ». *Le Monde* [en ligne], 10 octobre 2022 [consulté le 14/02/2025]. Disponible sur : https://www.lemonde.fr/international/article/2022/10/07/le-regime-iranien-cible-les-vpn-pour-limiter-l-acces-a-internet_6144812_3210.html.

[15] SZADOWSKI, Michael. « Internet coupé en Iran : « Le niveau de sophistication de ce blocage est une première ». *Le Monde* [en ligne], 20 novembre 20219 [consulté le 14/02/2025]. Disponible sur : https://www.lemonde.fr/pixels/article/2019/11/20/internet-coupe-en-iran-le-niveau-de-sophistication-de-ce-blocage-est-une-premiere_6019883_4408996.html.

[16] SHAMPLE, Steph. « Iranian APTs : An overview ». *Middle East Institute* [en ligne], 10 février 2023 [consulté le 14/02/2025]. Disponible sur : https://www.mei.edu/publications/iranian-apts-overview.

[17] « IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities ». *Cybersecurity and Infrastructure Security Agency* [en ligne], 18 Décembre 2024 [consulté le 22/03/2025]. Disponible sur : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

comme des *Advanced Persistent Threat* (APT)[18], sont plus particulièrement supposés d'être en lien avec le corps des Gardiens de la Révolution Islamique[19]. Néanmoins, malgré ses efforts récents, l'Iran reste vulnérable à certaines attaques comme l'a illustré celle qui a ciblé les stations essences du pays en décembre 2023[20]. Visant les lecteurs des cartes distribuées aux citoyens iraniens pour bénéficier de tarifs subventionnés pour l'essence, l'attaque avait mis hors service plus de 60% des stations du pays.

Des capacités moins importantes parmi les autres États

Outre ces deux principaux acteurs, les pays de la péninsule arabique prennent au sérieux les enjeux cyber et plus particulièrement ceux de cyberdéfense. En effet, la quasi-totalité d'entre eux ont mis en place des *Computer Emergency Response Team (CERT)*[21] pour assurer des missions de défense des infrastructures face aux risques cyber. À défaut d'être des organismes centraux dans leur pays respectif, ces CERT sont réunis au sein de l'Organisation de la coopération islamique[22], un projet dont l'Arabie Saoudite et les Émirats Arabes Unis sont des membres fondateurs[23].

Enfin, il est important de signaler que l'ancien régime syrien de Bachar El-Assad disposait lui aussi de capacités cyber. Sur le plan intérieur, à l'image de l'Iran, il était en mesure d'opérer de grandes coupures Internet comme ce fut le cas en 2012 au début de la guerre civile syrienne[24]. Pour ses actions tournées vers l'extérieur, le régime syrien était

[18] Le terme Advanced Persistent Threat désigne des groupes ou des attaques informatiques d'un haut niveau technique et opérant de manière récurrente.
[19] Le corps des Gardiens de la Révolution Islamique est une organisation paramilitaire placée sous l'autorité directe du Guide supreme. Il possède sa propre armée, sa propre marine et sa propre aviation, et évolue également dans le champ cyber. Il faut néanmoins le distinguer de l'armée de la République Islamique d'Iran qui fait office d'armée régulière.
[20] « Pirates. Qui est derrière la cyberattaque des stations-service en Iran ? ». *Courrier international* [en ligne], 22 décembre 2023 [consulté le 14/02/2025]. Disponible sur : https://www.courrierinternational.com/article/pirates-qui-est-derriere-la-cyberattaque-des-stations-service-en-iran.
[21] Les CERT sont des centres mis en place par des administrations et les entreprises pour réagir en urgence face à des alertes cyber.
[22] L'Organisation de la coopération islamique est une organisation intergouvernementale et confessionnelle qui vise à développer la solidarité entre ses États membres et à favoriser leur collaboration dans les domaines sociaux, économiques et scientifiques. Fondée en 1969, elle compte aujourd'hui 57 États membres.
[23] OIC CERT [en ligne]. 2025, [15/02/2025]. Disponible sur : https://www.oic-cert.org/en/.
[24] SEIBT, Sebastian. « Internet : la Syrie coupée du monde numérique ». *France 24* [en ligne], 29 novembre 2012 [consulté le 15/02/2025]. Disponible sur : https://www.france24.com/fr/20121129-internet-coupure-syrie-ste-black-out-censure-conflit-bachar-assad-rebellion-communication.

soupçonné de soutenir un groupe appelé *Syrian Electronic Army* qui menait des attaques cyber dans le but de promouvoir la propagande du régime[25].

Le Hezbollah et le Hamas : deux protagonistes inattendus

Connus comme deux acteurs incontournables de la région sur de nombreux plans, le Hezbollah et Hamas sont également présents dans le champ cyber. Leurs actions y sont principalement offensives et s'inscrivent à la fois dans le cadre de la lutte cyber mais également dans celui de la lutte informationnelle. Il s'agit plus précisément d'opérations cyber offensives ayant pour but d'alimenter une propagande en leur faveur[26]. Pour enrichir leur campagne de communication, ces groupes mènent des opérations de renseignement et de vol de données en ciblant les vulnérabilités cyber de leurs adversaires. À titre d'exemple, le Hamas est soupçonné par Israël d'être à l'origine de l'attaque qui a visé les smartphones de soldats israéliens pendant la coupe du monde de football en 2018. Cette attaque avait été lancée à partir de trois applications mobiles et avait pour but de récolter les données des téléphones sur lesquels les applications étaient installées, en activant par exemple les micros et les caméras des appareils à distance[27]. Le Hezbollah est, quant à lui, soupçonné d'être derrière la série d'attaque connue sous le nom de *Volatile Cedar*[28]. Initialement découvertes par la société israélienne Check Point en 2015[29], ces attaques ont ciblé des entreprises et des particuliers en implantant dans leurs ordinateurs un virus capable de voler leurs données. L'utilisation du cyber par ces deux

[25] « Le soulèvement syrien à la lumière du cyber ». *Institut français d'analyse stratégique* [en ligne]. [consulté le 15/02/2025]. Disponible sur : http://www.strato-analyse.org/fr/spip.php?article224.

[26] HANDLER, Simon. « The cyber strategy and operations of Hamas : Green flags and green hats ». *Atlantic Council* [en ligne], 7 Novembre 2022 [consulté le 18/02/2025]. Disponible sur : https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats/.

[27] Reuters. « Israel says Hamas tried to snare soldiers in world cup cyber traps ». *Reuters* [en ligne], 3 juillet 2018 [consulté le 18/02/2025]. Disponible sur : https://www.reuters.com/article/technology/israel-says-hamas-tried-to-snare-soldiers-in-world-cup-cyber-trap-idUSKBN1JT247/.

[28] SCHAEFER, Ben. « The Cyber Party of God : How Hezbollah Could Transform Cyberterrorism ». *Georgetown Security Studies Review* [en ligne], 11 mars 2018 [consulté le 18/02/2025]. Disponible sur : https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

[29] BALMAS, Yaniv et DAMSKY, Irena. « Volatile Cedar - Analysis of a Global Cyber Espionage Campaign ». *Check Point Blog* [en ligne], 31 Mars 2015 [consulté le 18/02/2025]. Disponible sur : https://blog.checkpoint.com/security/volatilecedar/.

entités leur permet d'obtenir des effets satisfaisants pour de faibles moyens engagés, et d'ainsi réduire l'asymétrie de puissance entre elles et leurs cibles. D'un autre côté, ces actions forcent les entités touchées, et notamment Israël, à se préparer plus sérieusement à être à nouveau la cible de telles attaques et par conséquent à poursuivre leurs efforts dans le domaine cyber.

Conclusion

À l'image de la région, l'écosystème cyber moyen-oriental reste en constante évolution et est le témoin des dynamiques qui animent la zone. En témoignent les multiples attaques observées le 7 octobre 2023, à la fois sur des infrastructures informatiques israéliennes et palestiniennes[30].

Le cyber, grâce à son coût relativement faible pour les effets qu'il peut produire, ne tient pas réellement compte des différences de moyens financiers entre les acteurs de la région. Dans un Moyen-Orient à l'avenir incertain, il pourrait représenter un domaine dans lequel des protagonistes globalement moins puissants joueraient à armes quasi égales avec les grandes puissances régionales.

[30] YOACHIMIK, Omer et PACHECO, Jorge. « Cyber attacks in the Israel-Hamas war ». *The Cloudflare Blog* [en ligne], 23 octobre 2023 [consulté le 18/02/2025]. Disponible sur : https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/.






publication@jeunes-ihedn.org