Lettre mensuelle – Février 2020 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES (1/2)

LA DÉSTABILISATION DES PROCESSUS ÉLECTORAUX PAR VOIE NUMÉRIQUE

L'élection présidentielle américaine aura lieu le 3 novembre 2020. Alors que le spectre des accusations d'ingérence russe en 2016 plane déjà sur son déroulement, Washington a réaffirmé, par le biais d'une déclaration commune, sa volonté de sécuriser cet évènement[1]. Visant explicitement la Russie, la Chine et l'Iran, le texte met en garde quant aux potentielles interférences et aux tentatives d'influence sur le vote des électeurs. Il précise également qu'il considèrera comme techniques déployées à ces effets les campagnes de manipulation de l'opinion sur les réseaux sociaux et les opérations de désinformation, ainsi que les cyberattaques contre les infrastructures locales et étatiques.

Les techniques susmentionnées englobent tant des actions de lutte informatique offensive (LIO) que de renseignement, et ont pour finalité de conduire un auditoire sélectionné à agir dans le sens d'intérêts et d'un « état final recherché ». Bien qu'elle ne soit pas la seule à avoir fait l'objet de tentatives de déstabilisation, l'élection américaine de 2016 constitue toutefois une référence en la matière. Les intérêts – supposément russes – y étaient notamment de remettre en cause le processus électoral aux États-Unis et l'« état final recherché » de favoriser la victoire du candidat républicain.

Les périodes d'élection sont particulièrement enclines à ce genre d'activités. Entre 2007 et 2017, près de quarante pays auraient vu leur processus électoral faire l'objet d'une perturbation par des cyber-capacités ennemies[2]. À la hausse et ciblant désormais davantage les électeurs que les infrastructures[3], afin d'influencer leur vote, cette dynamique s'expliquerait par la démocratisation des cyber-capacités, l'utilisation accrue des réseaux sociaux et les difficultés d'identification, d'attribution et donc de sanction des auteurs[4].

Une déstabilisation par voie numérique suppose la conduite de plusieurs types d'opérations pouvant viser l'ensemble des étapes et volets d'une élection (composition de listes électorales, organisation de la campagne, modalités de centralisation et décompte des résultats, etc.[5]) Pour l'élection américaine de 2016, elles se sont essentiellement articulées autour du piratage informatique (vol et fuite des courriels du Comité national démocrate) et de campagnes sur les réseaux sociaux (propagation de fausses informations vers des internautes susceptibles de les partager à plus grande échelle). Ainsi, le volet technique d'une opération numérique de déstabilisation vise généralement le dispositif physique des élections **(1)** alors que le volet lié à la manipulation de l'opinion cible directement les électeurs **(2)**.

[1] « Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections », *FBI* [en ligne] 5 novembre 2019.
[2] CST, *Cybermenaces contre le processus démocratique du Canada*, Ottawa, juin 2017, p. 32.
[3] CST, *Cybermenaces contre le processus démocratique du Canada en 2019*, Ottawa, juin 2017, pp. 16-17.
[4] *Op. cit.* CST, juin 2017, p. 32.
[5] « Le processus électoral : permanences et innovations », *Sénat* [en ligne], Paris, 22 novembre 2005.

1. Déstabiliser l'encadrement et l'organisation d'un processus électoral

Certaines opérations conduites en vue de perturber le déroulement ou le résultat d'une élection peuvent comprendre un volet numérique, comme celles présentées ci-dessous qui s'inscrivent dans le cadre de campagnes d'influence russes. Ces dernières ont notamment été accusées de chercher à affaiblir les sociétés ouvertes en exacerbant les clivages sociétaux, à réduire la confiance dans les institutions et à amener la population à remettre en cause le modèle dit « libéral ». Affectant la couche logique du cyberespace, elles constituent un moyen d'obtenir entre autres un accès non autorisé à des réseaux et des systèmes d'information afin d'altérer la disponibilité, l'intégrité ou la confidentialité de données[6].

Le volet technique de ces opérations a notamment pour finalité d'influencer les attitudes, comportements ou décisions d'un auditoire[7]. Leurs effets varient selon la sophistication mise en œuvre dans leur conduite. Les cas étudiés ci-dessous (liste non exhaustive) s'appesantiront sur les niveaux techniques jugés « bas » (défacement), « intermédiaire » (fuite de données) et « haut » (cyberattaque sur des infrastructures critiques)[8].

- Niveau bas : défacement

Dans le cas où un processus électoral prévoit une diffusion en ligne des résultats, cette dernière peut être altérée par une technique de défacement. Cette modification non sollicitée de la présentation d'un site Internet par un pirate informatique peut avoir d'importantes répercussions : semer la confusion chez les électeurs, réduire la crédibilité des autorités quant à leurs capacités à organiser une élection, retarder l'issue du scrutin[9]… Peu sophistiquée, ce type d'opération peut également être réalisé sur un ou plusieurs sites gouvernementaux, en amont d'une élection, afin de discréditer le processus électoral.

Lors de l'élection présidentielle ukrainienne de mai 2014, le groupe russe CyberBerkut s'est introduit dans les réseaux de la Commission centrale des élections. Il y a conduit une attaque de défacement sur le site Internet de cette dernière, en mettant le portrait du candidat d'extrême-droite en position de vainqueur alors qu'il n'avait recueilli en réalité que 0,70% des suffrages. Les administrateurs ont détecté l'anomalie moins d'une heure avant l'annonce officielle des résultats[10]. Bien que cette attaque – si elle n'avait pas été détectée – n'aurait sans doute pas eu d'impact sur l'issue de l'élection, la moindre perturbation aurait éveillé des suspicions sur la légitimité de cette élection et aurait même pu pousser certains citoyens à demander sa réorganisation[11].

- Niveau moyen : altérer l'intégrité, la disponibilité et la confidentialité de données

Les systèmes d'enregistrement en ligne des votes constituent une source de vulnérabilités. Lors de l'élection américaine de 2016, trente-neuf États ont vu leur système faire l'objet d'une intrusion informatique[12]. Des

---

[6] *Droit international appliqué aux opérations dans le cyberespace*, Ministère des Armées, septembre 2019, p. 18.
[7] P. Brangetto, M.A. Veenendaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*, 8th International Conference on Cyber Conflict, NATO CCDCOE Publications, Tallinn, 2016, p. 117.
[8] *Op. cit.* Sean Cordey, p. 15.
[9] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du CAPS et de l'IRSEM, Paris, août 2018, p. 92.
[10] Andy Greenberg, « How an Entire Nation Became Russia's Test Lab for Cyberwar », *Wired* [en ligne], 20 juin 2017.
[11] Nicolay Koval, « Revolution Hacking », *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn, 2015, p. 56.
[12] M. Riley, « Russian Hacks on U.S. Voting System Wider Than Previously Known », *Bloomberg* [en ligne], 13 juin 2017.

cyberattaques peuvent y altérer à la fois l'intégrité des listes électorales, avec par exemple l'introduction de faux électeurs sur les listes pour favoriser le trucage des suffrages, ou la disponibilité des listes électorales, qui peuvent être supprimées et perturber le déroulement du scrutin. Au-delà de leur publication, la revente cybercriminelle des données personnelles des électeurs recensés peut également être envisagée.

Les bases de données des partis politiques sont également des cibles stratégiques. Toujours lors de l'élection américaine de 2016, la Direction générale des renseignements (GRU) de la Fédération de Russie a été accusée d'avoir compromis les systèmes d'information du Comité national démocrate (DNC), puis d'avoir exfiltré des données confidentielles qui ont ensuite été publiées sur WikiLeaks. Couplé à l'utilisation du logiciel-espion X-agent[13], cette opération de doxing a eu pour effet de « *réduire la confiance du public dans le processus démocratique américain, de dénigrer* [Hillary] *Clinton et de nuire à son éligibilité et à sa présidence potentielle*[14] ».

- Niveau haut : cyberattaque sur le système de contrôle industriel d'infrastructures critiques

Des opérations peuvent viser les infrastructures critiques indispensables à l'organisation d'une élection. Bien qu'elle n'ait pas eu lieu en période électorale, le piratage en décembre 2015 d'un réseau de fourniture d'électricité en Ukraine est le seul exemple de cyberattaque d'une telle ampleur. Supposée d'origine russe, elle a causé une coupure de courant de quelques heures dans l'oblast d'Ivano-Frankivsk et a eu un impact sur 1,5 millions d'habitants. Hautement sophistiquée, cette cyberattaque s'est appuyée sur la compromission d'infrastructures par le cheval de Troie BlackEnergy[15]. Ce dernier intégrait un module permettant l'accès aux systèmes de contrôle et d'acquisition de données (SCADA) utilisés par les industries pour piloter leurs installations.

Bien que ces opérations visent essentiellement la couche logique (défacement et doxing) du cyberespace, elles permettent d'avoir un impact psychologique sur la population, difficile à mesurer toutefois. Elles montrent que des effets sont déjà accessibles avec un niveau bas de sophistication. Pourtant, de plus en plus de tentatives d'ingérence ont recours à des techniques moins complexes et basées sur l'ingénierie sociale[16].

2. Manipuler l'opinion des électeurs

Les élections peuvent aussi être déstabilisées par des opérations qui ciblent la couche cognitive du cyberespace. Relevant dans ce cas de la manipulation d'information, elles se déclinent en outils et techniques qui permettent de perturber ou de consolider un narratif (politique, militaire, etc.), notamment sur les réseaux sociaux. Ces opérations reposent sur la captologie, c'est-à-dire sur l'étude de l'influence de l'informatique et des technologies numériques sur l'attitude et le comportement des individus. En France, les réseaux sociaux constituent la première source d'informations de plus de 40% des jeunes électeurs[17].

[13] Robert Mueller, « U.S. v. Viktor Borisovich Netyksho, et al », p. 4.
[14] Office of the Director of National Intelligence, « Assessing Russian Activities and Intentions in Recent US Elections », National Intelligence Council, 6 Janvier 2017, p. 2.
[15] D. Goodin, « First known hacker-caused power outage signals troubling escalation », *Ars Technica* [en ligne], 4 janvier 2016.
[16] Propos de Klara Jordan, table-ronde intitulée « Déstabilisation des processus électoraux, vers une nouvelle guerre froide ? », FIC 2020, Lille, 30 janvier 2020.
[17] A. Brunel, « Réseaux sociaux et présidentielle : cinq bonnes raisons d'être prudent », *Franceinfo* [en ligne], 15 avril 2017.

- Les réseaux sociaux : un continuum entre média et publicité

Dans le cadre d'élections, certaines activités permettent d'agir sur la perception que porte une population sur la situation politique du pays concerné afin d'orienter son vote. Les réseaux sociaux constituent à cet effet un outil de manipulation à grande échelle car ils permettent de s'adresser à un individu « socialisé » et non « isolé ». Dans le cas où un réseau social soit sa principale voire son unique source d'informations, il est possible qu'un internaute soit enfermé dans une « bulle algorithmique »[18], qui le pousse à ne lire que des contenus partagés par des personnes ayant une tonalité politique et idéologique similaire.

Les algorithmes utilisés par les réseaux sociaux ont été conçus pour ne sélectionner que les publications pertinentes et intéressantes dans l'alimentation du fil d'actualité des utilisateurs. Comparant les contenus dans une perspective de fidélisation, la plateforme analyse les réactions des internautes (« likes », commentaires et partages d'une publication) et de leur réseau[19]. Ils se voient ainsi proposer des contenus similaires et des publicités adaptées à leurs centres d'intérêt[20]. Assurant le continuum entre médias et publicités pour certains, les réseaux sociaux sont considérés pour d'autres comme de véritables « plateformes publicitaires[21] ».

Cette mécanique du contenu ciblé peut être détournée au profit de la désinformation. Perméables à l'introduction de fausses informations, les réseaux sociaux peuvent être utilisées par certaines agences d'influence pour orienter et polariser les débats ou diffuser des rumeurs. L'affaire Cambridge Analytica révèle comment la collecte des données personnelles de 87 millions d'utilisateurs de Facebook a permis d'influencer les votes lors de l'élection américaine de 2016, en promouvant des contenus favorables à l'extrême-droite.

- Outils et techniques d'influence sur les réseaux sociaux

- **Trolling** : Ayant pour objectifs de susciter des polémiques et de semer la discorde, les trolls sont des publications provocatrices et non constructives qui s'efforcent de consolider ou de perturber un narratif, en saturant les plateformes de commentaires. Dans le cadre d'élections, le Trolling est un outil singulièrement efficace pour orienter les débats sur les réseaux sociaux. Outre la propagation de la désinformation, l'amplification ou l'éviction de contenu en ligne légitime, les trolls permettent surtout de polariser les opinions[22]. Le Trolling est le plus souvent impulsé par une organisation, un État ou une institution d'État[23].

  « Fabrique à trolls », l'organisation russe Internet Research Agency (IRA) est accusée d'avoir joué un rôle particulièrement actif lors de l'élection américaine de 2016. Suspectée de promouvoir les intérêts du Kremlin, l'IRA a conduit des opérations d'influence sur les principales plateformes américaines (Facebook, Instagram,

[18] *Ibid*.
[19] Claire Aboudarham, Louis Thibault, « Réseaux sociaux et médias à l'ère des algorithmes : une expérimentation sans fin ? », *Méta-Média* [en ligne], 4 juillet 2019.
[20] Propos de Paul-Olivier Dehaye, table-ronde intitulée « Déstabilisation des processus électoraux, vers une nouvelle guerre froide ? », FIC 2020, Lille, 30 janvier 2020.
[21] Propos de Klara Jordan, table-ronde intitulée « Déstabilisation des processus électoraux, vers une nouvelle guerre froide ? », FIC 2020, Lille, 30 janvier 2020.
[22] H. Agardh-Twetman, A. Fjällhed, H. Nothhaft, J. Pamment, *Countering Information Influence Activities: The State of the Art*, Department of Strategic Communication, Lund University, juillet 2018.
[23] « Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia », NATO Strategic Communications Centre of Excellence, Lettonie, 25 janvier 2016.

Twitter, Youtube). Ces dernières reposaient sur une centaine de citoyens russes[24] qui publiaient des trolls sur des sujets clivants afin d'exacerber les tensions sociales (armes à feu, homosexualité, immigration, racisme, religion, etc.). L'effet recherché de ces opérations était de polariser le débat et de critiquer la candidate démocrate[25].

- **Robot et botnet** : Force de frappe, les robots permettent de densifier de manière significative les actions de Trolling. Capables d'imiter les comportements humains, les robots peuvent réagir aux contenus, ainsi que publier des contenus et des commentaires. Pendant l'élection américaine de 2016, la stratégie d'influence de l'IRA sur Twitter reposait sur la création de faux comptes, dont les narratifs était massivement partagés par des milliers de comptes automatiques contrôlés par un botnet[26]. Quelques dizaines de comptes de l'IRA ont également pu atteindre 150 millions d'internautes américains via Facebook et Instagram à l'aide de robots[27].
- **Médias officiels** : Certains organes de presse sont en réalité contrôlés et utilisés par des acteurs afin de promouvoir et renforcer leurs narratifs. Dénoncés comme instruments de propagande russe par le Parlement européen, RussiaToday et Sputnik se caractérisent par leur volume élevé de publications. Ces derniers ne récoltent pas forcément beaucoup de réactions mais saturent en continu les réseaux de nouveaux statuts. À l'occasion du référendum de 2017 sur l'indépendance de la Catalogne, ces médias ont couvert de manière complaisante le mouvement catalan. Véhiculant de la désinformation quant à une Catalogne indépendante, qui serait favorable aux intérêts russes, leurs narratifs ont été amplifiés par les versions hispanophones qui ont trouvé une réelle résonnance en Amérique latine (Venezuela)[28].

La déstabilisation par voie numérique d'un processus électoral comprend un volet technique et de manipulation de l'opinion. Certaines opérations visent directement le dispositif physique d'une élection et permettent de décrédibiliser les autorités publiques quant à leur légitimité d'encadrer un scrutin. D'une sophistication variable, elles ont pour effet de réduire la confiance que porte la population envers ses institutions, voire de conduire à la réorganisation d'une élection. Centrées sur l'ingénierie sociale, d'autres opérations ont lieu sur les réseaux sociaux et ciblent directement les électeurs. Déployant une gamme diverse d'outils (Trolling, botnet, etc.), elles tirent profit des difficultés d'attribution pour influencer sur les votes.

[24] K. Cobiella, B. Popken, « Russian Troll Describes Work in the Infamous Misinformation Factory », *NBC News* [en ligne], 16 novembre 2017.
[25] R. Broderick, « Here's Everything The Mueller Report Says About How Russian Trolls Used Social Media », *BuzzFeed News* [en ligne], 18 avril 2019.
[26] *Ibid*.
[27] *Op. cit.* J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, août 2018, p. 87.
[28] *Ibid*., p. 96.

ANALYSES (2/2)

IRAN ET SOUVERAINETÉ NUMÉRIQUE : LE PROJET SHOMA

Lors des manifestations de novembre 2019 contre la hausse du prix de l'essence, l'Iran a réalisé une coupure volontaire et maitrisée de l'internet sans précédent de plusieurs jours, démontrant par la même le niveau de contrôle qu'exercent les autorités sur les infrastructures et réseaux de télécommunications en Iran à travers le projet SHOMA et la mise en œuvre d'un intranet national[29].

Le projet SHOMA qui se traduit principalement par la mise en place d'un intranet national, le « National Information Network » (NIN) est un projet mis en place par les autorités iraniennes dès 2006[30]. Son développement a été confié en 2007 au Centre de Recherche en Télécommunication (ITRC). Il a officiellement pris le nom de SHOMA (« VOUS » en français) dans le cadre du 5ème plan de développement quinquennal (2011-2016). Instruments de la politique de souveraineté numérique de l'Iran, le projet SHOMA et le réseau NIN suscitent cependant la controverse au sein même du pays, accusés d'être utilisés par les autorités pour censurer et contrôler les citoyens et les entreprises. Dans ce contexte, la coexistence d'un réseau national aux côtés du réseau internet global place de fait les autorités face à un véritable un dilemme dont la résolution pourrait alimenter encore cette méfiance. Elles ont en effet le choix entre simplement imposer par la force aux utilisateurs iraniens une stricte séparation entre l'intranet national de l'internet global d'une part, ou de façon plus subtile, inciter les utilisateurs à privilégier l'utilisation du réseau national et des plateformes nationales sur les réseaux et plateformes de l'internet global… mais sans certitude toutefois d'y parvenir.

SHOMA, instrument de la politique de souveraineté numérique

Le projet SHOMA doit permettre à l'Iran d'avancer vers la souveraineté numérique, à la fois en développant son propre réseau internet national et en se dotant d'un écosystème numérique propre (opérateurs et fournisseurs d'accès étrangers ou encore les plateformes comme les GAFAM par exemple) lui permettant de limiter sa dépendance à des prestataires étrangers.

Plus particulièrement, le projet SHOMA a été conçu pour :

- Offrir à 60% des familles et des entreprises iraniennes l'accès à la fois à l'internet global et à l'intranet national à l'horizon 2016 ;
- Héberger l'ensemble des communications des organes gouvernementaux et des services publics (développement d'un « e-gouvernement ») ;
- Faire transiter toute demandes d'accès aux informations hébergées dans des datacenters iraniens provenant de l'intérieur du pays ;
- Encourager les entreprises à utiliser des datacenters localisés sur le territoire national plutôt que des datacenters étrangers ;

[29] 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
[30] https://smallmedia.org.uk/sites/default/files/u8/IIIP_March2014.pdf

- Encourager les utilisateurs à utiliser des services et applications et solutions nationales : réseaux sociaux, email, moteur de recherche, hébergement, etc. Deux moteurs de recherche, ont été développés jusqu'ici – parsijoo.ir (جو پارسی) et yooz.ir (یوز) – ainsi qu'une vingtaine d'applications comme *Soroush*, équivalent de *Telegram*.
- Renforcer techniquement la résilience de l'intranet national en décentralisant l'architecture réseau.

L'architecture de SHOMA : permettre l'accès à l'internet global tout en privilégiant l'utilisation du réseau national

Concrètement, la mise en œuvre du projet SHOMA repose sur :

- Le développement d'importantes capacités nationales en matière d'infrastructure : fibre optique, téléphonie et internet mobile, communications satellitaires… D'après le site du Ministère de l'ICT, plus de 80% des équipements réseaux sont ainsi produits nationalement par la *Telecommunication Company of Iran* ;
- Le développement d'un réseau national (National Information Network) accessible depuis l'intérieur du pays qui permet aux internautes iraniens d'utiliser des plateformes nationales mais aussi d'accéder à l'internet global. Le réseau national et l'internet global ne sont donc pas physiquement séparés, les internautes iraniens utilisant les mêmes infrastructures nationales (opérateurs de télécommunications et fournisseurs d'accès) pour accéder aux deux réseaux.

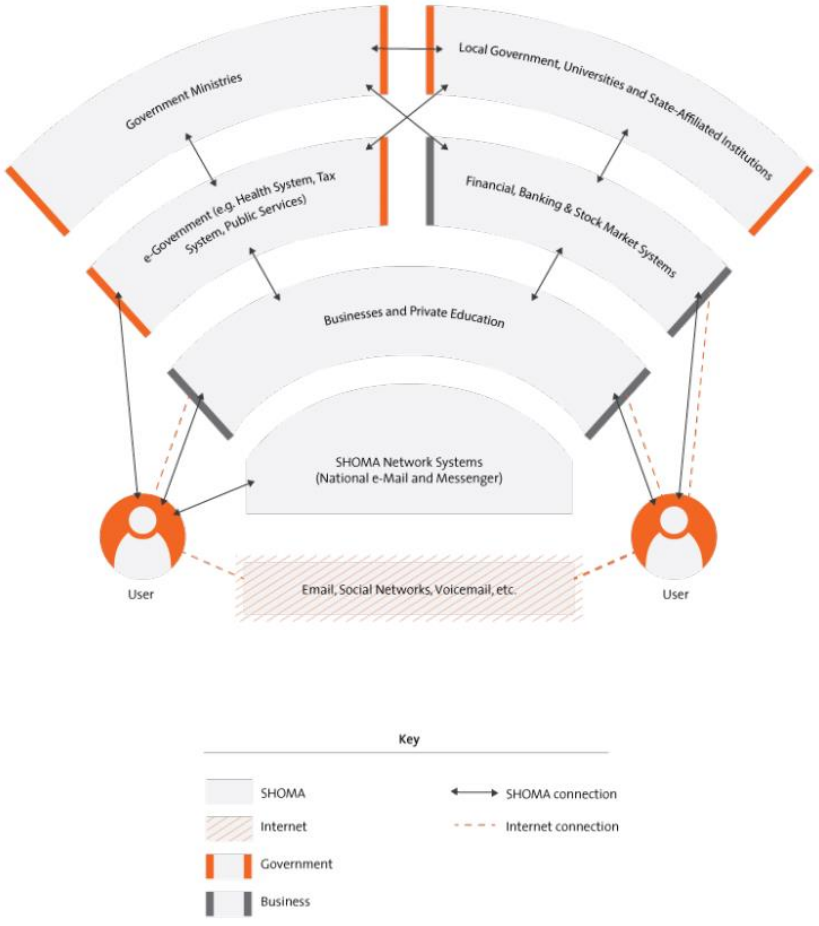

Figure 1 - Les relations entre l'internet global et l'intranet national (Source : SmallMedia)

Selon la figure ci-dessus :

- L'intranet national est utilisé par les utilisateurs pour accéder aux plateformes nationales gouvernementales ou des entreprises iraniennes ;
- L'internet global est utilisé par les utilisateurs pour accéder aux plateformes étrangères ou nationales mais ne peut pas servir à se connecter aux plateformes gouvernementales ;
- L'intranet national est utilisé par les entreprises iraniennes pour se connecter aux plateformes gouvernementales.

Ainsi, s'agissant de l'accès à l'internet global, le pays a fait le choix du contrôle des flux, avec un nombre limité de systèmes autonomes[31] connectés au réseau Internet mondial par lesquels transitent la majorité du trafic depuis et vers l'Iran. Les trois entités auxquelles appartiennent ces AS sont :

- **L'Information Technology Company**, filiale de la Telecommunication Company of Iran (TCI). Cette dernière appartenait aux Gardiens de la Révolution (IRGC) de 2009 à 2018, avant que ceux-ci s'en retirent suite au retour des sanctions américaines.
- **La Telecommunication Infrastructure Company,** affiliée au Ministry of Information and Communications Technology (ICT). Elle est l'unique fournisseur d'infrastructure de télécommunication à l'ensembles des opérateurs publics et privés en Iran.
- **L'Institute for Research in Fundamental Sciences (IPM)**, affilié au Ministry of Science, Research and Technology. Il s'agit historiquement de la première organisation iranienne à avoir été connectée à Internet et à avoir fourni une connexion à la nation.

En ce qui concerne l'accès au réseau national, le pays a fait le choix de la résilience, avec une faible centralisation des flux[32] : il s'agit d'éviter de créer des points de défaillance, donc d'éviter de faire transiter le trafic par un nombre trop limité d'AS pour en rendre plus difficile la prise de contrôle. L'Iran a volontairement laissé s'opérer cette décentralisation des flux, à l'opposé de certains autres pays de la région, qui maintiennent au contraire une centralisation forte (Arabie Saoudite, Égypte, Israël et Turquie notamment).

Ce choix d'architecture s'explique par la double volonté de :

- Mieux contrôler l'utilisation des infrastructures de télécommunications au sein du pays, notamment afin de réduire les risques de piratages ou dysfonctionnement venant tant de l'internet global que de l'intérieur du pays et qui seraient susceptibles de déstabiliser les infrastructures et plateformes iraniennes ;
- Renforcer dans le même temps l'utilisation de ces plateformes et solutions nationales par les internautes iraniens.

D'ailleurs, afin de privilégier l'intranet national et l'utilisation des plateformes nationales, les autorités ont :

- D'une part, imposé une réduction de la bande passante vers l'internet global, ce qui a pour effet de ralentir la connexion à ce dernier depuis l'intérieur du pays ;

[31] Système autonome

[32] The geopolitics behind the routes data travels: a case study of Iran. Loqman Salamatian, Frederick Douzet, Kevin Limonier, Kavé Salamatian : https://arxiv.org/abs/1911.07723

- D'autre part, demandé aux opérateurs de télécommunications et fournisseurs d'accès de réduire de moitié les tarifs d'accès aux contenus hébergés sur le réseau national, ce qui a pour objectif de rendre les plateformes nationales plus attractives que plateformes étrangères[33].

SHOMA, un instrument controversé à la croisée des chemins

Mieux contrôlé par les autorités que son pendant russe le Runet[34], mais moins performant et stable que l'internet chinois, le réseau national suscite dans son utilisation la controverse au sein même de l'Iran.

Un outil de la censure d'État

En pratique, la mainmise des autorités sur les opérateurs de télécommunications et fournisseurs d'accès iraniens leur permet depuis longtemps de contrôler l'accès de la population à l'internet global, notamment en filtrant les contenus ou encore en bloquant l'accès à certaines plateformes étrangères. À mesure que le projet SHOMA s'est développé, le contrôle des autorités iranienne n'a cessé d'augmenter et a pris de nouvelles formes, par exemple via le contrôle des fournisseurs de VPN pour limiter les possibilités de contournement des dispositifs de censure.

La coupure opérée par les autorités lors des évènements de novembre 2019 a d'ailleurs démontré l'étendue et la sophistication du contrôle des autorités iraniennes, tant sur l'internet global que sur le réseau national[35]. Ainsi, le dispositif de contrôle des opérateurs et fournisseurs d'accès mis en place par le projet SHOMA a permis aux autorités de couper très rapidement (environ 24 heures) et avec précision les accès à l'internet global au réseau national, ainsi que les communications mobiles, sur une période d'une dizaine de jours[36]. Néanmoins, le dispositif mis en œuvre reste difficile à déterminer en l'absence d'éléments concrets sur la manière dont les autorités peuvent contraindre les opérateurs et fournisseurs d'accès (engagement de la responsabilité des prestataires en cas de refus ou intervention directe des autorités chez les prestataires par exemple). Cette capacité inédite de contrôle de l'internet et sur les internautes suscite de plus en plus de craintes de la part de la population iranienne[37].

Un intranet national encore relativement fragile

Si, à travers le projet SHOMA, l'Iran cherche à imposer à sa population d'utiliser des services et applications numériques nationales comme le fait la Chine, il n'en demeure pas moins que ces dernières ont peu de succès et que la majorité de la population iranienne préfère utiliser des applications étrangères comme WhatsApp par exemple, par souci de qualité des services ou encore de protection des données contre la surveillance des autorités sur les plateformes nationales[38]. Dans ce cadre, la récente coupure de l'internet et du réseau national iranien sont susceptibles d'accentuer encore le manque de confiance, voir une certaine défiance, de la

[33] http://www.mehrnews.com/news/3970276
[34] OMC, Le Runet, construction politique ou réalité technique ? Lettre n° 69 – Décembre 2017
[35] https://netblocks.org/reports/internet-restored-in-iran-after-protest-shutdown-dAmqddA9
[36] https://information.tv5monde.com/info/iran-le-pays-est-desormais-capable-d-effectuer-une-coupure-controlee-de-son-reseau-334033
[37] https://www.independent.co.uk/news/world/middle-east/iran-internet-shutdown-protests-communications-tehran-a9226731.html
[38] https://www.telegraph.co.uk/news/2019/11/23/irans-internet-blackout-happening-did-government-turn/

population envers les autorités et envers le projet SHOMA, pouvant entrainer par la même une baisse d'utilisation des services et applications nationales. Les autorités se laissent malgré tous les moyens d'imposer une sorte d'« apartheid digital »[39] consistant à couper l'accès à l'internet global de façon sélective, par exemple pour la population mais pas pour le Gouvernement ou certains opérateurs (comme les banques) qui ont besoin de conserver un accès à l'internet global.

Cette approche risque toutefois d'entrer en contradiction avec l'objectif même du projet SHOMA, dont l'ambition était de pouvoir offrir aux utilisateurs iraniens un réseau national solide en complément de l'accès à l'internet global, et non, comme cela semble être le cas aujourd'hui, développer un réseau national tout en coupant les communications des entreprises et des citoyens iraniens à l'internet global. Dans ce contexte, le projet est « à la croisée des chemins » et les autorités doivent décider de :

- Suivre le modèle chinois en accentuant la logique d'« apartheid digital » et de contrôle de l'internet, en obligeant toujours plus les entreprises et les citoyens à utiliser les solutions nationales et le réseau national. Cependant, cette solution pourrait entrainer des difficultés économiques pour les entreprises iraniennes déjà dépendantes de l'internet global[40] et remettrait en cause le projet initial. Enfin, cette solution marquerait un net recul des libertés en Iran et renforcerait davantage la méfiance actuelle ;
- Ou revenir sur la politique de blocage de l'internet et du réseau national en privilégiant plutôt une politique d'influence destinée à inciter les citoyens et les entreprises à privilégier les solutions et le réseau nationaux.

En définitive, l'Iran a réussi à délimiter les contours de son réseau national au sein de l'internet global en contrôlant dès le début les infrastructures nécessaires au fonctionnement de l'internet et en développant des services et applications nationales. Cependant, une faille demeure : l'interconnexion de base entre le réseau national et l'internet global qui permet aux utilisateurs iraniens de bénéficier de services et applications étrangères plus attractives et plus performantes. Inverser la tendance dans les usages d'internet et du réseau national constitue alors un véritable défi pour l'avenir de SHOMA.

[39] http://www.rfi.fr/fr/moyen-orient/20190210-iran-internet-halal-republique-islamique-cyberespace-shoma-censure
[40] https://theglobepost.com/2020/01/13/iran-internet-paradox/

FOCUS INNOVATION

Tarides, développeur d'applications sécurisées par construction

Présentation

Fondée en janvier 2018, Tarides est le fruit d'une collaboration entre quatre chercheurs de l'Université de Cambridge (Thomas Gazagnaire, Gemma Gordon, Anil Madhavapeddy et KC Sivaramakrishnan), expert(e)s dans le développement de systèmes d'exploitation et d'infrastructures open-source. La startup regroupe une vingtaine de personnes qui travaillent à la mise au point d'un nouveau type d'OS spécialisé qui permet de développer des applications sécurisées par construction, performantes et décentralisées.

L'innovation

La solution logicielle OSMOSE permet de déployer une plateforme IoT sécurisée, distribuée, performante et centrée sur l'utilisateur. En s'appuyant sur les systèmes décentralisés et les unikernels, plus particulièrement le logiciel MirageOS (fruit de plus d'une dizaine d'années de recherche), OSMOSE rompt avec les solutions IoT traditionnelles de smart-building pour la maintenance et l'optimisation. Utilisant le cloud comme point central de leur architecture, ces dernières ne sont en effet pas adaptées aux cas d'usage futurs qui nécessitent une latence faible et une sécurité forte des données.

La technologie

Les technologies déployées par la solution OSMOSE sont open-source (OCaml, MirageOS et Irmin).

L'actualité

Après avoir remporté le prix i-Lab en 2019 et le prix coup de cœur du FIC2020, Tarides continue ses activités innovantes en se focalisant en 2020 sur le développement d'une infrastructure open-source dédiée aux objets connectés.

CALENDRIER

18/03/2020 : Petit-déjeuner thématique « Radioscopie des cybermenaces 2020 »

Organisé par CEIS au profit du COMCYBER, un petit-déjeuner sur le sujet "Radioscopie des cybermenaces 2020" aura lieu le 18 mars au CEIS Lab (40 rue d'Oradour-sur-Glane, 75015 Paris), de 8h30 à 10h30.

L'étude des attaquants et de leurs modes opératoires est essentielle aux organisations pour anticiper les futures attaques et adapter leurs capacités de détection et de réaction. La menace évolue et se transforme en effet à mesure que l'environnement numérique et ses usages se diversifient et se complexifient (cloud, IoT, 5G…). Au regard des évolutions observées au cours de l'année écoulée, quelles sont les grandes tendances observables en matière de TTPs (Techniques Tactiques Procedures) employées par les attaquants ? Au-delà de l'analyse technique, quelles sont les évolutions notables du « Cyber Threat Landscape » en termes d'attaquants, de motivations, de cibles ? Que peut-on déduire, à court et moyen terme, sur les menaces pesant sur les armées et leurs actions dans le cyberespace ? Rançongiciels, ciblage des chaines de sous-traitance, va-t-on vers une incidentologie quotidienne ?

La liste des intervenants sera disponible prochainement.

Pour toute demande d'inscription ou d'information complémentaire, contacter Amélie Rives : arives@ceis.eu

ACTUALITÉ

DGNUM : 2 ans de Transformation numérique

La Direction générale du numérique et des systèmes d'information et de communication (DGNUM) a organisé le 25 février la 2e édition de son évènement dédié à la transformation numérique du ministère des Armées.

Cette journée d'échanges a été l'occasion d'appréhender les concepts clés et les grands enjeux de la transformation numérique. Les thèmes traités cette année ont été ceux de la souveraineté numérique, de l'agilité et du cloud de confiance. Entamées il y a deux ans, afin de faciliter le quotidien des soldats et des agents du ministère, que ce soit en France ou sur le terrain, les effets de la transformation numérique ont également été abordés, ainsi que les nouveaux objectifs en matière de compétences et de conduite de projets.

Par le biais de présentations, cet évènement a permis de mettre en avant certaines entreprises issues de l'écosystème partenaire du ministère des Armées, telles que Thales (atelier sur l'identité numérique – « Connaître l'interlocuteur »), Saagie et Capgemini (atelier « Pour un ministère data-driven » sur la donnée et la mise en œuvre d'une plateforme dédiée). Cette dernière a notamment présenté sa plateforme POCEAD (ouverture, centralisation, exposition et analyse de données), qui montre comment la généralisation du Big Data, du cloud et de l'intelligence artificielle contribue à la transformation numérique des métiers du ministère.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com