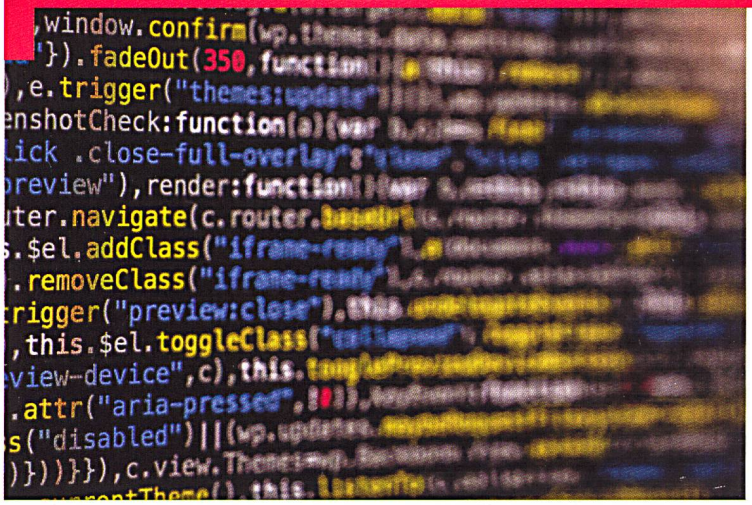
Zeitschrift: Revue Militaire Suisse
Band: - (2018)
Heft: 6

Artikel: Le rôle de la cyber threat intelligence dans la prévention des cyber-attaques et de la guerre d'information dans les élections
Autor: Baezner, Marie
DOI: https://doi.org/10.5169/seals-823426



Les campagnes d'influence représentent un épineux problème pour les démocraties qui doivent maintenir la liberté de parole et éviter la censure. Source : unsplash.com.

Renseignement

Le rôle de la *cyber threat intelligence* dans la prévention des cyber-attaques et de la guerre d'information dans les élections

Officier spécialiste Marie Baezner

Avec les élections de 2016, les démocraties ont réalisé que le vote, le processus qui est l'essence-même de la démocratie, pouvait être menacé par les cyberattaques. Plusieurs Etats sont même revenus au vote papier pour éviter les risques de cyberattaque. Cependant, revenir au papier n'est pas suffisant car les menaces visants les processus démocratiques sont complexes et doivent être traitées avec une approche complète. La *cyber threat intelligence* qui regroupe plusieurs sources du renseignement joue un rôle important dans la prévention des cyberattaques et des campagnes d'influence en ligne dans les processus démocratiques.

Vulnérabilités des élections face aux cyber-attaques et à la guerre d'information

En théorie, les processus de vote ou d'élections comportent plusieurs vulnérabilités dans le domaine cybernétique que des acteurs malveillants peuvent exploiter, Shackelford et al. (2017) en listent cinq. La première réside dans les informations que reçoit l'électeur. Ces informations peuvent être modifiées ou falsifiées pour influencer l'opinion de l'électeur. Cette vulnérabilité relève de la guerre de l'information et n'est pas spécialement technique ni réservée au cyberespace. La guerre d'information et les campagnes[1] d'influence ont toujours existé, la nouveauté réside donc dans le fait qu'elles se sont adaptées aux nouvelles technologies. La deuxième vulnérabilité concerne les bases de données d'électeurs. Celles-ci peuvent être piratées, modifiées ou rendues inutilisables pour empêcher certaines personnes de voter ou pour ralentir le processus de vote. Cette vulnérabilité est principalement technique et relève de la protection des données. Les listes d'électeurs doivent être suffisamment bien protégées pour empêcher leur altération. La troisième vulnérabilité relève des technologies de vote. Certains Etats possèdent des appareils de vote électronique et d'autres votent par Internet. Dans les deux cas, ces techniques de vote peuvent être la cible de cyberattaque visant à modifier les résultats. La quatrième réside dans les logiciels de comptage des votes. Ces logiciels peuvent être piratés et les résultats modifiés. La dernière vulnérabilité concerne le moyen d'acheminement des résultats aux instances officielles qui les diffuseront. Suivant la technique utilisée par l'Etat, elle peut être piratée et les résultats peuvent être interceptés et modifiés puis diffusés à la place des vrais résultats. Si les résultats sont diffusés avant la fermeture des bureaux de vote, cela risque d'influencer le vote des électeurs qui doivent encore voter.

Une cyberattaque ou une campagne de désinformation n'a pas besoin de réussir pour être efficace. Il suffit que la nouvelle de l'attaque soit rendue publique pour qu'elle instille le doute sur la crédibilité et la légitimité du processus démocratique. Un candidat donné perdant pourrait attaquer les résultats en arguant que la cyberattaque a modifié les scores ou que les informations reçues par les électeurs étaient biaisées.

Deux approches

La lutte contre les attaques utilisant des moyens cybernétiques pour nuire aux processus démocratique peut prendre deux approches. La première est considérée comme étroite et ne concerne que les aspects techniques du processus de vote. L'approche étroite ne se préoccupe donc que de la sécurité des éléments techniques, c'est-à-dire des bases de données des électeurs, des machines de vote électronique ou plateformes de vote par Internet, des logiciels de comptage et des moyens de transmission des résultats. Cette approche s'assure que ces éléments sont les plus sûrs et résistants possibles aux cyberattaques. Cependant, cette approche n'est pas suffisante. Comme il a été démontré lors des élections américaines de 2016,

1 Les campagnes d'influence sont généralement des séries d'opérations coordonnées cherchant à accomplir un ou plusieurs objectifs stratégiques sur le long terme.

la technologie impliquée dans le processus de vote n'est pas la seule concernée par les risques d'ingérences étrangères. L'approche large comporte la protection de tous les éléments techniques du processus démocratique, mais elle inclut aussi les informations que reçoivent les électeurs et donc la guerre d'information. L'approche large comprend ainsi des mesures pour faire face aux menaces visant la technologie et la société. Un Etat qui souhaite protéger ses processus démocratiques a donc intérêt à opter pour une approche large.

Cyber threat intelligence

La *cyber threat intelligence* est la réunion et l'analyse de diverses sources du renseignement pour cartographier et établir un profil précis des menaces dans le cyberespace. Pour établir ces profils, la *cyber threat intelligence* a recours à des informations techniques telles que les indicateurs de compromission, les noms de domaines ou les adresses IP, et aussi à d'autres sources du renseignement telles que le renseignement *open source* (OSINT), l'étude des médias sociaux ou le renseignement humain (HUMINT), pour n'en citer que quelques-unes. Dans la *cyber threat intelligence*, le partage d'information entre agences de renseignement ou même entre Etats est important pour établir un profil précis des menaces. L'objectif de la *cyber threat intelligence* est de recouper les informations pour se faire une image la plus précise possible d'un attaquant, ses techniques, ses buts et ses capacités. Ces analyses servent à trouver des tendances ou des vulnérabilités dans son comportement ou ses activités pour ensuite mieux pouvoir se défendre et anticiper suffisamment tôt ses nouvelles attaques.

Cyber threat intelligence dans l'approche étroite

Dans l'approche étroite de la protection des processus démocratiques contre les menaces cybernétiques, la *cyber threat intelligence* joue un rôle important. L'approche étroite se focalisant sur les éléments techniques des processus démocratiques, les services en charge de leur protection doivent s'attendre à ce qu'ils soient attaqués. Par conséquent, le recours à la *cyber threat intelligence* permet d'anticiper ces attaques en établissant les profils les plus détaillés possible des type de menaces pour ces éléments techniques, pour organiser leur surveillance, repérer toutes activités suspectes et les arrêter ou atténuer leurs effets le cas échéant.

Cyber threat intelligence dans l'approche large et ses limites

Cependant, dans l'approche large, la *cyber threat intelligence* reste utile pour contrer les cyberattaques contre les éléments techniques des processus démocratiques, mais a plus de difficulté à contrer les attaques qui ne sont pas d'ordre technique à proprement parler. Ces attaques cherchent à influencer les opinions des électeurs en visant les politiciens, les partis politiques et les médias (médias sociaux inclus). Ces campagnes d'influence existaient déjà avant l'invention d'Internet. Toutefois, il a permis à ces campagnes de toucher un public plus large et dans

La guerre d'information a toujours existé, elle s'est simplement adaptée aux nouvelles technologies. Source : unsplash.com

n'importe quelle zone géographique. Certaines de ces campagnes d'influence utilisent des moyens techniques, comme le piratage d'ordinateurs de partis politiques et utilisent les informations volées pour essayer d'influencer les votes, comme ce fut le cas lors des élections américaines en 2016 et en France en 2017. Un autre élément technique utilisé dans les campagnes d'influence sont les *social bots*[2] qui permettent de propager de fausses informations, de leur donner de l'importance ou de relayer les informations volées lors de piratages. La *cyber threat intelligence* peut être utile dans la détection de campagnes d'influence sur Internet et sur les médias sociaux, mais cela reste une tâche difficile. La *cyber threat intelligence* collecte et analyse les informations techniques ainsi que les structures des réseaux d'influenceurs et des *social bots*. La *cyber threat intelligence* est une mesure pro-active qui permet de mieux comprendre la mise en place et le déroulement de ces campagnes pour les arrêter suffisamment tôt. Cependant, dans l'approche large, la *cyber threat intelligence* ne peut pas faire face seule aux campagnes d'influence. Ces dernières, en ciblant les politiciens ou les médias, concernent la société toute entière. Les campagnes d'influence représentent un épineux problème pour les démocraties qui doivent maintenir la liberté de parole et éviter la censure, tout en agissant contre elles. Les mesures pour les contrer ne devraient donc pas se limiter aux services de renseignement et à la *cyber threat intelligence*, mais inclure des mesures à tous les niveaux de la société, les médias, les industries et l'éducation.

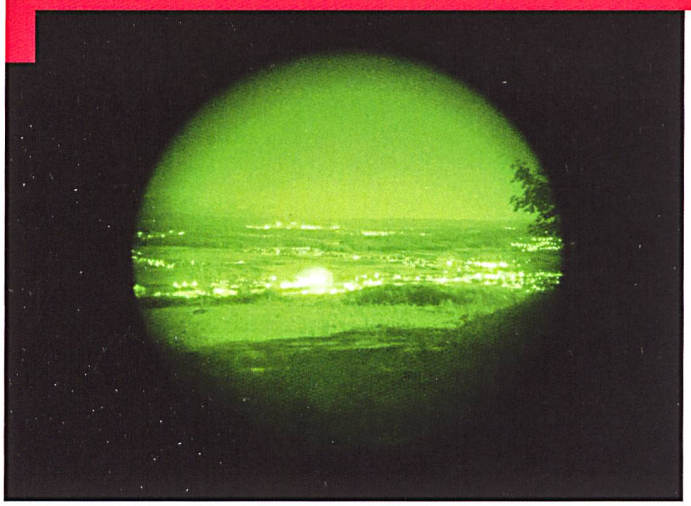
M. B.

Sources:

Shackelford, S., Schneier, B., Sulmeyer, M., Boustead, A. and Buchanan, B. (2017). *Making Democracy Harder to Hack*. University of Michigan Journal of Law Reform, [online] 50(3), pp.629-668. Available at: https://repository.law.umich.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1178&context=mjlr [Accessed 5 Nov. 2018].

Pour plus de renseignements sur le cas de la France, le lecteur peut lire : Baezner, Marie; Robin, Patrice (2017): *Hotspot Analysis: Cyber and Information Warfare in elections in Europe*, December 2017, Center for Security Studies (CSS), ETH Zürich.

2 Un *social bot* est un programme automatisé qui gère des tâches de routine sur les médias sociaux. Les *social bots* peuvent aussi gérer des faux profils d'utilisateurs qui seront utilisés pour partager des messages, des informations et/ou pour envoyer des spams.



Renseignement

France : De la réforme des services de renseignements

Chaouki Triai

Journaliste spécialiste des questions géopolitiques et sécuritaires

Dans de nombreux pays, l'Etat est doté de services de renseignement, c'est-à-dire de services secrets chargés de pratiquer de l'espionnage et du contre-espionnage. Un Etat, quelle que soit sa dimension, se doit de protéger son territoire et faire en sorte qu'il ne soit pas l'objet d'une agression extérieure ou intérieure. Mais pas seulement, car il se doit aussi de défendre les intérêts qui lui sont propres. Par conséquent, le renseignement a besoin de s'adapter aux différentes conjonctures qui traversent les époques.

Le renseignement : Un outil vital

Depuis la fin de la Seconde Guerre mondiale, le renseignement n'a eu de cesse, à l'échelle mondiale, de subir des assauts multiples. Durant la Guerre froide (1945-1989/90) les deux adversaires que représentaient les Etats-Unis d'un côté et l'ex-URSS de l'autre, s'affrontent de manière à positionner leurs influences au gré de l'échiquier de la géopolitique mondiale fluctuante, pour s'affronter avec l'aide de leurs services de renseignement respectifs. Quant à la France, par son histoire de puissance coloniale jusqu'au milieu du XX^{e} siècle et par sa capacité de résistance à l'agression de l'Allemagne hitlérienne, elle a fait du renseignement un outil majeur. D'une part pour maintenir sa puissance coloniale d'antan et, d'autre part, pour lutter contre l'Allemagne nazie qui occupait une partie de son territoire dès 1940.

Les Temps changent et l'Histoire avec

De la décolonisation et jusqu'à notre actualité la plus récente, le renseignement est bousculé par les nouvelles menaces et notamment le terrorisme qui s'est émancipé des frontières en se mondialisant à l'instar de l'économie des échanges planétaires, singulièrement après la chute de l'ex-URSS. Les attentats sur le sol américain en septembre 2001 ont reconfiguré le renseignement dans la lutte contre le terrorisme islamique de manière globale. Il doit désormais s'ancrer dans un réel où le terrorisme est une pandémie qui fait fi des frontières et devient transnationale. Pour ce faire, la France a nécessairement revisité ses moyens de renseignement dans son volet contre-espionnage et donc, son renseignement intérieur. Mais il faut noter toutefois que cette réforme arrive sept ans après les attentats du 11 septembre 2001 aux Etats-Unis et une année après l'arrivée au pouvoir de Nicolas Sarkozy, auparavant ministre de l'Intérieur sous la présidence de Jacques Chirac (1995-2007). C'est avec une détermination sans failles que l'ancien ministre de l'Intérieur allait restructurer le contre-espionnage avec des méthodes parfois spectaculaires. En 2003, il avait diligenté une intervention contre l'Organisation des Moudjahidins du Peuple d'Iran (OMPI) opposée au régime des ayatollahs en Iran dont le siège se trouve en France. Le contre-espionnage, à l'époque la Direction de la Surveillance du Territoire (DST), avait investi les lieux sous le feu médiatique. C'est cette même DST, sous sa présidence, qu'il transformera en Direction Centrale du Renseignement Intérieur (DCRI) en 2008.

De la DST à la DCRI

Trois réformes du contre-espionnage depuis 1945. Cela peut sembler une éternité sachant qu'entre- temps, il y a eu l'effondrement du Mur de Berlin en 1989, la dislocation de l'ex-URSS dès 1990, la Guerre du Golfe en 1991, les attentats américains en 2001, une nouvelle Guerre du Golfe en 2003, etc... La liste n'est pas exhaustive. Sur cette durée, Alain Chouet explique : *« En premier lieu, trois trains de réformes en 60 ans, c'est assez peu considérant des services supposés s'adapter aux évolutions géopolitiques de la planète, qui ont vu successivement dans cette période la liquidation des empires coloniaux, les déstabilisations inhérentes à la Guerre froide, la dissolution du Bloc de l'Est, la montée des affrontements asymétriques dont le terrorisme fait partie »*. Les étapes de l'histoire du contre-espionnage commencent en 1944, soit une année avant la fin de la Seconde Guerre Mondiale. C'est la DST qui en a la

primeur. Autant dire que la DST a présidé les services de renseignement durant un peu plus de 60 ans, soit plus de la moitié d'un siècle. Certes, au cours de son histoire, d'autres officines aidant le contre-espionnage ont apporté aussi leurs concours. C'est notamment le cas de la Direction Centrale des Renseignements Généraux (DCRG) qui a dirigé, à l'échelon local, les Renseignements Généraux (RG). Une direction qui se trouvait dépendre de la Direction Générale de la Police Nationale (DGPN). Une multiplication des services de renseignement, qui du national au local manquaient d'une entité unique et centrale qui rassemblerait la masse d'informations récoltée sur le terrain. Un décloisonnement où la multiplication des responsabilités sans lien unificateur perdait en efficacité. C'est ainsi qu'intervint un changement important en 2008 durant la présidence de Nicolas Sarkozy qui transforme la DST en DCRI.

De la DCRI à la DGSI

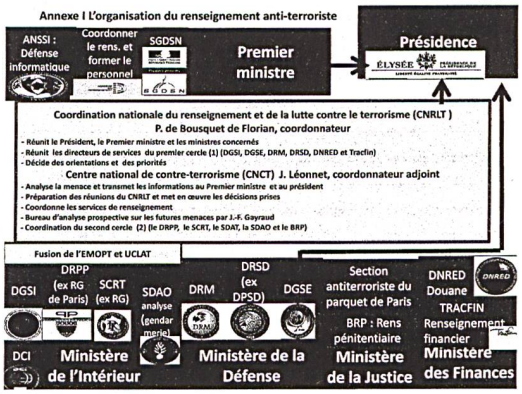
Avec une volonté pugnace, l'ancien ministre de l'Intérieur frappe un grand coup dans la fourmilière du contre-espionnage. Une transformation des services dont l'objectif est l'unification dans l'information et l'action. A ce propos, Alain Chouet souligne : *« Au début des années 2000, il a paru nécessaire de fondre dans un même organisme les attributions judiciaires de la DST (contre-espionnage, contre-ingérence, contre-terrorisme), avec celles (non judiciaires) des Renseignements généraux qui avaient développé une excellente expertise territoriale des milieux dits « à problèmes ». D'où la création de la DCRI (Direction centrale du Renseignement Intérieur) rapidement érigée en DGSI (Direction Générale de la Sécurité Intérieure) »*. Notons que la DGSI est née en 2014 sous la présidence de François Hollande, soit près de six ans après la DCRI et moins d'une année avant les attentats terroristes de Paris en janvier 2015. M. Chouet poursuit : *« Cette transition de Direction Centrale (subordonnée à la Direction Générale de la Police Nationale) en Direction Générale (autonome sous les ordres directs du Ministre) ne signifiait pas de changement dans l'organisme mais seulement une plus grande liberté d'organisation, en particulier pour le recrutement qui peut désormais se faire hors police nationale »*. Pour appuyer sa démonstration, A. Chouet souligne : *« La création de la DCRI a été marquée par une erreur conceptuelle. Il aurait été souhaitable de fusionner totalement les compétences de la DST avec les compétences territoriales des RG. Au lieu de quoi on a fusionné la DST avec les seuls échelons centraux parisiens des RG. Les échelons territoriaux étant transformés en SCRT (renseignement territorial) sous l'autorité des préfets locaux, [...] la communication n'a pas très bien fonctionné entre province et Paris (voir l'affaire Merah) »*.

Mai 2017 : Le Président Emmanuel Macron

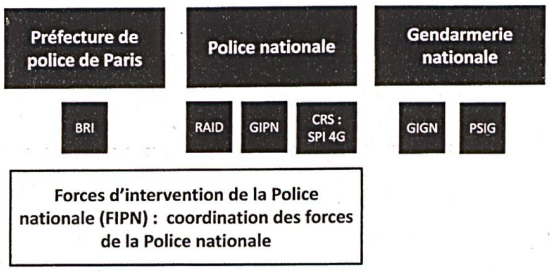
Dès son arrivée, le nouveau Président met en place une nouvelle entité : le Coordinateur national du renseignement et de la lutte contre le terrorisme hébergée à la Présidence et dirigée par le Préfet Pierre de Bousquet. Ce dernier est intervenu sur la lutte contre la radicalisation au Milipol en novembre 2017 à Villepinte (Paris). Le but : faire le lien avec le renseignement extérieur (DGSE) et intérieur (DGSI). De cette équation, le Président entend impulser une synergie dans la lutte essentielle contre le terrorisme. A quand un coordinateur au niveau de l'Union européenne ?

C. T.

188



189



Extrait : Entretien réalisé le 9 avril 2018 avec Alain Chouet, ancien fonctionnaire du service d'espionnage. Il commence sa carrière à la Direction Générale de la Sécurité Extérieur (DGSE) en 1972 anciennement appelé jusqu'en 1982 le SDECE (Service de documentation extérieure et de contre-espionnage).