CSFRS

Conseil Supérieur de la Formation et de la Recherche Stratégiques

GEOSTRATEGIA

L'agora stratégique 2.0 du CSFRS

WEBSOVI

Web social et violence

ifri institut français des relations internationales

Rapport WEBSOVI « Web social et violence »

Edité en Octobre 2015.

Le projet « Web social et violence » (Websovi) a été élaboré par le Centre des études de sécurité de l'Institut français des relations internationales (Ifri). Il s'est déroulé du 1er octobre 2014 au 30 septembre 2015 et a bénéficié du soutien du Conseil supérieur de la formation et de la recherche stratégiques (CSFRS).

Il avait pour objectif de mieux comprendre les articulations entre le développement du web social et différentes formes de violence. En pratique, ce projet a abouti – conformément à ce qui était prévu initialement – à la parution de trois rapports de recherche et à l'organisation d'un séminaire fermé d'une demi-journée.

Cette étude est à retrouver sur le site du Conseil Supérieur de la Formation et de la Recherche Stratégiques.

Auteur(s) : Marc Hecker

Source(s) : CSFRS, IFRI

WEB SOCIAL ET VIOLENCE (WEBSOVI)

Compte rendu scientifique de fin d'opération
Octobre 2015

Projet réalisé avec le soutien du
Conseil supérieur de la formation et de la recherche stratégiques
(CSFRS)

Le projet « Web social et violence » (Websovi) a été élaboré par le Centre des études de sécurité de l'Institut français des relations internationales (Ifri). Il s'est déroulé du 1er octobre 2014 au 30 septembre 2015 et a bénéficié du soutien du Conseil supérieur de la formation et de la recherche stratégiques (CSFRS). Il avait pour objectif de mieux comprendre les articulations entre le développement du web social et différentes formes de violence. En pratique, ce projet a abouti – conformément à ce qui était prévu initialement – à la parution de trois rapports de recherche et à l'organisation d'un séminaire fermé d'une demi-journée.

Les rapports de recherche ont été publiés dans la collection électronique « Focus stratégique » et ont fait l'objet d'une double campagne de communication : l'une, très large, par voie électronique (annonce de parution sur le site de l'Ifri, sur le blog Ultima Ratio, sur les réseaux sociaux, envoi d'un e-mailing à plusieurs milliers de personnes, etc.) ; l'autre, beaucoup plus ciblée, à destination de décideurs, par voie postale.

La réunion de lancement du projet Websovi s'est tenue au CSFRS le 28 novembre 2014. Les quatre sujets pressentis ont été confirmés. Le comité de pilotage a ainsi validé les sujets suivants pour les rapports de recherche : web social et djihadisme ; web social et gangs ; l'approche russe de la communication sur Internet dans le conflit ukrainien. Pour le séminaire, le sujet ayant retenu le plus l'attention était l' « hacktivisme ». A l'issue de cette réunion de lancement, les rapports de recherche ont été commandés à Marc Hecker pour le premier sujet, Daniel Ventre pour le deuxième sujet et Julien Nocetti pour le troisième sujet.

Le premier rapport de recherche a été publié en juin 2015 sous le titre « Web social et djihadisme : du diagnostic aux remèdes ». Compte tenu de la richesse de l'actualité (loi antiterroriste de novembre 2014, attentats de janvier 2015, lancement du dispositif « stop-djihadisme », etc.), ce rapport a été plus long que prévu (100 000 signes au lieu des 60 000 signes envisagés initialement). Sa publication a suscité des réactions très positives. L'Ifri a ainsi reçu des messages élogieux du Secrétaire général de la défense et de la sécurité nationale, du cabinet du Premier ministre, d'élus et d'experts des questions de défense. Ce rapport a également eu des retombées positives dans la presse. Une interview d'une page y a notamment été consacrée dans le journal *L'Opinion* (édition du 23 juin). Jean Guisnel, journaliste spécialisé sur les questions de défense au *Point*, a qualifié ce rapport de « remarquable » dans un article paru le 2 juillet[1]. L'auteur du rapport, Marc Hecker, a été interviewé par plusieurs médias dont

[1] Jean Guisnel, « La stratégie de la pieuvre », *Le Point*, 2 juillet 2015, pp. 55-56.

LePoint.fr[2], *Radio France Internationale* (RFI)[3] et *The Montreal Gazette*[4]. Il a également été invité à s'exprimer dans différentes institutions. Il a pris part, entre autres, à la conférence « Youth and the Internet : Fighting Radicalization and Extremism » qui s'est tenue à l'Unesco les 16 et 17 juin, et a été convié à présenter son travail au cabinet du ministre de la Défense.

Sur le fond, Marc Hecker – chercheur au Centre des études de sécurité de l'Ifri – démontre que la mouvance djihadiste internationale s'est mise à utiliser Internet dès le début des années 1990 et a su s'adapter aux évolutions du web. Les premiers sites web djihadistes ont ainsi cédé la place aux forums interactifs, puis aux réseaux sociaux. L'organisation Etat islamique a fait un usage impressionnant de Facebook et de Twitter, non seulement pour relayer sa propagande mais, de surcroît, pour diffuser des grandes orientations stratégiques, pour prodiguer des conseils tactiques, pour lever des fonds et pour recruter. En somme, Internet est devenu une véritable plateforme opérationnelle pour les groupes djihadistes. Au début de l'année 2015, on comptait environ 50 000 comptes liés à l'Etat islamique sur Twitter et cette organisation diffusait une demi-douzaine de vidéos par semaine. Pour faire face à cette présence massive des djihadistes sur le web, trois méthodes sont appliquées dans différents pays occidentaux. Premièrement, la censure consiste soit à supprimer soit à bloquer les contenus les plus radicaux mais elle se révèle particulièrement difficile à mettre en œuvre sur les réseaux sociaux. Deuxièmement, la promotion de contre-discours vise à décrypter et décrédibiliser la rhétorique djihadiste. Troisièmement, l'infiltration des réseaux djihadistes sur Internet permet non seulement de collecter du renseignement, mais aussi de susciter de la méfiance entre les cyberdjihadistes.

Le deuxième rapport a été rédigé par Daniel Ventre, titulaire de la chaire de cyberdéfense et cybersécurité des Ecoles de Saint-Cyr Coëtquidan, et publié en août 2015. Ce rapport est novateur et original : il n'existait jusqu'alors aucune publication scientifique en français sur l'utilisation du web social par les gangs. Daniel Ventre reprend la définition des gangs de la police de Peel dans l'Ontario : il s'agit d'un « groupe de trois personnes ou plus, avec une organisation formelle ou informelle, disposant d'un nom commun ou d'un signe ou symbole d'identification, formant une association dans un but criminel commun. Les membres s'engagent collectivement ou individuellement dans des modèles de comportement criminel [et] créent une atmosphère de

[2] Jean Guisnel : « Hecker : la manière dont l'EI utilise les réseaux sociaux est réellement innovante », *LePoint.fr*, 11 juillet 2015.

[3] Olivier Fourt, « La bataille médiatique face à l'organisation Etat islamique », RFI, 6 septembre 2015.

[4] Catherine Solyom, « As radicalization grows online, so do efforts to combat it », *The Montreal Gazette*, 24 juin 2015.

peur et d'intimidation dans la communauté »[5]. A partir de cette définition, il étudie les pratiques de plusieurs gangs ou membres de gangs sur les réseaux sociaux, en particulier Facebook et Twitter. Les gangs semblent utiliser le web social de façon disparate et sans véritable stratégie. Il est toutefois possible d'observer certaines pratiques récurrentes. Le web est ainsi utilisé pour promouvoir une sous-culture criminelle et créer de la cohésion entre les membres d'un même gang. Il sert aussi à intimider les membres de gangs adverses et à susciter tantôt de la fascination, tantôt de la terreur à l'égard d'un public plus large (forces de l'ordre, populations locales, etc.).

Pour faire face aux gangs, les forces de l'ordre ont su s'adapter aux évolutions technologiques et bénéficient de l'apport de nouveaux logiciels qui permettent de traquer les membres de gangs sur Internet. D'autres outils innovants, qui misent sur les applications du « Big Data », se veulent prédictifs : ils permettraient de cibler les individus à risque et d'identifier les lieux et les moments les plus propices au passage à l'acte criminel. Il serait ainsi possible de concentrer les effectifs de police de manière optimale. Si ces méthodes sont parfois jugées opaques et potentiellement dangereuses pour les libertés individuelles, elles n'en demeurent pas moins prometteuses pour lutter contre les gangs et, plus largement, contre la criminalité. Pour conclure, Daniel Ventre revient sur le concept de *netwar* développé depuis une vingtaine d'années par John P. Sullivan, John Arquilla et David Ronfeldt. Ces auteurs définissent la *netwar* comme une forme de conflit de faible intensité dans lequel des acteurs non-étatiques pourraient mettre en échec des acteurs étatiques plus puissants en raison de l'apport des nouvelles technologies. Ces technologies leur offriraient la capacité de se développer en réseaux, sans contrainte de frontières. A cet égard, Daniel Ventre se veut rassurant : les gangs n'ont pas réussi, pour l'instant, à bénéficier du web au point de remettre en cause la suprématie des Etats.

Le troisième rapport de recherche a été publié à la fin du mois de septembre 2015. Son auteur, Julien Nocetti, est spécialiste de la Russie et des questions de gouvernance de l'Internet à l'Ifri. Sa recherche s'appuie sur des sources de première main en russe et permet de mieux comprendre la manière dont Moscou cherche à agir sur les perceptions. Avant d'étudier le cas spécifique du conflit en Ukraine, Julien Nocetti montre comment, depuis le début des années 2000, la Russie développe des institutions spécialisées dans les problématiques de communication et élabore des doctrines insistant sur l'importance de la maîtrise de l'« espace informationnel ». Ces doctrines font apparaître une approche « holistique » de la guerre de l'information : il ne s'agit pas uniquement de garantir la sécurité des infrastructures de communication mais,

[5] Crime Prevention Services, « Street gangs, facts and myths », Peel Regional Police, Brampton, 2009.

de surcroît, d'influer sur les différentes opinions publiques. En pratique, la Russie a investi des sommes importantes dans des outils d'influence, comme la chaîne de télévision RT ou la radio Sputnik International. Elle a également pris des dispositions légales pour mieux contrôler Internet et asseoir sa souveraineté numérique. Le principal réseau social russe, VK, est passé sous le contrôle d'oligarques proches du Kremlin.

Dans le cadre du conflit en Ukraine, la Russie a mis en place une campagne de désinformation de grande ampleur. Les partisans du mouvement « Maïdan » ont été comparés à des fascistes et à des nazis. La présence de soldats russes en Crimée et dans l'est de l'Ukraine a été niée. Puis, l'action de la Russie a été justifiée par des raisons humanitaires, au nom de la protection des populations russophones. Le concept de *Novorossiya* (« nouvelle Russie ») a été utilisé pour justifier la reconfiguration géographique de l'Europe orientale. Sur le web, le discours officiel russe a été relayé par des institutions publiques (notamment les ambassades russes à travers le monde) mais la guerre de l'information a aussi été partiellement privatisée. Des agences de communication spécialisées – employant des « armées de trolls » – ont ainsi été chargées de propager les arguments du Kremlin sur les principaux sites d'information et réseaux sociaux russes et occidentaux. Par exemple, les modérateurs du site web du *Guardian* ont eu à gérer jusqu'à 40 000 commentaires pro-russes par jour. Face à la stratégie russe de contrôle de l'espace informationnel, les pays occidentaux ont manqué de préparation et ont eu le plus grand mal à réagir. Toutefois, on ne peut pas conclure que la Russie a « gagné » la guerre de l'information. En effet, certains arguments employés par les dirigeants russes étaient tellement outranciers qu'ils ont fini par entacher la réputation de la Russie. Dans les pays occidentaux, Moscou conserve néanmoins un noyau non négligeable de soutiens dans les mouvances « anti-système » qui contestent l'objectivité des médias traditionnels et recherchent de l'information dite « alternative ».

Le quatrième livrable du projet « Websovi » – le séminaire fermé sur l'hacktivisme – s'est tenu à l'Ifri le 18 septembre 2015. Il a réuni une quarantaine de personnes provenant de différents ministères, de grandes entreprises et du milieu de la recherche. Ces personnes avaient des formations disciplinaires très variées (informaticiens, mathématiciens, politistes, sociologues, juristes, spécialistes de *war studies*, etc.) ce qui a permis des échanges de vues particulièrement riches et originaux. Les échanges ont aussi été facilités par le fait que ce séminaire était soumis aux règles de confidentialité dites de « Chatham House ».

L'accent a été mis sur l'analyse du phénomène hacktiviste, puis sur les réponses apportées par les pays occidentaux. La notion d'hacktivisme – néologisme formé par la fusion des termes « hackers » et « activisme » – peut être définie comme « l'utilisation non violente d'outils digitaux illégaux ou transgressifs à

des fins politiques »[6]. Au cours des dernières années, deux catégories d'hacktivistes se sont fait particulièrement remarquer : d'une part, des libertariens agissant contre des Etats ou des groupes privés puissants au nom de la défense des libertés individuelles et de la justice (Anonymous, Telecomix, etc.) ; d'autre part, des sympathisants djihadistes agissant notamment au nom de l'Etat islamique (Cybercaliphate, ISIS Cyber Army, etc.). On constate également une plus grande porosité des sphères de la cybercriminalité et de l'hacktivisme.

Les cyberattaques commises par les hacktivistes sont généralement peu évoluées d'un point de vue technique. Elles consistent le plus souvent à « défacer » des sites web ou à les rendre inaccessibles par des attaques de déni de service. Cependant, des attaques « simples » peuvent se révéler gênantes si elles sont réalisées en masse. Dans la semaine qui a suivi l'attentat contre *Charlie Hebdo*, environ 20 000 sites web français ont fait l'objet de cyberattaques. Les attaquants étaient très opportunistes, ciblant les sites vulnérables quel que soit le secteur concerné (collectivités territoriales, associations, restaurants, etc.). Les sites atteints ont vu leur page d'accueil remplacée par des messages hostiles. Même si ces sites n'étaient pas stratégiques, ces attaques doivent être prises au sérieux car elles participent de la stratégie de terreur des djihadistes.

On observe depuis quelque temps une tendance à la complexification des modes opératoires. Ceci est dû à la coopération de plus en plus poussée de cellules de hackers sur des opérations fédératrices, au développement des cours de hacking en ligne et, surtout, à la mise à disposition sur Internet de logiciels de piratage performants dérobés à des entreprises spécialisées dans la cybersécurité (Gamma International, Hacking Team, etc.).

Pour pouvoir répondre à une cyberattaque – qu'elle ait pour origine des hacktivistes ou d'autres acteurs –, il faut être capable d'en déterminer l'origine. Le processus d'attribution est complexe. Il se déroule essentiellement à trois niveaux. Tout d'abord, au niveau technique, des spécialistes étudient les caractéristiques d'une attaque : mode opératoire, heure de l'attaque, type de claviers utilisés, langage utilisé par les attaquants, erreurs éventuelles, etc. Ensuite, au niveau opératif, il s'agit d'étudier le contexte géopolitique, d'essayer de déterminer si l'attaque a pu être commise sous faux pavillon, d'analyser la manière dont le virus se répand géographiquement, etc. Enfin, au niveau stratégique, l'objectif est de comprendre quel est le but ultime de l'attaque et à qui elle bénéficie. Ce processus relève probablement davantage de l'art que de la science. Pour les attaques les plus sophistiquées, l'identité exacte de

[6] Alexandra Samuel, *Hacktivism and the Future of Political Participation*, thèse de doctorat, université de Harvard (Department of Government), 2004.

l'attaquant peut être impossible à prouver. En d'autres termes, l'attribution des cyberattaques est souvent éminemment politique. Les hommes politiques sont pressés – notamment par les médias – de désigner très rapidement les responsables d'une attaque mais le processus d'attribution prend du temps. Des tensions peuvent ainsi apparaître entre le niveau des techniciens et celui des politiques. Dans le cas de la cyberattaque contre TV5 en avril 2015, les plus hautes autorités politiques ont attribué immédiatement cette action à l'Etat islamique mais il pourrait en fait s'agir d'une attaque sous faux pavillon.

D'un point de vue technique, la réponse à une cyberattaque consiste d'abord à comprendre les failles qui ont été exploitées pour pouvoir les combler et à renforcer les défenses des systèmes. Eventuellement, des représailles peuvent être déclenchées pour atténuer ou détruire les capacités cyber de l'adversaire. D'un point de vue juridique, les moyens dont dispose la justice française sont limités. Au parquet de Paris, deux substituts sont spécialisés dans la cybercriminalité. Au siège, 7 ou 8 magistrats sont spécialisés dans la « délinquance astucieuse » dont 1 ou 2 traitent les dossiers relatifs à Internet. Il faut distinguer les infractions traditionnelles dont le vecteur principal est Internet des infractions cyber proprement dites. Parmi ces dernières, différents types d'attaques se combinent souvent : accès ou maintien frauduleux de données, entrave à un système automatisé de données ou détention de logiciels illégaux. La loi antiterroriste du 13 novembre 2014 introduit des facilités procédurales pour la poursuite des hackers. Elle permet notamment la qualification pénale du vol de données informatiques. La loi de juillet 2015 sur le renseignement dépénalise quant à elle le piratage informatique lorsqu'il est commis à l'extérieur du territoire français et quand l'objectif est de protéger les intérêts fondamentaux de la nation. En pratique, la réponse judiciaire aux attaques commises par des hacktivistes se heurte souvent à la problématique de la coopération judiciaire internationale. Cette coopération fonctionne relativement bien entre Etats signataires de la convention de Budapest sur la cybercriminalité, qui permet notamment le gel de données informatiques. Cette convention n'a cependant été ratifiée que par une cinquantaine d'Etats. Des pays comme la Chine ou la Russie n'en font pas partie.

En conclusion, le projet Websovi a permis d'étudier différentes interactions entre web social et violence. Les pratiques des acteurs varient sensiblement selon les moyens dont ils disposent et l'intérêt qu'ils portent au web. Les acteurs étatiques disposent de moyens nettement supérieurs aux acteurs non étatiques et peuvent donc avoir des stratégies plus ambitieuses. Dans le domaine des cyberattaques, les opérations les plus sophistiquées ne peuvent être réalisées que par des services étatiques. Dans le domaine des perceptions et de l'action psychologique, les Etats peuvent développer des outils d'influence coûteux, à l'instar du système élaboré par la Russie qui combine des

aspects télévisuels, radiophoniques et web. Les acteurs non étatiques ont une maîtrise du cyberespace très variable. La stratégie web de la mouvance djihadiste internationale est très évoluée. Internet est utilisé par cette mouvance non seulement comme un vecteur de propagande mais aussi comme une véritable plateforme opérationnelle qui sert à diffuser des grandes orientations stratégiques ou à recruter. Les gangs sont encore loin de ce niveau de sophistication. Quant aux hacktivistes, ils progressent et développent des modes opératoires de plus en plus perturbants pour les Etats qu'ils visent. Les innovations étant permanentes dans le domaine d'Internet et le champ de la conflictualité étant en pleine évolution (apparition de Daech, développement du concept de « guerre hybride », etc.), il apparaît souhaitable que le projet Websovi ouvre la voie à d'autres recherches sur le lien entre web social et violence.