L’action cyber Russe au service du renseignement stratégique

Thierry Berthier (MC Univ. Limoges), Capitaine Djammel Metmati

Janvier 2015, article III.19

La plupart des activités humaines donnent lieu aujourd'hui à la production massive de données numériques. Le volume global des données produites en 2013 a dépassé les 4,4 Zettaoctets et devrait atteindre les 44 Zettaoctets en 2020. Ce déluge de données nécessite de puissantes infrastructures de traitement par des moteurs de recherche toujours plus performants. Ces derniers permettent de collecter, trier, classer et hiérarchiser l'information. Dans un contexte de cyberconflictualité croissante, les moteurs facilitent l'obtention de données sur un adversaire désigné lorsque celui-ci possède une projection algorithmique référencée.

La communauté des États a mesuré l'importance stratégique des moteurs de recherche dans le maintien d'une souveraineté informationnelle qui apparaît aujourd'hui comme un outil de puissance pour une nation technologique.
Ainsi, la Russie tente d’imposer un moteur de recherche national limitant l’exploitation des données russes au profit de puissances étrangères. A cela s’ajoute une volonté de contrôler, par des partenariats historiques et des alliances, les architectures des systèmes d’information et de communication en misant sur des plateformes collaboratives inhérente à la logique réseau.
En cas de crise, cette posture engendre des vulnérabilités dans l'architecture Cyber et ouvre la voie à la consultation des données adverses, vecteur d’actions cinétiques et de cyber-opérations déstabilisatrices.

I-Défendre le champ informationnel national : l’exemple du moteur Yandex

Au regard d'une production mondiale exponentielle de données, les moteurs de recherche constituent des organes essentiels dans la collecte et le traitement de l’information. Chaque utilisateur des systèmes numériques produit de l’information

sous la forme de données et de métadonnées. Cet ensemble informationnel devient alors une cible naturelle pour les sphères du marketing et du commerce comme pour les grands acteurs de la sécurité nationale.
Les informations mises en ligne par l'utilisateur permettent parfois de mener, à partir d'autres pays, des opérations de guerre de l'information. Elles offrent souvent une première image du contexte social et politique dans lequel les données ont été produites. Elles apparaissent enfin comme une importante source de renseignements pour l'entité qui supervise une cyber-opération dans le champ économique, politique ou militaire[1].

1.1. Le caractère stratégique des moteurs de recherche

La Russie a mesuré et évalué la valeur d'impact stratégique et géopolitique des moteurs de recherche. Créé en 1997 par Arkadi Voloj et basé à Moscou, Yandex est le moteur de recherche le plus populaire en Russie et le plus utilisé sur le Web russophone. La société devenue rentable à partir de 2002 est revendue en 2004 pour 17 millions de dollars. En 2012, Yandex a lancé son propre navigateur « Yandex, proche dans sa structure de Chromium », la base dont Google s'est servie pour développer Chrome. Ce navigateur intègre des fonctionnalités de sécurité issues d'un partenariat noué avec Kaspersky Lab. En décembre 2013, Yandex totalisait 62% des requêtes et recherches en Russie contre 27% pour Google.
Le Président russe s'est récemment exprimé sur la pertinence stratégique du moteur de recherche russe Yandex en déplorant le fait que la société Yandex soit en partie enregistrée à l'étranger. La critique de Vladimir Poutine ne portait pas sur le volet fiscal de cet enregistrement mais sur l'aspect stratégique et le risque de perte de supervision nationale de l'infrastructure. Le Président russe a publiquement dénoncé la présence de cadres dirigeants européens et américains au sein des conseils d'administration et de gestion de Yandex. Il s'est dit particulièrement préoccupé par la perte d'une partie de la souveraineté de la Russie au profit de puissances étrangères. Une nation technologique qui souhaite maintenir son socle de souveraineté numérique doit favoriser l'émergence de moteurs nationaux afin de contenir la suprématie du géant américain. Cette orientation devient même prioritaire pour la Russie qui s'inscrit dans une forme de repli nationaliste**.**

1.2. Contrôler les données nationales

Plusieurs lois ont été votées pour les usagers d'Internet. Elles touchent à la politique de gestion des données produites par la population russe.
La loi du 4 juillet 2014 contraint les sites Internet contenant des données personnelles de citoyens russes à utiliser des serveurs basés en Russie. De plus, cette loi stipule qu'à partir du 1er septembre 2016, les réseaux sociaux, les services de messagerie, les moteurs de recherche et les utilisateurs devront être hébergés sur des serveurs en Russie.
La loi fédérale russe[2] prévoit également l'établissement d'une liste noire de sites Web contenant des informations interdites de diffusion en Russie[3]. Elle oblige les

[1] Surtout en appui d'une opération terrestre, aérienne, maritime
[2] Loi n°89417-6

blogueurs russes à enregistrer leurs sites Web et à se conformer aux mêmes règles éditoriales que celles en vigueur pour les médias de masse en Russie.
Cette posture protectionniste vise à promouvoir la puissance numérique russe à travers un système capable de capter et d'utiliser de la donnée. En renforçant la maîtrise de ce processus, l'Etat russe consolide une volonté de gestion et de traitement de l'information en entrée-sortie avec des territoires étrangers[4]. Dès lors, ce verrouillage intérieur du Web russe traduit la volonté de maintenir une indépendance nationale[5]. La Russie souhaite développer un moteur de recherche national nommé Spoutnik[6] sur lequel elle aurait un contrôle plus direct que sur l'actuel leader Yandex. Le contrôle du contenu informationnel s'effectue donc de bout en bout dans une posture de sécurité nationale : du blogueur indépendant jusqu'à la chaîne d'information nationale. En construisant une architecture Cyber capable de défendre le périmètre réseau russe, Vladimir Poutine place également la Russie dans une posture offensive vis-à-vis de son « étranger proche ». Elle s'exprime par l'exploitation de l'architecture réseau post guerre froide des anciens pays du pacte de Varsovie au profit du renseignement stratégique et de cyber-opérations. Le conflit opposant la Russie[7] à l'Ukraine permet de comprendre l'articulation du renseignement stratégique au profit d'une cyber-opération.
Selon BAE systems, l'Ukraine a été la première cible d'un malware[8] avec 32 exemples enregistrés et 22 depuis janvier 2013. En perturbant les systèmes du gouvernement ukrainien avec une possible capacité de destruction des réseaux informatiques, cette cyber-attaque s'associe dans le temps à une situation conflictuelle opposant deux États. Enfin, elle montre l'utilité du renseignement d'intérêts cyber dans la perturbation d'un adversaire étatique en ciblant son architecture réseau.

II - Maîtriser l'adversaire par le Cyber

Dans un contexte contraint, le Cyber apparaît comme un des moyens innovant permettant d'atteindre un objectif avec un coût marginal réduit. L'exploitation des vulnérabilités des architectures adverses associées à leurs systèmes d'information donnent les angles d'attaques potentielles. Elles se traduisent par des formes d'actions stratégiques et tactiques originales dans une gestion de crise ou un engagement.

2.1. Une cyber-arme de cœur de réseau : l'exemple de Snake

La dénomination de cette attaque s'appuie sur un Trojan de classe Agent.Btz[9]. Il se distingue des variantes existantes depuis 2008 par l'emploi de techniques spécifiques. Après l'installation d'une « backdoor »[10] sur un système Windows corrompu, cet agent offre un mécanisme de communication avec des serveurs ou des machines

[3] L'article 4 de la loi n°89417-6 envisage la création d'un registre de domaines et de sites web à caractère pédophile, promouvant ou commercialisant des stupéfiants, incitant au suicide ou propageant des idées "extrémistes"
[4] Virtuel et physique
[5] D'autres pays empruntent cette voie. La Chine dispose aujourd'hui d'une dizaine de moteurs de recherches efficaces dont le populaire Baidu dépassant Google Chine arrivé en 2005.
[6] Le projet Spoutnik est porté par Rostelecom
[7] via les russophones de l'ouest de l'Ukraine.
[8] Snake
[9] Un malware affectant les systèmes fonctionnant sous Windows. Perçu comme dépassé, il reste prolifique et continue d'infecter des ordinateurs
[10] Ce rôle est joué par les différents types de mémoires propres aux matériels constructeurs

distantes. L'installation permet ensuite d'exfiltrer des informations pertinentes sur un point déterminé du réseau. Dans le même temps, Snake montre une variabilité et une flexibilité dépendante de l'architecture de communications dans lequel il évolue. Cette caractéristique induit une connaissance précise de la cartographie de l'architecture des équipements réseau déployés par l'opérateur ukrainien Ukrtelecom[11]. L'attaque a été planifiée sur une semaine selon des tranches horaires s'étalant de 10h à 22h du 24 au 28 février 2014. Deux pics ont été enregistrés : à 11h et 17h et deux modes d'attaque ont été identifiés**.** Un premier procédé d'exécution s'établit en mode utilisateur. Un second plus complexe s'appuie sur l'infection du noyau gérant les ressources de la machine Windows. L'exécution du Rootkit s'appuie sur le chargement d'un module DLL dans les processus user mode. Ces derniers prennent des noms divers comme taskhost.exe ou service.exe masquant ainsi le fichier DLL mscpx32n.DLL. Ce module initie la communication avec d'autres serveurs en mode « PIPE ». Ces derniers placent ce module sur leurs listes blanches, permettant l'infection d'autres systèmes malgré les firewalls. Cette action permet d'identifier la structure interne du code source. Les noms de fichiers apparaissent et le contrôle des logs donne les pseudo-des développeurs : Vlad et gilg. Il s'agit certainement d'une forme de signature du malware. Ensuite, une notification de « callback » permet à Snake de rester sur un système et d'être capable de créer un nouveau processus infecté, même après une suppression. Le Trojan reste passif tant qu'aucune connexion Internet n'est active. Dans ce cas, le code malicieux sous la forme de la DLL est en sommeil dans le navigateur. L'activité du Trojan suit celle du navigateur, ce qui le rend difficilement détectable. Cette particularité tient à la nature des pages Web. Elles se construisent à partir de données provenant de différents serveurs générant des centaines de requêtes HTTP et DNS. Le second procédé d'exécution est unique. Il se manifeste par un trafic réseau routé à travers un hôte infecté dans lequel sont exfiltrés des données. En revanche, les vecteurs sont traditionnels : thumb drive, pièces jointes, un exploit. Une fois lancé, le malware s'installe dans un lieu défini comme « Ultra3 ». Le système crée alors une entrée dans la base de registre avec une nouvelle clé d'entrée :
« KEY_LOCAL_MACHINE\System\CurrentControlSer\Services\Ultra3 ». Les hooks[12] systèmes masquent la présence de Snake en bloquant l'entrée des registres contenant le terme « Ultra3 ». Ils injectent la DLL dans l'environnement de l'utilisateur. Ils s'adaptent à l'état de marche du système. L'injection ne s'effectue que si le système est en marche « ZwshutdownSystem ». Si l'utilisateur partitionne son disque, des hooks comme « ObOpenObjetByname » et « IofCallDriver » cachent la présence de Snake et cryptent le fichier corrompu. Une fois la connexion établie avec un autre système, le trafic est intercepté et l'injection du code malveillant s'opère suivant plusieurs procédés liés au processus Windows et aux vulnérabilités des interfaces de réseau[13].

2.2. Contre-mesures et posture d'attaque

Les contre-mesures immédiates s'évaluent en termes de capacités. Une organisation

[11] Ukrtelecom est le seul fournisseur de lignes terrestres de télécommunications de l'Ukraine
[12] Ils permettent de personnaliser le fonctionnement d'un logiciel suivant les objectifs choisis.
[13] WFP constitue un processus natif qui surveille les systèmes installés par Windows.
Les interfaces réseau ont pour origine le succès des interfaces de programmation API. Elles permettent de construire un logiciel en réutilisant les fonctionnalités d'un autre.

confrontée à ce malware pourrait s'appuyer sur un « Mass scan[14] » d'environ une heure sur un réseau où agissent plusieurs acteurs. En enregistrant les flux réseau, cette méthode sert à suivre et à cartographier le chemin pris par le malware. De facto, les cibles potentielles peuvent être reconnues sans être détectées. Du point de vue machine, l'utilisation d'une partition conduit à transférer les logs de Snake sur cet emplacement. Il faut également modifier les paramètres d'une clé de registre, contrôler la taille et la nature des fichiers, utiliser des commandes spécifiques. Les conséquences stratégiques et tactiques se situent à deux niveaux.
Avant un engagement militaire, des coups de semonce sous la forme de cyber-attaques sur les structures étatiques adverses apparaissent possibles. Associées à des manœuvres militaires, elles semblent s'inscrire dans une des étapes menant à l'action armée. Les décideurs disposeraient d'un cycle structuré en trois temps : diplomatie, cyber-attaques et intimidation militaire, intervention armée. Aussi, un Etat doit se virtualiser dans son action. Autrement dit, sa souveraineté et sa puissance s'expriment également dans les réseaux. Pendant un conflit, la défense de ses intérêts passe par la sauvegarde de l'intégrité de ses réseaux. Perdre cette garantie conduit à la perte de souveraineté par l'accès aux données nationales et donc à la lecture des intentions.

Si l'action cyber russe a pris la forme d'attaques informatiques en Estonie et en Géorgie, le conflit ukrainien met en perspective la capacité d'un Etat à exploiter à son profit les architectures de communication et d'information adverse.
Cette démarche consiste en amont à établir sur le territoire adverse sa propre infrastructure d'équipements réseau. Une fois établie le principe du cheval de Troie, les cyber-opérations sont facilitées par un environnement technique favorable. Face aux potentialités de cette méthode, la seconde perspective tient à une gestion organisée des données de la population russe. L'action cyber russe devient également un moyen de préserver un espace informationnel au motif que les données produites par les russes se confondent avec les intérêts stratégiques de la Russie.

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18
La chaire remercie ses partenaires

[14] Cette opération permet d'analyser des millions d'adresses IP et de ports d'équipements informatiques