Cyberguerre

Source
levif.be / afp
13 mai 2017

1. Les principales cyberattaques entre 2007 et 2017

La vague de cyberattaques simultanées qui a touché une centaine de pays et des dizaines d'entreprises et d'organisations à travers le monde est sans précédent. Entre « cyberguerre » et « hacktivisme », voici un rappel des principales attaques informatiques menées entre 2007 et 2017.

Cyberguerre

La première cyberattaque majeure visant un État frappe au printemps 2007 l'Estonie alors en plein conflit diplomatique avec la Russie. Le réseau internet de cette ancienne république soviétique, et en particulier son réseau bancaire, est paralysé pendant plusieurs jours. L'Estonie accuse la Russie, qui dément.

Un an plus tard, les sites internet de la présidence géorgienne et les principaux réseaux télévisés du pays sont à leur tour cibles d'une cyberattaque, là aussi sur fond de conflit avec Moscou sur le sort des régions séparatistes d'Ossétie du Sud et d'Abkhazie.

En juillet 2009, les sites internet de la Maison Blanche, du Département d'Etat, du Pentagone ou de la Bourse de New York sont touchés par des attaques coordonnées qui affectent également la présidence sud-coréenne ainsi que les ministères de la Défense et des Affaires étrangères. La Corée du Sud est de nouveau visée en 2013 dans un contexte de vives tensions avec son voisin du nord. Les réseaux informatiques de plusieurs chaînes de télévisions et de certaines banques sont paralysés.

À l'automne 2014, Pyongyang est encore mis en cause dans le piratage du studio de cinéma américain Sony, contraint d'annuler la sortie de « L'interview qui tue ! », une comédie sur un complot fictif de la CIA pour assassiner le leader nord-coréen Kim Jong-Un. Les données personnelles de quelque 47'000 employés sont volées et une bonne partie mises en ligne.

Si des pirates russes, nord-coréens ou chinois sont souvent cités, le virus Stuxnet qui s'abat en 2010 sur des installations nucléaires de l'Iran est probablement d'origine américaine.

Hacktivisme

Anonymous, le plus connu des groupes de piratage informatique, s'attaque depuis quinze ans à tout type de cibles sous couvert de lutte contre les injustices. Parmi ses nombreux faits d'armes, on compte des attaques contre divers sites gouvernementaux dont le Pentagone, l'Eglise de Scientologie, le groupe Etat islamique (EI) ou encore le groupe bancaire MasterCard.

Créé il y a dix ans par l'Australien Julian Assange, le site Wikileaks s'est lui spécialisé dans le piratage de documents classifiés. Il a notamment mis en ligne en 2010, 251.000 correspondances d'ambassades américaines classifiées puis des milliers de documents militaires sur l'Afghanistan. Le site a également révélé des affaires d'espionnages d'alliés des États-Unis et publié les emails piratés du parti démocrate américain.

Dans cette affaire de piratage du parti démocrate, survenue à l'automne 2016 en pleine campagne pour la présidentielle américaine, les agences de renseignement ont accusé la Russie d'avoir interféré dans l'élection afin de favoriser le candidat républicain Donald Trump, élu le 8 novembre aux dépens d'Hillary Clinton.

Une affaire comparable a éclaté le 5 mai dernier en France, à quelques heures du deuxième tour de l'élection présidentielle, quand des milliers de documents de l'entourage du candidat centriste Emmanuel Macron ont été diffusés sur les réseaux sociaux. L'équipe du candidat, élu deux jours plus tard, a dénoncé une « action de piratage massive et coordonnée », y voyant une « opération de déstabilisation » des « forces conservatrices », notamment russes et américaines

Cyberterrorisme

En janvier 2015, des hackers se réclamant du groupe jihadiste État islamique prennent brièvement le contrôle des comptes Twitter et YouTube du commandement militaire américain au Moyen-Orient (Centcom), une intrusion embarrassante pour l'armée américaine en pleine guerre contre l'EI en Syrie et Irak.

Deux mois plus tard, un groupe se présentant comme la « Division des hackers de l'Etat islamique » met en ligne une liste de 100 militaires américains à abattre, précisant leurs noms et adresses ainsi que des photos.

Parmi les innombrables cyberattaques de nature criminelle recensées chaque jour dans le monde, on peut citer le piratage entre 2005 et 2012 de systèmes de paiement en ligne, qui a provoqué plus de 300 millions de dollars de pertes pour une quinzaine de sociétés américaines et européennes.

Grandes entreprises et médias font aussi figures de cibles de choix pour les pirates informatiques. A deux reprises, en 2013 et 2014, le groupe internet américain Yahoo! et des centaines de millions de ses utilisateurs ont été visés par des cyberattaques.

En avril 2015, la télévision francophone TV5 Monde est victime d'une cyberattaque menée par des inconnus se réclamant de l'EI, mais qu'une enquête identifie ensuite comme des hackers russes. TV5 avait alors perdu le contrôle de ses sites internet, de ses comptes sur les réseaux sociaux, et avait dû couper pendant plusieurs heures ses programmes.

Source
Le point
Baudouin Eschapasse
25 avril 2019

2. Cyberguerre : les grandes manœuvres ont commencé...

Les statistiques peuvent être trompeuses. Alors que le nombre de cyberattaques d'ampleur, signalées à l'Agence nationale de la sécurité des systèmes d'information (Anssi), s'est stabilisé en 2018, Guillaume Poupard, directeur de l'établissement public, chargé de la protection des réseaux des administrations et entreprises « d'importance vitale », reste vigilant. « Certes, avec 1869 signalements [contre 2435 l'année précédente et 3235 en 2016, NDLR], le nombre de dossiers traités reflue légèrement. Mais la menace reste forte et nos équipes demeurent pleinement mobilisées face à la sophistication croissante des agressions numériques », confie ce haut fonctionnaire qui dirige près de 600 agents spécialisés en cybersécurité. Pour preuve ? Le nombre d'incidents majeurs, concernant des infrastructures critiques, ne recule pas (il s'est établi à 16 l'an dernier) et la part des « opérations de cyberdéfense » (le plus haut niveau d'alerte avant l'opération militaire proprement dite) augmente... de 12 en 2017 à 14 en 2018.

Cybersoldats chinois

Nommée en mars 2018 à la tête du Secrétariat général de la défense et de la sécurité nationale (SGDSN) qui chapeaute l'agence et est placé sous l'autorité directe du Premier ministre, Claire Landais ne tient pas un autre discours. « Le calme relatif de ces derniers mois ne doit pas nous faire oublier que l'Anssi est très sollicitée. Elle se tient prête à intervenir à tout moment et le fait d'ailleurs

régulièrement », surenchérit-elle. Même si elle se refuse à livrer le moindre nom de groupes français attaqués ces douze derniers mois et si elle évite aussi de détailler les interventions de ses équipes de « pompiers numériques », l'attaque dont ont été victimes les groupes français Altran et Airbus, en janvier dernier, était dans toutes les têtes au moment de la présentation du rapport annuel de l'Anssi, le 15 avril.

La finance, la santé, l'énergie et les télécommunications souvent visées

« Les modes opératoires évoluent. Parce que nous avons rehaussé les dispositifs de sécurité, les pirates informatiques ne peuvent plus emprunter les portes traditionnelles. Ils doivent désormais passer par les fenêtres », évoque, sous forme de métaphore, Guillaume Poupard. Les fenêtres ? Ce sont, avant tout, les prestataires de services informatiques à qui les entreprises et administrations hexagonales sous-traitent de plus en plus de chantiers. Et c'est ce qui explique l'augmentation d'attaques « par rebond » observée depuis quelques mois. À quelques semaines du 10e anniversaire de l'Anssi (le 4 juin), ses experts focalisent donc leur attention sur cette nébuleuse de PME spécialisées en cybersécurité à qui certains grands opérateurs publics comme privés externalisent la maintenance de leurs réseaux.

« Ces sous-traitants ont généralement un niveau de privilège élevé au sein des réseaux dont ils s'occupent. Se faire passer pour un prestataire constitue donc un moyen facile pour s'introduire au cœur d'un dispositif sensible », décrit François Deruty, sous-directeur « opérations » de l'Anssi. « Pour parvenir à ses fins, le hackeur peut réaliser un long travail d'approche et passer plusieurs mois à glaner des renseignements sur la société tierce qui lui permettront d'atteindre sa cible. Il peut ensuite rester tapi, à l'abri des regards, pendant plusieurs mois. Et ce, avant d'agir au moment opportun : pendant un long week-end ou à la veille d'une fusion-acquisition », poursuit l'ingénieur. Lequel glisse que, « dans un cas sur deux, ce travail de longue haleine qui nécessite souvent des moyens importants est l'œuvre d'un service d'espionnage étatique ».

Aucun secteur d'activité n'est épargné. La semaine dernière, le groupe agroalimentaire Fleury Michon a ainsi vu ses chaînes de production mises à l'arrêt pendant près d'une semaine par un virus informatique. Reste que les secteurs de la finance, de la santé, de l'énergie et des télécommunications sont plus souvent visés. En décembre dernier, le groupe de cybersécurité McAfee révélait ainsi qu'un important groupe de hackeurs baptisé « Rising Sun » (à défaut de pouvoir qualifier plus précisément l'agence de renseignements nord-coréenne à l'œuvre) était parvenu à s'introduire dans plus d'une centaine de réseaux d'infrastructures critiques dans 87 pays occidentaux. Et surtout, à y rester pendant une longue période sans être détecté : d'octobre à novembre 2018. L'entreprise Symantec avait identifié que ces cyberespions s'étaient introduits en utilisant un programme sophistiqué (connu sous le nom de Duuzer) ouvrant, en toute discrétion, une « porte dérobée » dans les serveurs, permettant d'exfiltrer des informations sensibles. Quelques semaines plus tôt, la compagnie FireEye dévoilait que la conception du virus informatique Triton, dont les effets destructeurs se sont fait sentir sur des installations pétrolières, en Arabie saoudite notamment, était l'œuvre d'un groupuscule russe dénommé Xenotime... (Les groupes énergétiques saoudiens font l'objet d'attaques régulières et très violentes depuis quelques années).

Restaurer la confiance

C'est pour « rendre de la sérénité aux acteurs », selon les propres termes de Guillaume Poupard, que l'Anssi se lance aujourd'hui dans un gros chantier de certification des sociétés de services informatiques de confiance. « Pour ce faire, nos agents vont expertiser leurs méthodes de travail et la robustesse de leurs serveurs afin de garantir aux groupes qui recourent à leurs services que ces PME ne sont pas compromises en matière de cybersécurité », glisse un salarié de l'agence. « Les mois qui viennent vont être marqués par de grands événements démocratiques : des élections qui peuvent potentiellement être la cible de cyberattaques. 2024 sera aussi l'année des Jeux olympiques à Paris. Nous devons nous tenir prêts », émet Cyril Demonceaux, chef de la division « Connaissance et anticipation » de l'Anssi.

Ses agents installent des sondes sur les serveurs dont ils assurent la sécurité, et ce, afin de repérer tout comportement suspect. Ils développent également, au sein de sept départements de recherche-développement, des marqueurs destinés à garder la signature, ou du moins l'empreinte, d'éventuels intrus. Autant de procédés qu'ils ne décriront pas devant la presse. « L'enjeu est de se prémunir contre l'éventuel piégeage du matériel [certains composants électroniques, produits à l'étranger, présentent parfois des portes dérobées, NDLR], celui des logiciels [qui peuvent être infectés par des codes malveillants], mais aussi les membres de la *supply-chain* (ces prestataires qui opèrent de plus

en plus souvent à distance, notamment au sein du cloud) », poursuit le spécialiste. « En la matière, l'imagination des pirates informatiques est incroyable », poursuit-il. « Le malware NotPetya s'est propagé par le biais d'un logiciel de compatibilité ukrainien. Même les logiciels antivirus peuvent se retrouver infectés, la preuve avec CCleaner qui prétendait nettoyer les PC sur lesquels on l'installait et qui a contaminé plus de 2 millions d'internautes [en 2017, NDLR] », complète-t-il.

Des recherches en perpétuelle évolution

« Avec 48 publications dans des revues de haut niveau, l'an dernier, l'expertise de notre agence est désormais reconnue à l'international », affirme Vincent Strubel, son sous-directeur « Expertise ». L'Anssi couvre ainsi un large spectre de compétences : de la cryptographie aux protocoles réseaux, en passant par l'intelligence artificielle (IA). « Cette dernière constitue autant une menace pour nos infrastructures qu'une chance, car elle nous permet aussi d'aller plus vite dans la détection de codes malveillants », énonce cet ingénieur venu de l'univers de l'aérospatiale. « Nous nous préparons aussi aux nouveaux défis que constitueront demain l'entrée en service des ordinateurs quantiques et la généralisation de la blockchain, même si je me garde bien de faire des pronostics en la matière », poursuit Vincent Strubel.

L'augmentation du nombre de systèmes industriels, de télécommunications, de transports ou de santé opérés à distance par le biais de systèmes d'information potentiellement vulnérables oblige les autorités à prendre cette menace « cyber-physique » très au sérieux. « Nous avons vu des hôpitaux, mais aussi des centrales d'énergie prises en otages par des cybergangs. Nous savons qu'à tout moment de telles agressions peuvent provoquer des morts. Nous n'avons pas d'autre choix que d'anticiper ces risques et de nous préparer à y faire face », émet Guillaume Poupard.

C'est la raison pour laquelle, l'Anssi promeut désormais son propre système d'exploitation sécurisé (CLIP OS) ainsi qu'une messagerie privée baptisée Tchap pour éviter que les plus hauts représentants de l'État n'utilisent des instruments étrangers (l'américain WhatsApp ou le russe Telegram) dont la fiabilité est désormais sujette à caution. C'est aussi pourquoi l'Anssi préconise que tous les achats de matériels sensibles (serveurs de télécommunications 5G notamment) auprès de fournisseurs étrangers fassent l'objet d'une autorisation préalable des services. « Il ne s'agit pas de montrer du doigt telle marque ou tel pays, mais juste de sécuriser les intérêts hexagonaux », justifie Guillaume Poupard, au moment même où est voté un texte de loi, souvent décrit comme antichinois. « Ce n'est pas parce que Donald Trump veut bannir Huawei ou ZTE que nous devons nous aligner sur eux. Nous savons bien quels enjeux commerciaux sous-tendent la bataille que se livrent Washington et Pékin. Nous n'entendons pas entrer dans ce jeu-là : ce ne sont pas des constructeurs que nous voulons rejeter. C'est plutôt une hygiène numérique que nous voulons promouvoir », conclut-il. Et ce combat ne pourra pas être conduit à la seule échelle du pays. « C'est bien au niveau européen que se situe l'enjeu », insiste Yves Verhoeven, sous-directeur « Stratégie » de l'Anssi. « De ce point de vue, l'adoption du Cybersecurity Act est un succès pour la France », surenchérit Amélie Perron, chargée de mission de l'agence pour les affaires politiques européennes et internationales.

En ouverture de sa conférence de presse, le directeur général de l'Anssi avait commencé par un « satisfecit » en soulignant le succès remporté par ses équipes lors d'un « exercice » de cyberguerre, organisé à Tallinn (Estonie), du 7 au 12 avril dernier. « Notre délégation qui comptait 60 experts en cyberdéfense (civils, militaires et réservistes) est parvenue à faire face à plus de 2500 cyberattaques en deux jours. La très bonne coopération des composantes cyber des armées, sous l'égide du commandement de la cyberdéfense (Comcyber), de la Direction générale de l'armement et de l'Anssi, nous a permis d'arriver en tête des 23 nations participantes. Mais nous ne savons pas si les autres puissances avaient vraiment envoyé leurs meilleurs éléments », a-t-il nuancé. Sur la Toile mondiale, les grandes manœuvres ont bel et bien commencé !

Source
lebigdata.fr
Bastien L
6 mai 2019

3. Le Japon crée des malwares défensifs en cas de cyberattaque militaire

Le Japon annonce la création de sa première cyberarme : un malware défensif, qui sera déployé en cas de cyberattaque militaire contre le pays. Ce dispositif sera déployé d'ici la fin de l'année 2019.

Depuis juin 2016, l'OTAN reconnaît officiellement l'espace informatique, le « cyber », comme un champ de bataille au même titre que les airs, le sol et la mer. Dans ce contexte, alors que le Japon

cherche à étendre et moderniser son armée pour faire face à la menace chinoise, le gouvernement annonce la création de « cyberarmes ».

Il s'agira de malwares, tels que des virus et des portes dérobées, spécialement conçus à des fins défensives. En cas de cyberattaque militaire, ces malwares seront utilisés contre l'ennemi. L'objectif sera sans nul doute de neutraliser son système informatique. Pour l'heure, toutefois, on ignore quelles seront exactement les capacités de ces maliciels…

Selon les porte-paroles du gouvernement, l'objectif principal sera avant tout de dissuader d'éventuels attaques contre le pays. Malheureusement, la notion de puissance dissuasive ne semble pas s'appliquer au domaine du cybernétique. Ainsi, alors que les Etats-Unis détiennent le plus large arsenal de cyberarmes, ils sont constamment pris pour cible par les hackers Nord-Coréens, Russes, Chinois et Iraniens.

Quoi qu'il en soit, ce malware de défense devrait être fin prêt d'ici la fin de l'année 2019. Il ne sera pas créé par des employés du gouvernement, mais par des sous-traitants spécialisés.

C'est la première cyberarme développée par le Japon. D'autres pays, tels que le Royaume-Uni, les Etats-Unis et l'Allemagne en ont déjà développé. De même, la Chine, la Russie, la Corée du Nord, l'Iran ou même Israël développent et utilisent des cyberarmes, mais ne le reconnaissent pas officiellement.

Source
Usbek & Rica
Vincent Lucchese
21 août 2019

4. Une cyberattaque pourrait faire « autant de dégâts qu'une attaque nucléaire »

C'est ce qu'affirme Jeremy Straub, chercheur américain en informatique, dans un article publié sur The Conversation. De nombreux systèmes de services vitaux pour les populations seraient déjà infiltrés par des logiciels malveillants, prêts à causer des dégâts majeurs en cas d'éclatement d'une cyberguerre.

En 2016, des hackers ont pris le contrôle d'une usine de traitement de l'eau potable américaine et ont changé la composition chimique des produits utilisés pour purifier l'eau. La même année, des cyberattaques s'en sont pris au réseau électrique ukrainien, menaçant de le détruire. En 2018, le réseau électrique britannique a été pénétré par des cybercriminels et une intrusion similaire a touché le réseau américain l'année suivante. En 2017, des usines pétrochimiques de l'Arabie saoudite ont été touchées par une cyberattaque avant que des systèmes de contrôle de pipelines américaines soient touchés à leur tour quelques mois plus tard. Le FBI craint que des installations nucléaires soient également la cible de cyberattaques.

Cette liste est dressée par Jeremy Straub, chercheur en informatique à l'université du Dakota du Nord, aux États-Unis. Dans un article publié le 16 août sur *The Conversation*, il argumente ainsi sur les dangers des cyberattaques et les destructions massives que générerait une cyberguerre. Il n'est pas le seul à tirer la sonnette d'alarme : nous serions actuellement en situation de « *cyberguerre froide* », nous expliquait en avril le chercheur à l'Ifri Julien Nocetti. La cyberguerre aurait même déjà commencé, nous disait quant à lui Boris Razon, co-auteur du livre-enquête *Les nouvelles guerres – sur la piste des hackers russes* (ARTE Editions/Stock), en mai 2019. Des cyberattaques russes contre l'Ukraine (qui auraient causé jusqu'à 10 milliards de dollars de dégâts en une seule journée), aux cyberattaques américaines contre l'Iran en juin dernier, l'ère de la cyberguerre semble donc déjà advenue.

Pénuries alimentaires et accidents industriels

Nous serions toutefois loin d'avoir pris la mesure du danger, selon Jeremy Straub, qui ose cette glaçante comparaison : une cyberattaque serait aujourd'hui susceptible de causer autant de dégâts et faire autant de victimes qu'une arme nucléaire. « *Contrairement à une arme nucléaire, qui vaporiserait toute personne dans un rayon de 30 mètres et tuerait presque tout le monde dans un rayon de 800 mètres, les morts causées par la plupart des cyberattaques interviendraient plus lentement. Les gens pourraient mourir à cause d'une pénurie alimentaire, d'énergie ou de gaz pour se chauffer ou d'accidents de voitures résultants d'un sabotage contre le système de signalisation. Cela pourrait concerner des régions très étendues, provoquant de nombreuses blessures et même des morts* », écrit le chercheur, qui illustre alors notre vulnérabilité par ses nombreux exemples d'attaques déjà recensées contre des industries ou réseaux vitaux pour les populations.

Et le pire serait à venir selon le chercheur : « *Jusqu'à présent, la plupart des incidents de hacking*

bien documentés, même ceux impliquant un gouvernement étranger, n'ont pas été beaucoup plus loin que le vol de données. Malheureusement, nous avons des indices indiquant que les hackers ont placé des logiciels malveillants dans les systèmes d'eau et d'énergie américains, où ils attendent, prêts à être déclenchés. L'armée américaine aurait aussi pénétré les ordinateurs qui contrôlent les systèmes électriques russes ».

Empoisonnements massifs, pénuries ou sabotage entraînant des catastrophes – « *une cyberattaque pourrait causer un évènement similaire à l'accident de Tchernobyl* » - seraient ainsi à portée de clic. Le problème, souligne Jeremy Straub, c'est qu'aucun garde-fou n'existerait contre ces nouvelles armes de destruction massive. Face à la menace nucléaire, l'équilibre des arsenaux et la menace de représailles ont permis à la stratégie de la dissuasion nucléaire de nous prémunir – jusqu'à présent – de l'apocalypse nucléaire. Or, l'origine d'une cyberattaque est bien plus facile à camoufler que celle d'un missile nucléaire. Et une cyberattaque peut commencer par une attaque de très faible niveau, avant de provoquer une dangereuse escalade. Ces deux caractéristiques de la cyberguerre rendent donc inefficiente la stratégie de la dissuasion qui a fonctionné face au risque nucléaire, s'inquiète le chercheur.

Augmenter la cybersécurité

Autre fragilité inquiétante pour Jeremy Straub : la culture du risque et les niveaux de cybersécurité des citoyens, des entreprises et des gouvernements sont loin d'être à la hauteur du danger encouru. « *Nos analyses montrent que seulement un cinquième des entreprises qui utilisent des ordinateurs pour contrôler leurs équipements industriels aux États-Unis les surveillent pour détecter de potentielles attaques – et que dans 40 % des cas où les attaques sont détectées, les intrus sont présents dans le système depuis plus d'un an* », écrit-il. Au cours de l'année écoulée, pas moins de trois-quarts des entreprises énergétiques auraient connu des intrusions dans leur réseau.

Se prémunir totalement des menaces que font planer ces cyberattaques semble impossible, et Jeremy Straub plaide plutôt pour faire en sorte de rendre leur survenue « *moins probable* ». La première chose à faire pour cela consiste à renforcer le niveau de cybersécurité de l'ensemble des acteurs et de renforcer tout particulièrement la sécurité des « *systèmes critiques* », comme les usines produisant des produits chimiques dangereux ou les entreprises de transport. Ce qui passe en premier lieu par le développement de la culture de la cybersécurité et la formation massive de professionnels. À l'heure actuelle, conclut-il, un quart des postes liés à la cybersécurité sont vacants aux États-Unis, et les personnes en poste ne sont pas toujours suffisamment qualifiées. La situation est tout aussi critique en France : selon une étude publiée en juin par le cabinet Vason Bourne, 78 % des entreprises françaises auraient des difficultés à recruter des responsables qualifiés en cybersécurité.

Source
letemps.ch
Boris Busslinger
27 novembre 2019

5. La défense suisse s'installe à l'EPFL pour dénicher des talents

À l'instar des États-Unis ou d'Israël, la Suisse lance un programme national pour tirer profit du potentiel des hautes écoles dans le domaine défensif. Une antenne de l'armée vient d'ouvrir à Lausanne, au plus près des meilleures start-up de l'école polytechnique.

Dans un discret bâtiment gris du parc d'innovation de l'EPFL, l'Office fédéral de l'armement (Armasuisse) termine d'installer son nouveau « cyberdéfense campus ». Centre de compétence chapeauté par le Département de la défense, le bureau ambitionne de répliquer ce qui se fait déjà depuis longtemps aux États-Unis et en Israël : dynamiser la recherche en matière de défense en créant des synergies entre l'industrie militaire et le domaine académique. Visite des lieux.

Débusquer les talents avant Google

« Ici nous allons encore mettre quelques écrans, explique Vincent Lenders, le nouveau directeur du campus. C'est encore en développement. » Dans un large open space avec vue sur le lac, le bureau sera l'une des trois antennes d'une nouvelle organisation distribuée entre Lausanne, l'École polytechnique fédérale de Zurich et la caserne de Thoune – où sont abrités les serveurs les plus sensibles du système. Quel objectif ce nouveau triptyque poursuivra-t-il exactement ? « Après l'attaque informatique contre Ruag en 2015, un plan d'action pour la cyberdéfense a été mis en place, explique Vincent Lenders. Ces centres font partie du plan. »

D'ici à fin 2020, un tiers d'étudiants, un tiers de professionnels du secteur de la sécurité et un tiers

d'employés d'Armasuisse y travailleront main dans la main. Soixante personnes réparties sur trois sites nationaux, dont vingt employés au bord du Léman, auront pour but de soutenir la défense suisse, mais aussi d'attirer de nouveaux talents. « Il faut les chercher tôt pour qu'ils n'aillent pas chez Google », plaisante Vincent Lenders. Pour les convaincre, le campus proposera prochainement des bourses pour l'écriture de thèses de master, de doctorat ou de post-doc. Assorties d'une place de stage.

Toute nationalité bienvenue

Et pour trouver les perles rares, le nouveau centre pourra compter sur Alain Mermoud, titulaire d'un doctorat HEC en système d'information. Celui-ci est également chargé de cours à l'université… et employé d'Armasuisse. « Depuis mon poste, je peux regarder quels étudiants paraissent prometteurs, explique-t-il. Et faire un peu de pub. » Les conditions de travail au sein du campus seraient bien moins stressantes que chez les géants de la technologie, loue ce dernier. Qui concède quand même un point noir : « Nous ne pouvons pas offrir de salaires équivalents. »

Qu'importe : Vincent Lenders est confiant, les profils nécessaires seront dénichés : « Tous les étudiants sont les bienvenus, ajoute-t-il. De toutes les nationalités. » Quid des potentiels problèmes d'espionnage ? « C'est un risque à prendre en compte, répond le fonctionnaire. En cas de doute et selon la sensibilité d'un dossier, des contrôles personnels de sécurité sont toutefois possibles.» A l'instar de l'agence américaine Darpa (Defense Advanced Research Projects Agency), le cyberdéfense campus lorgne également sur les capacités des start-up alentour. « Certaines d'entre elles partagent les mêmes préoccupations que nous pour protéger leurs données, juge le directeur. Des coopérations sont envisageables. »

Source
letemps.ch
Alexandre Steiner
18 mars 2022

6. Le bataillon Cyber, nouveau bras de l'armée suisse

La prise de commandement de cette entité militaire créée en début d'année s'est déroulée vendredi dans le canton de Neuchâtel. L'occasion de faire le point sur sa mission avec son commandant, le major EMG Davide Serrago.

Ambiance solennelle vendredi au Château de Colombier (NE). En fin d'après-midi s'y est déroulée la prise de commandement du nouveau bataillon Cyber de l'armée, dont la mise en œuvre a débuté le 1er janvier. Elle s'inscrit en parallèle de la transformation de la Base d'aide au commandement (BAC) en commandement Cyber début 2024.

Le nombre de cyberattaques contre des entreprises helvétiques a augmenté de 65 % l'an dernier, selon la société spécialisée israélienne Check Point. La guerre en Ukraine et les tensions géopolitiques mondiales font craindre une nouvelle hausse.

Concernant les infrastructures militaires suisses, le Département fédéral de la défense (DDPS) indique au *Temps* que les principaux risques identifiés sont une disponibilité limitée des systèmes en raison d'attaques par dénis de service (DDoS) ou de rançongiciels, ainsi que d'éventuelles pertes de données. « Nous détectons chaque année plusieurs dizaines de milliers d'événements de sécurité. Ils donnent lieu à plusieurs centaines d'incidents à la criticité et à la durée de résolution variables », une porte-parole.

Recrutement intensif

Dans ces circonstances, ce nouveau bataillon est l'une des mesures prises pour renforcer les capacités de réaction de l'armée face aux cybermenaces la visant. Au service de la BAC, sa mission porte sur trois domaines. « Cybersécurité, connaissance de la situation militaire cyber et cryptologie », détaille son commandant, le major EMG Davide Serrago.

Les restructurations en cours feront augmenter les effectifs dédiés à la cyberdéfense de 200 à près de 600 personnes. « Nous ne donnons pas de chiffre exact sur la composition du bataillon, poursuit-il. Nous prévoyons de recruter 200 miliciens d'ici à janvier 2024. C'est moins de 0,2 % du corps militaire, mais nous devons trouver des profils spécialisés pour augmenter nos compétences et assurer une meilleure résistance des équipes en cas de crise. »

Pour ce faire, l'armée recherche des jeunes suivant une formation dans l'informatique ou ayant un intérêt marqué pour la cybersécurité. « Beaucoup se présentent, notamment des étudiants des EPF, mais tous ne réussissent pas les tests de capacité. Ils doivent démontrer une certaine maîtrise technique pour pouvoir ensuite accéder à l'instruction de base déjà dispensée depuis 2018 », relève le commandant. Elle propose également une reconversion à des militaires affectés à d'autres troupes s'ils disposent des compétences requises.

Bénéfice indirect pour les acteurs civils

Est-il certain de trouver suffisamment de spécialistes, qui sont aussi de plus en plus recherchés dans l'économie privée et les institutions publiques ? « Comme nous parlons de miliciens, nous ne sommes pas en concurrence. Ces acteurs ont tout intérêt à employer des personnes qui disposent d'une formation militaire dans ce domaine, dont ils pourront aussi bénéficier. Nous collaborons avec ICT Switzerland, ce qui permet à nos soldats d'obtenir un brevet fédéral de spécialiste en cybersécurité s'ils disposent d'au moins un an d'expérience professionnelle. Tout le monde est gagnant », répond-il.

Le revers de la milice, c'est qu'après l'instruction de base, les membres du bataillon ne seront mobilisés que trois semaines par an pour gérer des problématiques en constante évolution. « C'est pour cela que nous misons sur des personnes qui travaillent en permanence sur ces questions, dans le monde professionnel ou académique, poursuit Davide Serrago. Nous évaluons régulièrement leurs compétences. Si elles ne répondent plus à nos exigences, nous les réaffectons à d'autres fonctions. » L'organisation des cours de répétition se fait de telle manière qu'une équipe soit à disposition de la BAC tout au long de l'année : « Nous ne pouvons pas nous permettre de ne pas être efficaces. »

Renfort massif et rapide en cas de crise

Pourquoi ne pas simplement renforcer les effectifs de la BAC avec des professionnels ? « Notre rôle est de pouvoir lui apporter un renfort massif et rapide en cas de crise grave. Si les cyberattaques deviennent si nombreuses qu'elle ne parvient plus à y faire face, nous nous pourrons être mobilisés. C'est à comparer avec le renfort apporté par l'armée aux hôpitaux durant la pandémie. »

En plus de leur soutien à la BAC, les spécialistes du bataillon Cyber peuvent être engagés en soutien subsidiaire aux autorités civiles, précise le DDPS. Mais uniquement lorsque les moyens dont elles disposent sont épuisés ou « qu'il est prouvé que les moyens nécessaires ne sont pas disponibles et ne peuvent pas être fournis dans l'ampleur requise et en temps voulu par des prestataires commerciaux ».

Pour Davide Serrago, l'armée n'est pas en retard dans le domaine de la cybersécurité, mais il concède qu'il y a encore beaucoup à faire pour gagner en flexibilité. « Nous avons pris conscience que nos moyens étaient trop limités pour répondre aux défis actuels. Avec les projets de bataillon et de commandement Cyber, je pense que nous sommes sur la bonne voie », conclut-il.

7. Pour l'OTAN, la cyberguerre a déjà commencé

Source
letemps.ch
Richard Werly
21 janvier 2022

Outre l'envoi en Ukraine d'experts en cybersécurité pour contrer les menaces russes, l'Alliance atlantique a conclu le 17 janvier un accord de coopération avec Kiev en matière de défense technologique.

Il ne porte pas d'uniforme. Il n'a pas le regard vissé sur les cartes de l'Ukraine et les images par satellite de ses frontières avec la Russie, scrutées en permanence depuis des mois par le

commandement militaire de l'Organisation de l'Atlantique nord (OTAN) basé près de Mons (Belgique). Le colonel Ludwig Decamps est pourtant, aujourd'hui, l'un des responsables les mieux informés des 30 pays alliés sur la réalité des actions de déstabilisation menées contre l'Ukraine, tandis que plus de 150 000 soldats russes, l'arme au pied, campent à proximité.

Patron de la NCI, l'agence d'information et de communication de l'Alliance, cet officier belge a la responsabilité d'acquérir et de moderniser les systèmes de défense technologique de l'OTAN (brouillage anti-drones, cybersécurité, radars…). Lundi 17 janvier, Ludwig Decamps a signé le nouvel accord de coopération entre l'Alliance et les autorités ukrainiennes, dont le but officiel est « d'approfondir la collaboration » et d'aider le pays « à moderniser ses technologies de l'information ». Un texte paraphé en urgence au QG bruxellois de l'OTAN, moins d'une semaine après l'envoi à Kiev d'experts chargés d'identifier les assaillants informatiques responsables des cyberattaques en série survenues en début d'année.

Attaques attendues

« Les assauts informatiques que l'Ukraine a subis depuis le début du mois – notamment contre plusieurs sites web gouvernementaux – étaient attendus, confirme une source diplomatique à l'OTAN. Le même type d'attaques avait eu lieu en 2015 et 2016, suite à l'invasion de la Crimée et au début des hostilités dans le Donbass, en particulier avant la visite conjointe de François Hollande et d'Angela Merkel à Moscou, Kiev et Minsk, à la mi-février 2015. A l'époque, les hackers appartenaient tous à un groupe baptisé « ver de sable » (Sandworm) que les experts de l'Alliance avaient ensuite identifiés comme liés au GRU, la direction générale du renseignement de l'armée russe.»

Bis repetita en ce début 2022 ? « La signature de l'accord par la NCI n'intervient pas par hasard», poursuit notre interlocuteur, selon lequel des moyens financiers supplémentaires vont être investis dans le « NATO-Ukraine Command, Control, Communication and Computers (C4) Trust Fund », un fonds dédié financé à ses débuts en 2015 par le Canada, l'Allemagne et le Royaume-Uni. En surface, la poursuite des négociations diplomatiques. Dans les profondeurs du web, la cyberguerre: «Il ne faut pas oublier que les communications entre les unités de l'armée ukrainienne sont particulièrement vulnérables, explique Michael Kofman, spécialiste de la Russie au Center for Naval Analysis (CNA) de Washington. Les experts de l'OTAN envoyés sur place depuis le 15 janvier sont sans doute là pour sécuriser ces réseaux informatiques militaires critiques. » D'autant que beaucoup d'infrastructures critiques ukrainiennes fonctionnent, dit-on, sur des programmes piratés…

Cas d'école

Cette guerre informatique n'est sans doute pas à sens unique. Depuis sa décision de réviser sa cyberdéfense, prise lors de son sommet de juin 2021 à Bruxelles, l'OTAN teste aussi, de son côté, les réseaux russes. Basé à Mons, comme son état-major, le QG cyber de l'Alliance est le pilier d'une éventuelle réaction collective en cas d'application de l'article 5 de la charte de l'OTAN – à savoir une attaque contre l'un des alliés – dont le principe a été acté l'an dernier. Deux pays neutres non membres de l'OTAN, la Suède et la Finlande, ont récemment demandé son assistance.

« On peut voir l'Ukraine de deux manières, expliquait récemment Oleh Derevianko, un expert basé à Kiev, au portail en ligne Politico. Soit comme un pays ami que l'OTAN doit secourir s'il est cyberattaqué. Soit comme un cas d'école, un champ de bataille qui permet à la Russie et à l'Alliance de se jauger à distance. Les destructions de réseaux comptent autant que les réponses qui sont apportées. » Cette guerre-là se nourrit d'elle-même : « L'Ukraine est un espace de tir informatique réel », tranche Kenneth Geers, consultant du centre de coopération sur la cyberdéfense de l'OTAN basé à Tallinn, en Estonie, un pays balte visé en 2017 par d'importantes cyberattaques attribuées à la Russie.

Source
letemps.ch
Alexandre Steiner
18 mars 2022

8. En silence, la Russie se fait piller ses données par les hackers

Ce n'était au départ que des attaques symboliques. Mais, depuis plusieurs jours, les hackers affiliés à Anonymous ciblent avec succès plusieurs institutions clés russes : la banque centrale, Rosatom ou encore Roskomnadzor, organisme chargé de la censure.

Une déclaration solennelle sur Twitter, la revendication d'une poignée d'attaques symboliques,

puis des actions reléguées au second plan derrière les atrocités de la guerre. Plus de cinq semaines après le début de l'invasion russe de l'Ukraine, les cyberattaques menées par des groupes opposés ne font presque plus de bruit. Et pourtant. Si le conflit se joue avant tout sur le terrain, une bataille au long cours se joue aussi en ligne. Et sur ce plan-là, la Russie est en train de perdre gros.

C'est un véritable siphonnage de données sensibles dont on parle aujourd'hui, touchant des institutions clés de la Russie, ayant trait à l'énergie, à la finance et à internet. Tout avait commencé le 24 février, premier jour de l'invasion, avec ce message mis en ligne par le collectif Anonymous : « Nous sommes officiellement en cyberguerre contre le gouvernement russe. » Des actions symboliques ont été entreprises dans la foulée. Ainsi, juste après le début des hostilités, des chaînes de télévision russes ont été piratées, avec la diffusion pendant quelques minutes d'images de la guerre. Le 20 mars, un groupe se revendiquant d'Anonymous affirmait avoir pris le contrôle d'imprimantes en Russie pour y publier 100 000 messages d'opposition à la guerre. Des missives similaires auraient été envoyées par SMS à 5 millions de numéros russes.

Banque centrale touchée

Mais Anonymous et des groupes affiliés, tels les hacktivistes polonais Squad303 et les Cyber Partisans biélorusses, sont allés beaucoup plus loin, galvanisés sans doute par l'appel de Mykhailo Fedorov, vice-premier ministre de l'Ukraine, qui affirmait que son pays était en train de créer une « armée informatique ». Le 16 mars, les hackers ont réussi à s'introduire dans les serveurs de Rosatom, l'agence nucléaire russe. Plusieurs gigaoctets de données ont été subtilisés, et Anonymous a affirmé qu'il n'allait pas pirater les centrales nucléaires elles-mêmes. Comme a pu le constater *Le Temps*, ces données sont en ligne – on y voit notamment la confirmation que la Suisse se fournit en Russie pour une partie du combustible de ses centrales nucléaires.

Le 24 mars, c'est la banque centrale de Russie qui était ciblée, avec succès, par des hackers, ceux-ci parvenant à s'emparer de plus de 35 000 fichiers. Là encore, *Le Temps* a pu voir une partie de ces documents, rédigés pour la plupart en russe. La masse de données est colossale, puisque 28 gigaoctets de données ont été exfiltrées. Les noms d'UBS ou de Morgan Stanley y figurent.

Noms d'agents du FSB

Un peu plus tôt, c'était Roskomnadzor, l'agence russe chargée notamment de faire respecter la censure draconienne dans le pays, qui avait été victime d'une cyberattaque, avec la publication de 360 000 fichiers. Le FSB, soit les services secrets russes, a aussi été l'une des victimes d'Anonymous. On trouve, peut-être en lien avec ce piratage, des photos de personnes s'entraînant au maniement des armes, ainsi que des copies de documents d'identité et les données personnelles de 620 agents. Le moteur de recherche Yandex, numéro un du marché russe, a aussi été piraté, avec pour conséquence la divulgation d'adresses e-mails et de mots de passe concernant 150 000 de ses utilisateurs.

Enfin, la filiale allemande du géant pétrolier Rosneft a elle aussi vu des pirates s'introduire dans ses serveurs, avec au total 40 téraoctets de données dérobées, dont 32 gigaoctets d'e-mails. Certains sont sans doute liés à Gerhard Schröder, l'ancien chancelier allemand aujourd'hui président de Rosneft Allemagne. Les hackers affirment avoir aussi réussi à siphonner le contenu de téléphones. Mais pour l'heure, aucune information s'y rapportant n'a été publiée.

Plusieurs risques

Que penser de ces données ? Le chercheur en cybersécurité indépendant Jeremiah Fowler, qui a analysé plusieurs de ces piratages, estime qu'Anonymous ne bluffe pas. Les vols ont bel et bien eu lieu, certains contenant des répertoires avec les identités de plus de 272 000 Russes. « Anonymous s'est révélé être un groupe très efficace pour pénétrer des cibles de valeur importante, des dossiers et des bases de données en Russie », écrivait récemment ce chercheur dans une analyse.

A priori, ce siphonnage de données, dont l'ampleur ne sera sans doute pas dévoilée avant longtemps, présente trois risques pour la Russie. D'abord, il mettra sans doute à nu des informations sensibles sur le fonctionnement de plusieurs institutions clés du pays, offrant des données précieuses à d'autres hackers, voire à des puissances étrangères. Le deuxième risque concerne les centaines de milliers, voire les millions, de Russes dont des informations personnelles figurent dans ces documents: ils pourraient, selon leur profil, devenir des cibles faciles pour des cyberattaques plus précises, voire des attaques physiques. Enfin, le troisième risque concerne le moral de la communauté des informaticiens, voire des hackers russes : depuis des décennies, leurs qualités sont louées sur la planète. Or, non seulement les cyberattaques russes contre l'Ukraine ne semblent pas

avoir eu d'effets majeurs, mais en plus, ce sont plutôt des organismes russes qui ont été attaqués.

Source
Blick.ch
Simon Marti
28 août 2022

9. La Russie cherche à influencer les élections occidentales depuis la Suisse

La Russie voudrait diviser l'Occident et influencer les élections. Le Service de renseignement de la Confédération a constaté que Moscou recourrait probablement à des infrastructures en Suisse, selon un document confidentiel que Blick a pu consulter.

La guerre de la Russie contre l'Ukraine est aussi une cyberguerre. Et sur le champ de bataille numérique, Moscou aurait les pays soutenant l'Ukraine dans sa ligne de mire.

En première ligne : les élections. Cela fait bien longtemps que le Service de renseignement de la Confédération (SRC) se demande s'il y a des influences et des manipulations. Un nouveau rapport du SRC affirme qu'à ce sujet, les citoyens suisses peuvent se rassurer : il est peu probable que la Russie tente d'influencer les élections fédérales de l'année prochaine, écrivent les services secrets dans ce document confidentiel que Blick a pu consulter.

Mais ce n'est toutefois pas une raison pour lever l'alerte, poursuivent-ils. Moscou tente manifestement de saper les processus démocratiques dans d'autres Etats. Et ce, à l'aide de l'infrastructure suisse. « Le SRC estime probable que des serveurs situés en Suisse soient utilisés pour de futures cyberattaques contre d'autres élections occidentales. » Ce qui sape la souveraineté de la Suisse, concluent-ils.

Mélange de désinformation, propagande et cyberattaques

Avec la guerre en Ukraine, les possibilités de la Russie d'influencer les Etats occidentaux par des moyens politiques ou économiques ouverts se sont amenuisées. « C'est pourquoi le SRC estime qu'il est très probable que ce pays continue, même après la césure que représente la guerre, à manipuler la politique dans les pays occidentaux par des activités d'influence telles que l'influence électorale, poursuit le rapport confidentiel. Pour ce faire, elle continuera à miser sur un mélange personnalisé de désinformation et de propagande, sur des cyberattaques, sur des personnes, des groupes et des institutions instrumentalisés et probablement aussi sur de nouveaux moyens ».

L'ingérence dans les élections serait pour la Russie un moyen d'atteindre l'objectif général d'affaiblir la communauté des Etats occidentaux. Les services secrets sont formels : même si cette influence ne change pas le résultat d'une élection, « elle délégitime en partie la prise de décision démocratique et donc le modèle libéral-démocratique 'occidental' ».

Miner le système

Des ordinateurs suisses pourraient-ils être utilisés dans ce cadre ? Tout à fait, selon le programmeur et conseiller national Vert'libéral Jörg Mäder, qui évalue que ce scénario est «tout à fait plausible». « Je peux imaginer que des serveurs puissent par exemple être loués en Suisse via une société écran, dans le but de dissimuler l'origine de la propagande », explique le Zurichois.

Markus Christen est l'un de ceux qui s'occupent précisément de cette question. Il dirige la Digital Society Initiative à l'université de Zurich et mène notamment des recherches sur l'éthique des systèmes de communication, l'intelligence artificielle et la cybersécurité. «Pensons aux trolls des médias sociaux ou aux programmes qui génèrent automatiquement des entrées qui énervent tout le monde. Ces actions doivent bien passer par une certaine infrastructure», s'exclame-t-il.

Il est possible que des différences juridiques par rapport à l'Union européenne rendent les serveurs suisses dignes d'intérêt, avance le chercheur. Ou alors les services russes concentrent de plus en plus leurs activités en Suisse parce que d'autres Etats européens ont expulsé plusieurs de leurs diplomates russes.

« Saper la confiance des électeurs »

Mais comment ces campagnes de désinformation pourraient-elles influer sur un vote ? Les électeurs ne retournent en général pas si facilement leur chemise. « On ne vote bien sûr pas soudainement pour un autre parti, reprend Markus Christen. Par contre, de telles actions peuvent aider à saper la confiance des électeurs vis-à-vis de leur système politique. » Ainsi, l'enveloppe de vote ne serait pas différente, mais il n'y aurait plus d'enveloppe du tout : cette désinformation aurait

pour effet de faire monter le taux d'abstention.

En juin, Microsoft a publié une étude détaillée sur les combats online de la Russie. De nombreuses opérations de cyberinfluence russes ne seraient pas rendues publiques ou passeraient carrément inaperçues, s'inquiète le géant de l'informatique. Outre les cyberattaques dévastatrices sur des cibles en Ukraine et l'espionnage à grande échelle, la stratégie aurait pour but de saper l'unité occidentale.

Attaques contre Annalena Baerbock

Et Moscou opérerait à long terme. Pour le service de renseignement suisse, c'est certain: la Russie a tenté dès 2021 en Allemagne de manipuler les résultats des élections en sa faveur par le biais d'un matraquage médiatique et de cyberattaques, pointe-t-il du doigt. Les réseaux de propagande auraient notamment pris pour cible l'actuelle ministre des Affaires étrangères des Verts, Annalena Baerbock. Des tentatives d'intrusion dans les comptes de messagerie de politiciens et de partis auraient également eu lieu. Les agresseurs étaient en relation avec le service de renseignement militaire russe GRU, accuse le SRC.

Quelles sont les futures cibles ? Les services secrets ne citent aucun nom dans le document. « Le SRC estime que les Etats ayant une influence moyenne à grande sur la politique européenne ou mondiale, un système électoral vulnérable (plutôt des élections au scrutin majoritaire) ainsi qu'une liste de candidats fortement polarisée par rapport aux affaires importantes pour la Russie constitueront des cibles opportunes pour les manipulations électorales de la Russie. »

Même sans indication explicite des analystes, des regards inquiets se tournent vers le sud. Le 25 septembre, l'Italie votera. La droite de Giorgia Meloni a de bonnes chances de remporter le scrutin. Alors que la «post-fasciste» soutient le cours occidental du gouvernement encore en place, ses alliés sont dans une tout autre position. Le chef de la Lega, Matteo Salvini, remet publiquement en question les sanctions contre la Russie. Et l'éternel Silvio Berlusconi se flatte de son amitié avec l'autocrate russe Vladimir Poutine.

Empêcher la cyberguerre en Suisse

L'enjeu est donc de taille. Et pour de nombreux parlementaires suisses, l'idée que Moscou essaie d'influencer de telles élections via la Suisse est insupportable. «En tant que pays neutre, la Suisse doit empêcher la cyberguerre sur son territoire!», tonne Fabian Molina, membre du PS chargé des affaires étrangères. « Les autorités doivent tout mettre en œuvre pour que le plan russe n'aboutisse pas », assène le conseiller national.

Gerhard Andrey, conseiller national vert, abonde aussi dans ce sens. « Le SRC doit s'éloigner de la surveillance des citoyens et se concentrer beaucoup plus sur un contre-espionnage efficace », tance-t-il. «Nous savons que la Suisse est un pays attractif pour l'espionnage classique. Cela vaut bien entendu aussi pour les opérations dans l'espace numérique», explique le Fribourgeois.

Celui qui est également programmateur informatique pense notamment aux diplomates de l'Est accrédités en Suisse. Selon la Confédération, il est très probable que des agents russes agissent directement depuis la Suisse, poursuit-il. « Ils disposent ici de l'infrastructure technique nécessaire, sans qu'il soit nécessaire d'accéder aux ordinateurs locaux depuis l'étranger. »

« La Suisse devrait aussi expulser ces personnes »

Or, si la Suisse devient de plus en plus le point de départ de tentatives de manipulation et de cyberattaques, la réputation du pays en pâtira, argumente encore Gerhard Andrey. Dans ce contexte, il faut noter que d'autres Etats européens ont expulsé à tour de bras des collaborateurs d'ambassades russes. « Et beaucoup d'entre eux semblent avoir atterri en Suisse. En cas de soupçon d'espionnage, la Suisse devrait aussi expulser ces personnes », assène encore le conseiller national des Verts.

Interrogée par Blick, une porte-parole du service de renseignement explique que le SRC ne s'exprime généralement pas sur ses activités et procédures opérationnelles. Elle reconnaît toutefois que « la Suisse, en tant qu'Etat européen et membre de la communauté de valeurs occidentale, est bien la cible d'activités d'influence dirigées contre les sociétés occidentales et qui portent la narration russe. »