OBSERVATOIRE DU MONDE CYBERNÉTIQUE

Lettre n°38 - **mai 2015** - **disponible sur omc.ceis.eu**

Brève du mois

"*The license review policies for cybersecurity items controlled under NS and AT will not be revised. A new license review policy for cybersecurity items is proposed under § 742.6(b) for regional stability. Cybersecurity items controlled for RS are proposed to be reviewed favorably if destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1, foreign commercial partners located in Country Group A:5, government end users in Australia, Canada, New Zealand or the United Kingdom, and on a case-by-case basis to determine whether the transaction is contrary to the national security or foreign policy interests of the United States, including the foreign policy interest of promoting the observance of human rights throughout the world.*" **Modification de l'arrangement de Wassenaar proposé le 20 Mai 2015[1].**

LE RAPPROCHEMENT SINO-RUSSE DANS LE CYBERESPACE

Les Etats-Unis dominent toujours le cyberespace mais les BRICS (Brésil, Russie, Inde, Chine, Afrique du Sud) contestent de plus en plus fortement cet ordre établi.

La République populaire de Chine et la Fédération de Russie sont en premières lignes sur ce sujet, et défendent une approche souveraine opposée à celle des Etats-Unis de l'internet global et ouvert. En septembre 2011, la Chine, la Russie, le Tadjikistan et l'Ouzbékistan ont soumis à l'Organisation des Nations Unies une proposition conjointe sur la bonne conduite sur Internet[2].

[1] https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items
[2] https://web.archive.org/web/20120113233019/http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf

Le document stipule que les pays respectueux des droits de l'Homme et des libertés fondamentales s'engagent à soutenir « *la lutte contre les activités criminelles et terroristes qui utilisent des technologies de l'information et de la communication, y compris les réseaux* ». Mais, il prévoit que les états signataires de ce texte doivent également s'engager à « *réduire la dissémination de l'information qui incite au terrorisme, à la sécession, à l'extrémisme ou qui nuit à la stabilité politique, économique et sociale ainsi qu'à l'environnement spirituel et culturel* » des différents pays. Une façon de permettre, comme l'ancien vice-président américain Joe Biden l'a observé, de « *conduire exclusivement à un contrôle gouvernemental des ressources présentes sur Internet, des institutions et du contenu et des frontières nationales à la libre circulation de l'information en ligne* »[3].

Le deuxième point d'opposition porte sur la lutte anti-cybercriminalité. Les Etats-Unis ont fait de la lutte anti-cybercriminalité le fer de lance de leur stratégie de cybersécurité ; la Russie dispose elle d'un écosystème cybercriminel très développé, a minima toléré par les autorités et surtout protégé par une législation qui ne reconnait pas la cybercriminalité comme un délit. Une enquête menée par des chercheurs basés en Russie[4] souligne ainsi le laxisme des lois russes qui ont permis à des groupes très organisés de se développer, parfois sous le contrôle de la mafia. Alors que les Etats Unis offrent près de 3 millions de dollars pour des informations permettant d'arrêter le pirate russe Evgueni Mikhaïlovitch Bogachev, considéré comme l'un des plus importants cybercriminels mondial[5], les mêmes pirates disposent en outre d'un réel capital sympathie aux yeux de l'opinion publique russe. Un capital alimenté par un fort ressentiment anti-occidental et une vision quasi romantique de la cybercriminalité, puisque le vol informatique est souvent considéré comme un outil de redistribution et « une forte de justice sociale »[6]. Impossible, enfin, pour un gouvernement occidental de faire extrader des cybercriminels russes, ce qui leur permet d'agir en toute impunité : la Fédération de Russie n'a pas adhérée à la Convention internationale sur la cybercriminalité[7] du Conseil de l'Europe du 23 novembre 2001.

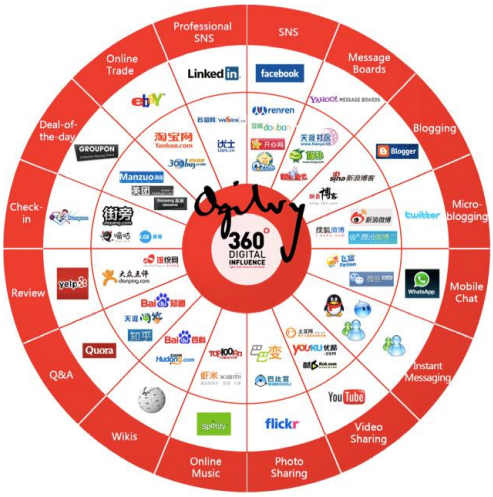
Les révélations Snowden n'ont évidemment pas arrangé les choses et la Russie cherche plus que jamais à maitriser « son » cyberespace. Le ministre des télécommunications Nikolai Nikiforov a ainsi annoncé en 2014 la préparation d'un plan d'action au cas où le segment russe de l'Internet serait fermé de l'extérieur[8]. Le président Poutine a lui-même déclaré qu'il désirait que toutes les infrastructures connectées russes soient hébergées en Russie, Internet étant un « projet de la CIA»[9]. La Russie s'est également engagée à créer d'ici à 2016 des services permettant de stocker sur le territoire russe les données personnelles de ses résidents.

Sous couvert de la protection des données personnelles et de la lutte contre la cybercriminalité, la législation russe a en outre mis en place un contrôle de l'information sur internet. Une loi oblige ainsi les blogs ayant plus de 3 000 lecteurs inscrits à se déclarer auprès du ministère de la Communication, tandis qu'une autre oblige l'identification des utilisateurs de WIFI public ou d'entreprise. Dans le même élan, une loi initialement rédigée pour la protection de l'enfance a été détournée pour supprimer l'accès à des sites contestataires[10].

Côté chinois, on retrouve les mêmes velléités du gouvernement en matière de contrôle de l'information, avec des moyens nettement supérieurs. La protection de l'Internet y est

[3] http://www.huffingtonpost.com/2011/11/02/london-conference-on-cyberspace_n_1071242.html
[4] http://www.lemondeinformatique.fr/actualites/lire-comment-la-russie-est-devenue-une-superpuissance-de-la-cybercriminalite-48739.html
[5] http://www.lefigaro.fr/flash-actu/2015/02/24/97001-20150224FILWWW00410-usa-3m-pour-trouver-un-cyber-criminel-russe.php
[6] http://www.lexsi-leblog.fr/cert/les-cybercriminels-russophones-lassaut-finances-occidentales.html
[7] http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm
[8] http://www.wsj.com/articles/moscow-considers-moves-to-secure-and-defend-internet-in-russia-1411145000
[9] http://fr.euronews.com/2014/04/26/poutine-internet-est-un-projet-de-la-cia/
[10] http://www.infoguerre.fr/guerre-de-l-information/strategie-de-puissance-russe-dans-le-cyberespace-5644

assurée par le « Grand Firewall », par une police qui possèderait 2 millions d'agents ou d'informateurs en 2013[11](contre 40 000 en 2007[12]) et des règlementations très strictes (le gouvernement a contraint les fournisseurs d'accès à fournir les coordonnées des utilisateurs). Le pays ne veut pas contrôler uniquement les flux, mais aussi ce qu'ils contiennent. Les réseaux sociaux tels que Twitter ou Facebook y sont toujours interdits, la Chine interdisant progressivement de plus en plus de technologies américaines et services web qui ne peuvent que difficilement être surveillés[13]. Motivée par des raisons idéologiques, cette stratégie se révèle également payante au plan économique. Chaque service web étranger a aujourd'hui son pendant chinois, contrôlé et maîtrisé par le gouvernement.



Source: Ogilvy-360 Digital Influence

Le président chinois a accentué la politique de répression de la liberté d'expression sur le web. Un utilisateur chinois, Dong Rubin, a été arrêté par exemple au mois de septembre de 2013 et condamné à 6 mois de prison pour avoir créé un blog[14]. Le Parti mène ainsi une politique de « nettoyage de l'internet[15] » qui a commencé par l'arrestation de près de 30 000 personnes dans le cadre d'enquêtes sur la pornographie en ligne et les paris clandestins. Le Vice-Président du Bureau de l'Information du Conseil d'état chinois a jugé que ces sites « polluaient gravement la morale sur l'internet[16] ». A noter que le pays n'a pas non plus ratifié la Convention de Budapest du 8 novembre 2001[17].

Les deux pays se sont enfin dotés d'organisations de cyberdéfense pour protéger leurs souverainetés numériques respectives. La Russie a ainsi ouvert un centre de contrôle national de la défense[18] pour protéger son cyberespace[19], tandis que la Chine, qui utilise désormais clairement la notion de souveraineté du cyberespace[20], a reconnu très récemment de façon officielle l'existence de capacités offensives au sein de l'Armée Populaire de Libération répartis au sein de trois sections spécialisées[21].

Au-delà de ces préoccupations communes, la Russie et la Chine se sont engagées également depuis quelques années dans un rapprochement bilatéral sans précédent en matière de cyberespace.

Le 8 mai 2015, une nouvelle étape dans la coopération été franchie avec la signature d'un accord bilatéral de non-agression et de coopération qui est passé presque inaperçu, parmi les 32 accords très divers qui ont été signés ce même jour entre les deux nations[22].

[11] http://www.lemonde.fr/asie-pacifique/article/2013/10/05/deux-millions-d-agents-pour-surveiller-le-net-chinois_3490636_3216.html
[12] http://www.lemonde.fr/technologies/article/2007/08/28/la-censure-sur-internet-etats-contre-cyberdissidents_948415_651865.html
[13] http://www.usine-digitale.fr/article/windows-media-player-et-internet-explorer-vises-par-l-enquete-chinoise-contre-microsoft.N280114
[14] http://chrdnet.com/2014/08/prisoner-of-conscience-dong-rubin/
[15] http://www.franceinfo.fr/actu/monde/article/internet-la-chine-entre-reprise-en-main-et-lutte-contre-la-cybercriminalite-622173
[16] http://lexpansion.lexpress.fr/high-tech/la-chine-veut-nettoyer-internet-de-la-pornographie_1426890.html
[17] http://fr.jurispedia.org/index.php/D%C3%A9lits_de_la_cybercriminalit%C3%A9_%28fr%29
[18] http://tass.ru/en/russia/767317
[19] http://www.wsj.com/articles/moscow-considers-moves-to-secure-and-defend-internet-in-russia-1411145000
[20] http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/
[21] http://www.nextinpact.com/news/93527-la-chine-reconnait-enfin-existence-ses-hackers.htm
[22] http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0

Selon le projet d'accord[23], non disponible sur le site en anglais du gouvernement russe, il est convenu d'une non-agression dans le cyberespace entre la Russie et la Chine et le non-recours à leurs outils et aux infrastructures des deux pays pour mener à bien des cyberattaques contre l'autre : « *Article 4 Point 3 : chaque Partie a un droit égal à la protection des ressources d'information de son état contre l'utilisation illégale et l'intervention non autorisée, y compris contre des cyber-attaques sur ces ressources. Chaque Partie n'effectue pas des actions de ce genre par rapport à l'autre Partie et prête assistance à l'autre Partie dans l'application de ce droit.* »

Il est aussi stipulé dans cet accord, le partage des informations relatives aux opérations de cybersécurité et à la sécurité de leurs infrastructures de communication : « *Article 3 Point 5 : l'échange d'informations et la coopération dans l'application de la loi pour enquêter sur les affaires qui impliquent l'utilisation de technologies de l'information et de la communication pour fins terroristes et criminelles.*

Article 3 Point 7 : La coopération entre les autorités compétentes des Parties pour assurer la sécurité de l'infrastructure critique de l'information[24] des Parties, l'échange des technologies et la coopération entre les autorités compétentes des Parties afin de réagir aux incidents informatiques.

Article 3 Point 15 : la mise en place d'un mécanisme de coopération entre les autorités compétentes des Parties pour l'échange d'informations et l'utilisation commune d'informations sur les risques, les menaces et les vulnérabilités existantes et potentielles dans le domaine de la sécurité de l'information, leur identification, évaluation, étude, échange réciproque à leur sujet et prévention de leur apparition. »

Dernier sujet couvert par cet accord, la coopération entre les deux puissances pour contrer les technologies pouvant nuire à l'ordre public ou interférant avec les affaires internes de l'Etat. « *Article 3 Point 4. Réponse commune aux menaces dans le domaine de la sécurité informationnelle telle que définis dans l'Article 2 de l'Accord;*

Article 2 Les principales menaces dans le domaine de sécurité de l'information internationale

Sont considéré comme menaces l'utilisation des technologies de l'information et de la communication en vue de :

1. *procéder à des actes d'agression visant à la violation de la souveraineté, la sécurité, l'intégrité territoriale des Etats et une menace pour la paix internationale, la sécurité et la stabilité stratégique*
2. *porter atteinte préjudice à de dommages économiques et autres, y compris à travers un impact destructeur sur les objets de l'infrastructure de l'information;*
3. *à des fins terroristes, y compris pour la promotion du terrorisme et le recrutement dans des activités terroristes des nouveaux adhérents ;*
4. *commettre des infractions et de crimes, y compris ceux liés à l'accès non autorisé aux données informatiques ;*
5. *interférer dans les affaires intérieures des États, les violations de l'ordre public, l'incitation à la haine ethnique, raciale et religieuse, la propagande des idées et des théories racistes et xénophobes qui donnent lieu à la haine et à la discrimination, l'incitation à la violence et l'instabilité, ainsi que la déstabilisation de*

[23] http://government.ru/docs/17952/

[24] *« systèmes d'information, réseaux d'information et de télécommunication des autorités publiques; systèmes d'information, réseaux d'information et de télécommunications et systèmes automatisés de contrôle de processus opérant dans l'industrie de la défense, santé publique, transport, communication, crédit et finance, énergie, industries nucléaire, aérospatiale, minière, métallurgique et chimique. »*

la situation politique et socio-économique interne, violation de la gestion étatique ;

6. *diffuser des informations préjudiciables aux systèmes socio-politiques et socio-économiques, spirituelles, morales et de l'environnement culturel des autres États. »*

Cette coopération encourage donc les deux pays à échanger des informations, à travailler ensemble et à protéger leurs intérêts communs, afin de *« (…) contrer les technologies pouvant nuire à l'ordre public ou interférant avec les affaires internes de l'Etat.* ». Les termes utilisés sont sans ambiguïtés : il s'agit de lutter ensemble contre l'utilisation de technologies qui risqueraient de « *Déstabiliser l'atmosphère politique et socio-économique interne* », « *troubler l'ordre public* » ou « *interférer avec les affaires intérieures de l'État* ».

Cette posture défensive se double d'une approche industrielle, la Russie ayant, à l'instar de la Chine[25], annoncé vouloir développer avec une société finlandaise un système d'exploitation mobile souverain[26].

Ce rapprochement s'inscrit enfin dans une dynamique de coopération croissante entre les deux pays.

Au plan économique, le volume du fonds d'investissement russo-chinois atteignait près de 4 milliards de dollars en 2012[27]. Notons également que la Chine est l'un des premiers consommateurs mondiaux d'énergie et que la Russie est l'un des principaux producteurs d'hydrocarbures[28]. La Russie a ainsi signé un contrat à 400 milliards de dollars pour la livraison de gaz à la Chine[29]. De même, depuis janvier 2011, un gazoduc permet le transport annuel d'environ 15 millions de tonnes de pétrole de la Russie vers la Chine.

D'un point de vue militaire, enfin, la Russie et la Chine sont aujourd'hui des puissances militaires de premier ordre et de nombreuses coopérations ont été initiées. Les deux pays mènent des exercices militaires communs[30] (le dernier en date est l'exercice naval *Joint Sea*, mené en méditerranée du 11 au 21 mai 2015[31]) et ont signé en novembre 2014 plusieurs accords de coopération militaire lors de leur « 17ème ronde de consultations stratégiques »[32].

Contrairement aux membres du BRICS, comme la Brésil et Inde qui voient la maîtrise d'Internet comme la clef de leur développement économique, la Chine et la Russie la considèrent comme un instrument politique. Ce rapprochement est donc une étape de plus dans un cloisonnement du cyberespace entre superpuissances.

[25] http://www.usine-digitale.fr/article/apres-la-chine-la-russie-veut-elle-aussi-reduire-sa-dependance-a-ios-et-android.N330557
[26] http://www.numerama.com/magazine/33127-la-russie-veut-son-propre-os-mobile.html
[27] http://fr.sputniknews.com/economie/20120428/194488789.html
[28] http://www.opex360.com/2012/06/06/la-russie-et-la-chine-vont-accroitre-leur-cooperation-militaire/
[29] http://www.jeuneafrique.com/Article/JA2788p048.xml0/
[30] http://www.opex360.com/2012/04/22/la-chine-et-la-russie-entament-des-manoeuvres-navales-conjointes/
[31] http://fr.sputniknews.com/international/20150505/1015957937.html
[32] http://french.peopledaily.com.cn/n/2014/1106/c31354-8805374.html

SATELLITE : QUELLES VULNERABILITES AUX ATTAQUES INFORMATIQUES ?

Satellite SICRAL 2 - Source: Thalès

Le mois dernier, le 26 avril 2015, a été mis en orbite avec succès le satellite artificiel Sicral 2[33]. Issu du programme de coopération franco-italien, ce satellite vient renforcer les satellites de télécommunications militaires français et italiens déjà positionnés, afin d'assurer des liaisons stratégiques et tactiques. Ce lancement intervient après la mise en orbite en 2005 et 2006 de Syracuse III, la troisième génération du programme Syracuse, dont l'objectif était de créer un réseau de télécommunications militaires français sécurisé grâce à des satellites dédiés, non partagés avec des organismes civils comme ces prédécesseurs (les 4 satellites prédécesseurs du programme Telecom 2, étaient cogérés avec France Telecom par exemple). Il y a donc maintenant un contrôle complet de la charge utile par les armées françaises.

Les satellites ont en effet pris une place de plus en plus importante dans le monde militaire, avec différentes spécialités :

- le satellite de télécommunication militaire, dont l'objectif est de permettre la communication entre les unités déployées sur le terrain, et les structures, à l'aide de liaisons sécurisées. (Syracuse III en France),

- le satellite de reconnaissance, dont l'objectif est d'obtenir des cartographies d'un territoire et d'identifier des installations fixes, armes et troupes. (HELIOS et bientôt MUSIS en France),

- le satellite d'écoute électronique, dont l'objectif est de capter les signaux radio (CERES pour 2020 en France),

- le satellite d'alerte précoce, dont l'objectif est de détecter le lancement de missiles balistiques, à l'aide de détecteurs infrarouges. (Satellites expérimentaux SPIRALE[34] en France).

L'évolution des satellites a profité de la course effrénée entre les Etats-Unis et l'URSS lors de la guerre froide. Le premier satellite artificiel, Spoutnik 1, fut lancé en 1957 par les soviétiques ; son unique mission était d'émettre un simple signal radio, afin de démontrer l'avance soviétique aux américains dans le domaine des fusées[35]. Puis, au fur et à mesures des années, les applications militaires se sont développées dans l'espace, leurs utilisations ont été démocratisées au monde civil et les satellites porteurs d'armes de destruction ont été interdits[36]. Aujourd'hui, on retrouve la technologie satellitaire partout autour de nous : GPS, télécommunications, télévision, internet, etc.

[33] http://www.defense.gouv.fr/salle-de-presse/communiques/ministre/lancement-reussi-du-satellite-franco-italien-de-telecommunications-militaires-sicral-2
[34] http://www.defense.gouv.fr/actualites/articles/spirale-premier-pas-vers-l-alerte-avancee
[35] http://nssdc.gsfc.nasa.gov/sound/sputnik.wav
[36] https://www.admin.ch/opc/fr/classified-compilation/19670016/index.html

En près de 50 ans, les pays les plus industrialisés sont ainsi devenus de plus en plus dépendants des moyens spatiaux, sur le plan militaire comme civil, ce qui renforce la nécessité de prendre en compte dès leur conception les différentes menaces, parmi lesquelles la menace informatique. Comme tout système informatisé, les satellites sont en effet vulnérables aux attaques informatiques, que celles-ci aient pour objectif d'atteindre l'intégrité des données, leur confidentialité, ou bien la disponibilité des charges utiles du satellite.

Selon une étude de la NASA de 2008, 20% des destructions de satellites ne sont pas expliquées et certaines pourraient bien résulter d'attaques informatiques. L'explosion, début février 2015, d'un satellite militaire américain de l'US Air Force DMSP-F13[37] après « une soudaine hausse de température », probablement due, selon les sources officielles, à une défaillance du système d'alimentation montre qu'une faiblesse sur l'un des équipements informatisés peut avoir des conséquences radicales sur le satellite. La sécurité informatique est donc devenue un véritable enjeu pour les constructeurs de satellites. Le sujet est aussi prioritaire pour les gouvernements, comme pour les pirates, au point que la sécurité des satellites constitue aujourd'hui l'un des piliers de la stratégie de cybersécurité gouvernementale.

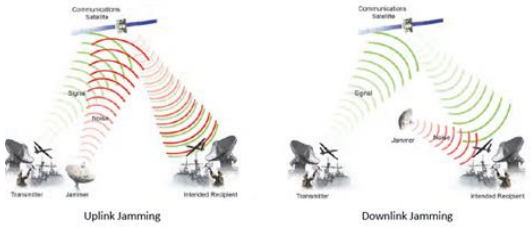
De nombreuses attaques et vulnérabilités ont été observées sur les systèmes satellitaires.

Le brouillage des liaisons montantes et descendantes (*Uplink & Downlink Jamming*) est depuis longtemps la menace la plus sérieuse et la plus facile à mettre en œuvre contre les satellites artificiels. Elles consistent à pointer vers le satellite des antennes émettant à la même fréquence pour la liaison montante (*Uplink)* ou à utiliser des émetteurs de grande puissance pour la neutralisation de la liaison descendante (*Downlink*).

Il est aussi possible de brouiller le signal directement au niveau de la station destinataire au sol, mais ce type d'attaque provoque des dommages moins importants, et affecte uniquement les utilisateurs se trouvant dans la ligne de mire du brouilleur.

Ces attaques sont réalisées sur des satellites artificiels géostationnaires, couvrant une large zone géographique, voire même un continent. Les satellites géostationnaires sont donc « accessibles » à partir de n'importe où dans leurs zones de couverture, et constituent ainsi une cible facile, contrairement aux satellites artificiels orbitaux.

Dans un brouillage satellitaire, l'attaquant envoie un faisceau de signaux contradictoires directement vers un satellite via une *rogue* station de liaison montante. Les signaux de brouillage sont mélangés avec les signaux légitimes, interférant ainsi avec eux. Ces signaux de brouillage sont ainsi en mesure de remplacer la transmission légitime, ce qui bloque cette dernière avant d'avoir pu renvoyer le signal au destinataire. De plus, cette attaque est assez difficile à détecter, en particulier si elle est produite à des intervalles irréguliers.



Présentation des méthodes de brouillage des signaux Uplink et Downlink

En juin 2009, le satellite Hot Bird 6, utilisé notamment par BBC Persian, a par exemple été la cible d'attaques par brouillage, ce qui a poussé la chaine de télévision à se replier vers un satellite moins puissant au moment des élections iraniennes[38]. Cette attaque a fortement bouleversé les différents services qu'il fournissait, tel qu'internet et la télévision.

[37] http://spacenews.com/20-year-old-military-weather-satellite-wasnt-first-of-its-kind-to-explode/

[38] http://www.theguardian.com/media/2009/jun/19/iran-bbc-worldwide

D'autres méthodes d'attaque sur le signal, comme la surcharge du signal (*Overpower Uplink*) peuvent également être relevées. La faisabilité de celle-ci a été démontrée par un ingénieur américain utilisant le pseudonyme de Captain Midnight en avril 1986[39] lorsque ce dernier, mécontent des tarifs de l'opérateur a remplacé la diffusion des programmes par un message de protestation. En 1987, deux chaînes de télévision américaines, la WGN-TV et la WTTV, sont attaquées à quelques heures d'intervalle : une vidéo montrant un homme masqué interrompt quelques dizaines de secondes les programmes. Cet incident est resté connu sous le nom de Max Headroom, héros d'une série Britannique des années 80 qui faisait passer des messages en s'introduisant de cette manière dans les signaux de télévision[40]. Au plan technique, l'attaque consiste à surcharger énergétiquement le satellite, afin de faire passer son signal en priorité, ou de saturer le satellite (au point parfois de l'endommager). Pour contrer ces attaques, la meilleure solution consiste à identifier les signaux afin de valider les signaux entrants.

Contrairement aux signaux HF, VF et UHF présents sur Terre, où l'utilisation de puissance électrique supplémentaire permet d'émettre un meilleur signal, la communication satellitaire a elle besoin de signaux faibles pour fonctionner[41], afin, entre autres, d'économiser les batteries équipant les satellites (elles se rechargent via les panneaux solaires). En effet, un satellite recevant un signal montant de forte puissance, générera un signal de même niveau électrique, en puisant sur les batteries du satellite, afin d'émettre un signal sortant identique.

Le risque d'attaque de brouillage est encore accru par le fait que les équipements de guerre électronique sont largement accessibles, non seulement pour les états, mais aussi pour les groupes terroristes ou les organisations criminelles. Les brouilleurs terrestres portables sont en effet faciles à acheter et à utiliser : ils ont généralement une portée de 3 à 5 kilomètres en zone urbaine, et peuvent atteindre les 20 kilomètres en zone rurale. Lors de l'opération *Freedom Iraq*, des brouilleurs terrestres de la société russe Aviaconversiya[42] ont par exemple été retrouvés chez les insurgés qui s'en servaient pour brouiller les systèmes de guidage de missiles GPS américains[43].

Les satellites militaires présentent cependant moins de vulnérabilités que les satellites civils en raison du niveau des exigences de sécurité et de la mise en place de mesures techniques comme le chiffrement, l'authentification ou l'étalement de spectre. Des attaques visant à intercepter des signaux de télécommunication militaire sont donc peu probables, ces communications étant généralement chiffrées.

Les satellites civils n'offrent pas ce niveau de sécurité. Des solutions commerciales permettent, en effet, en interceptant des liaisons descendantes, à la fois vers les stations terrestres (bande C) et vers les abonnés (bande L), d'obtenir des statistiques d'appel et des enregistrements de contenus (télévision numérique par exemple). Le chiffrement n'est de plus pas systématiquement utilisé car, comme l'ont démontré Geovedi, Iryandi, et Zboralski lors d'une conférence en 2008[44], chiffrer un signal de satellite peut diminuer jusqu'à 80 % sa performance.

Mais en 2009, des communications militaires non chiffrées ont aussi été observées. Cela a permis aux irakiens de pirater les drones américains Predator, ces derniers utilisant un simple shareware Windows dénommé Skygrabber[45]. Et ce n'est pas tout, car ce système de réception vidéo dénommé ROVER (*Remotely Operated Video Enhanced Receiver*), développé en 2002, a ensuite été étendu à presque toute la flotte de l'US Air Force, sur les F-16 et les F/A-18 en

[39] https://www.youtube.com/watch?v=N4kqBe8J-Tg
[40] https://www.youtube.com/watch?v=tWdgAMYjYSs
[41] http://www.amsat.org/xtra/Getting%20Started%205.pdf
[42] http://cnsnews.com/news/article/russian-gps-jammers-pose-little-threat-iraq
[43] http://www.idexuae.ae/ExhibitorLibrary/1573/Neutralization_of_ACC_AB_2.pdf
[44] http://docslide.us/documents/d1t1-jim-geovedi-hacking-a-bird-in-the-sky-20.html
[45] http://fr.ubergizmo.com/2009/12/17/les-drones-predator-pirates-avec-un-banal-shareware-windows.html

passant par les A-10, les Harrier et les B-1B[46]. Tous transmettent à ROVER, et en clair. Selon un officiel américain interrogé, il serait plus compliqué d'écouter un flux émis par un avion (émission non continue du signal, signal unidirectionnel), mais cela est théoriquement possible.

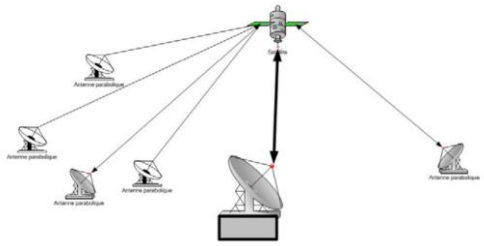
Les liaisons de données vers les satellites ne sont pas les seules vulnérabilités existant dans le domaine satellitaire. En avril 2014, la société américaine IOActive a ainsi publié une étude démontrant que la plupart des flux échangés grâce à des satellites de télécommunications étaient susceptibles d'être piratés[47]. Les recherches d'IOActive se sont concentrées non sur les satellites eux-mêmes mais sur les terminaux d'accès aux satellites depuis la Terre. Plus particulièrement sur les terminaux Inmarsat et Iridium les plus utilisés, et que l'on retrouve au cœur de plusieurs activités industrielles (aéronautique, maritime, militaire, bancaire, plateformes pétrolières, éoliennes, SCADA, etc.). La société de sécurité y a observé différentes failles, tel que des présences de backdoors, de protocoles mal sécurisées et documentés, d'algorithmes de chiffrement faibles…

Vendor	Product	Vulnerability Class	Service	Severity
Harris	RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

Source IOActive

Autant de vulnérabilités qui peuvent permettre l'envoi de fausses informations, voire même la prise de contrôle à distance de l'équipement, comme le démontre IO Active avec le terminal Cobham AVIATOR, qui équipe notamment certains avions militaires américains.

La société Intercrawler continue sur la même voie en janvier 2014 : selon un rapport de la société, les terminaux VSAT seraient particulièrement exposés aux cyberattaques. Le VSAT est un système qui repose sur un site principal, le hub (antenne avec un diamètre de 5 à 9m), où les données sont présentes, et les stations distantes (antennes avec un diamètre de 0,75 à 1,2m), qui se connectent à l'ensemble des ressources du réseau. Le satellite est quant à lui le relais hertzien entre le hub et les stations VSAT.



Présentation du concept VSAT

Ce système est largement répandu dans le secteur industriel, notamment dans les domaines de l'énergie, du pétrole et du gaz, mais également dans le monde militaire[48], en particulier lorsque l'infrastructure technique est basée sur des environnements isolés, comme c'est le cas lors des opérations extérieures. Selon des statistiques récentes, il y aurait un peu moins de 3 millions de terminaux VSAT actifs dans le monde, avec une majorité installée aux Etats-Unis. Sur ce total, les chercheurs de Intercrawler, qui ont scanné l'ensemble des adresses IPV4 depuis 2010, ont

[46] : http://www.wired.com/2009/12/not-just-drones-militants-can-snoop-on-most-us-warplanes/?+WiredDangerRoom+%2528Blog+-+Danger+Room%2529

[47] http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

[48] http://defensesystems.com/articles/2012/07/24/c4isr-1-vsats.aspx

dénombré plus de 10 000 failles de sécurités, dues à des faiblesses de configuration, comme des comptes telnet utilisant des mots de passe faibles.

Il parait donc essentiel d'analyser de façon fréquente tous les éléments du système satellitaire et de mettre en place des mesures de protection sur l'ensemble de ces maillons. Si le terminal et le satellite sont les pièces structurantes, les stations-sol de contrôle et de navigation sont en effet les moyens les plus dimensionnant du réseau. Quelle que soit l'application (communications, surveillance, etc.), un système spatial comprend ces deux composantes (sol et spatiale), qui bénéficient en permanence des progrès de l'informatique, mais peuvent en corollaire être affectés par la sophistication grandissante des cyberattaques. On peut ainsi observer, au cours de ces dernières années, l'apparition d'opérations plus complexes et évoluées, du type Advanced Persistent Threat (APT), qui se traduisent par des intrusions sur plusieurs niveaux, souvent silencieuses et lancées par des adversaires déterminés disposant de financements importants.

Afin de lutter contre ces menaces, des techniques de réjection (ou de rejet de données suspectes) efficaces peuvent être mises en place sur les satellites et sur les moyens sols. Elles pourront également intégrer des moyens de détection et de localisation des signaux parasites. Il s'agira enfin de prendre en compte la protection des moyens terrestres et des équipements utilisateurs (terminaux par ex.) afin de se prémunir des vulnérabilités observées en mettant en place une résistance au brouillage, en durcissant les configurations réseau, en auditant le niveau de sécurité des équipements, etc.

Attention, cependant : si la perturbation d'un système satellitaire, la prise en main de terminaux ou l'interception d'informations « civiles » sont réalistes, l'utilisation et la prise de contrôle frauduleuse d'un satellite à l'insu de son exploitant ne semblent guère envisageables pour le moment. Les satellites militaires semblent pour l'instant, en effet, compte tenu de leurs spécificités (séparation physique des réseaux, chiffrement systématique des communications, résistance au brouillage par étalement au spectre, etc.), être à l'abri de ces menaces, tant que le cyberespace militaire sera constitué de réseaux et de systèmes d'informations cloisonnés du monde civil.

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

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com