Centre Jean Gol

ANALYSE

LA CYBER-SÉCURITÉ À L'ÈRE SPATIALE

FÉDÉRATION
WALLONIE-BRUXELLES

Une analyse réalisée par

JEAN-LUC TRULLEMANS*

Richard Miller, Administrateur délégué du CJG
Corentin de Salle, Directeur du CJG

Novembre 2019

Avenue de la Toison d'Or 84-86
1060 Bruxelles
Tél. : 02.500.50.40
cjg@cjg.be

www.cjg.be

LA CYBERSÉCURITÉ À L'ÈRE SPATIALE

**Jean-Luc Trullemans, Conseiller du Ministre de la Mobilité François Bellot, Expert auprès du Ministre de la Politique Scientifique David Clarinval,Chargé des dossiers de sûreté dans les transports, des programmes de radionavigation de l'UE (EGNOS & Galileo) et des questions spatiales.*

UN FUTUR PAS SI LOINTAIN

Projetons-nous dans le temps et ajoutons cinq années au compteur, pas davantage. Rassurez-vous, il ne s'agit ni d'un doux rêve ni d'un exercice d'anticipation d'un scénariste en mal de sensations fortes. Non, il s'agit simplement d'imaginer l'évolution de technologies existantes que nous croisons déjà dans notre quotidien.

Au petit matin, le soleil pointe, vous attendez devant votre habitation avec votre famille et quelques bagages le mode de transport qui va vous déposer à l'aéroport pour partir en vacances. Très précis et ponctuel, le véhicule autonome s'arrête devant votre maison. Une voix douce, mais artificielle, vous invite à charger vos bagages et à prendre place.

Quel degré de confiance dans la technologie vous faudra-t-il pour grimper dans le véhicule sans chauffeur qui n'attend plus que vous ?

Aujourd'hui, cette confiance est écornée en raison des menaces qui pèsent sur notre cybersécurité. Comme nous allons le voir, des procédés extrêmement sophistiqués sont aujourd'hui utilisés pour attenter aux systèmes satellites complexes[1] assurant notre communication, notre navigation, notre positionnement et quantité d'autres services. C'est de ces menaces et des moyens d'y faire face dont nous allons traiter dans cette étude.

BIENTÔT DES TAXIS VOLANTS ?[2]

Le projet de taxis volants de Volcopter avance à bonne allure : « Après avoir dévoilé la version finale de son appareil muni de 18 rotors électriques dont elle espère pouvoir débuter l'exploitation commerciale dans les deux à cinq ans qui viennent, l'entreprise vient de présenter un prototype de terminal qui servira à gérer le trafic des passagers. Résultat, l'autonomie est passée de 30 à 35 km et la vitesse maximale de 100 à 110 km/h ».

1 Un système complexe est un ensemble constitué d'un grand nombre d'entités en interaction qui empêchent l'observateur de prévoir son comportement ou son évolution par le calcul.
2 Confer site Futura, consulté le 28 octobre 2019. https://www.futura-sciences.com/tech/actualites/drone-volocopter-presente-terminal-taxis-volants-volocity-68718/

LES SYSTÈMES SPATIAUX

Dans notre inconscient collectif, l'Espace et les satellites qui gravitent autour de la Terre sont d'abord l'affaire de scientifiques un peu loufoques ou concernent des applications militaires, des prévisions météorologiques et parfois, la télévision. La réalité est bien éloignée de cette image d'Epinal. En fait, rien n'est moins faux !

Les informations générées par les systèmes spatiaux participent de manière significative au *développement de notre économie.* Les systèmes d'information et de communication (ICT) auxquels elles participent constituent une partie essentielle du fonctionnement des pouvoirs publics, de l'activité des entreprises, de la production de services ainsi que de notre vie quotidienne. Les services qu'ils assurent nous sont aussi indispensables que les transports, la distribution d'électricité ou d'eau. Les systèmes ICT, et les informations générées par les systèmes spatiaux, sont désormais devenus des données constitutives de notre société.

Les performances sans cesse améliorées des systèmes ICT et notre dépendance à ceux-ci renforcent significativement leur attrait en cas de conflits ou d'agressions. Ils constituent des cibles de choix pour tous ceux qui souhaitent affaiblir nos institutions, nos entreprises ou nous porter atteinte individuellement.

Les organisations terroristes et criminelles (comme l'Etat Islamique) ne cachent d'ailleurs pas leurs objectifs de détruire notre sécurité et nos institutions. L'actualité nous prouve que le cyberespace est devenu le théâtre d'actions récurrentes et agressives aux conséquences sous-estimées[3].

Ainsi, la sécurité du secteur des transports repose dans une large mesure sur des services assurés par des systèmes d'information et de communication. Qu'elles soient volontaires ou non, les interruptions de service sont susceptibles de générer des conséquences catastrophiques pour la sécurité des utilisateurs (Etat, organisations et concitoyens). Ces risques seront renforcés par l'autonomisation progressive du transport.

3 La RTBF rapporte le 12 juin 2019 que : « L'équipementier aéronautique ASCO Industries, situé à Zaventem, est à l'arrêt. Le groupe, qui, entre autres, fabrique des pièces pour les géants Boeing et Airbus a été victime d'un piratage informatique. Et c'est toute la production au niveau international qui est à l'arrêt, en Belgique, mais aussi au sein des filiales en Allemagne, aux Etats-Unis et au Canada. Rien que sur le site de Zaventem, ce sont plus 1000 personnes qui sont en chômage technique » in RTBF, Journal Télévisé, consulté le 28 octobre 2019

L'INFORMATION, UN ACTIF PARTICULIÈREMENT CONVOITÉ

La priorité aujourd'hui est d'assurer la cybersécurité[4]. Qu'on le souhaite ou non, nous évoluons dans un monde hyper-connecté. Avec le développement de nouveaux usages, le piratage de données est plus fréquent que jamais… et ce, quelque soit le secteur. Les technologies de transformation numérique façonnent le management des organisations et renforcent leur ancrage dans le monde des données. Un acteur du secteur de la cybersécurité précise que plus de 90 % des organisations utilisent des données sensibles stockées dans le nuage *(cloud)*, recourent au *big data* et aux objets connectés.

En d'autres mots, si la transformation numérique améliore sensiblement l'efficacité des acteurs commerciaux, industriels et étatiques, elle expose les organisations à des modifications fondamentales. Ces transformations induisent de nouvelles surfaces d'attaque et de nouveaux risques qui ne peuvent être contrés que par des mesures sécurisant les informations.

4 Consultez, à ce sujet F. Fanuël, Quelles armes pour faire face aux cyberattaques ?, Analyses du Centre Jean Gol, 2019

L'AVÈNEMENT DU NUMÉRIQUE, AUX SOURCES DU CRIME

La numérisation du périmètre des activités des acteurs régaliens, de l'industrie, du commerce et de leurs interactions a connu une formidable accélération, ces dernières années, avec, notamment, la révolution *internet* et les progrès technologiques qui améliorent notre quotidien. Ce phénomène va bien au-delà des acteurs du numérique ; il est en fait impossible de s'en absoudre. Toutes les entreprises, les administrations utilisent des solutions et des applications connectées au réseau. Des GAFAM[5], en passant par les multinationales, les PME, Start-up et particuliers, ce sont des milliards d'entités qui sont interconnectées.

La numérisation fulgurante jette des passerelles entre quantité d'acteurs qui n'envisageaient pas de se côtoyer il y a quelques années encore. A titre d'exemple, des données issues des activités spatiales sont mises à disposition de nouveaux acteurs économiques qui développent de nouveaux modèles et une foule d'applications et services interconnectés dont nous sommes de plus en plus dépendants.

Le « pirate » trouve, dans cette nouvelle réalité, un terrain d'action aux frontières sans cesse repoussées encore renforcé par un terreau favorable.

En effet, certaines pratiques actuelles tendent à mêler vie numérique professionnelle et personnelle. C'est le cas du New Way of Working (NWoW) qui est défini comme étant : « *une autre façon de travailler qui répond aux attentes et aux besoins des clients. L'accent est mis sur l'atteinte des résultats en responsabilisant les collaborateurs, grâce à une culture organisationnelle orientée humain basée sur la confiance. Cette façon de travailler se veut flexible et mobile, tout en utilisant les nouvelles technologies* ».[6]

Pourquoi ces nouvelles méthodes augmentent-elles les menaces ? Très concrètement, des utilisateurs connectent des équipements non certifiés (clé USB, média externe, ...) ou installent des applications en dehors de toute supervision ou autorisation des responsables de la sécurité de l'information. Cette situation constitue une réelle menace pour l'organisation confrontée à ce que le professionnel de la sécurité appelle « l'informatique de l'ombre » (Shadow IT). Cela illustre clairement le télescopage entre les exigences de sécurité d'une organisation et la souplesse attendue par les utilisateurs.

5 L'acronyme GAFA désigne quatre des acteurs économiques les plus puissants du monde de l'internet à savoir : Google, Apple, Facebook et Amazon.
6 https://fedweb.belgium.be/fr/a_propos_de_l_organisation/developpement_et_support/nwow

LORSQUE LE PIRATE SE FAIT CORSAIRE, ESPION, MILITANT OU ENCORE VOLEUR

Il est convenu de qualifier de « pirate » (c'est presque une caricature), l'individu qui accède à d'autres ordinateurs et serveurs, sans en avoir obtenu la permission. C'est d'ailleurs ce comportement illicite qui a déterminé le législateur dans la qualification des infractions « informatiques » de notre code pénal. Cette qualification de pirate est moins pertinente qu'il n'y paraît. Au sens premier, tel que le donne le dictionnaire Larousse[7], le pirate est un « aventurier qui courait les mers pour se livrer au brigandage, attaquant les navires de commerce ». Le dictionnaire affine quelque peu la définition lorsqu'elle qualifie le pirate informatique de *: « personne qui contourne à des fins malveillantes ou même détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique* ».

En réalité, ce terme générique ne correspond plus précisément à la pratique. En effet, le cyber-crime s'est organisé, professionnalisé, spécialisé, industrialisé et internationalisé comme un marché. Le pirate agit en véritable entrepreneur, avec ses sous-traitants, ses activités de recherche et développement et ses partenaires d'affaire. Le cyber-crime est d'autant plus lucratif[8] que le risque judiciaire est proche de zéro. Il arrive par ailleurs que l'agresseur soit lui-même un Etat.

Nous savons aujourd'hui que certains outils et applications prisés par les pirates ont été développés par des organisations liées à des Etats. Le pirate des temps modernes, s'il reste mobilisé par l'appât du gain comme son ancêtre qui écumait les mers des Caraïbes (mais, notons que cette pratique existe encore, notamment dans la Corne de l'Afrique), se fait aujourd'hui corsaire, espion ou militant. Les attaques peuvent également être inspirées par l'espionnage (nullement réservé aux seuls Etats). Il n'est pas rare d'observer l'exfiltration massive de données de serveurs d'une organisation que ce soit dans le domaine commercial, militaire, étatique ou privé..

En dehors d'une escalade et d'une montée en puissance, les cyber-attaques recensées à travers le monde démontrent le caractère polymorphe de la menace mais également les différentes motivations qui animent les auteurs.

7 Le Littré donne encore une autre définition. Le pirate est : ***« celui qui n'a de commission d'aucun gouvernement, et qui court les mers pour piller ».*** *Dictionnaire consulté en ligne le 29 octobre 2019.*
8 Selon le ***Trustwave Global Security Report****, le taux de retour sur investissement (ROI) sur un rançongiciel est de 1425 %.*

L'Institut Montaigne, dans son rapport sur la cyber-menace, distingue quatre groupes d'auteurs essentiels (cybercriminels,[9] insider,[10] Etats[11] et hacktivistes[12]). L'examen de la littérature nord-américaine révèle encore deux groupes supplémentaires (terroristes et individualistes). En résumé, les auteurs et leurs motivations peuvent être synthétisés dans le tableau suivant :

AUTEURS	MOTIVATIONS
Etats (services de sécurité)	Géopolitique, influence, espionnage
Hacktivistes	Idéologie
Cybercriminels/Crime organisé	Gains financiers
Terroristes	Objectifs politiques et idéologiques criminels
Individualistes	Sensation forte, challenge
Insider ou rogue employee	Frustration, vengeance

Cette mutation opportuniste rend le travail des services de sécurité plus complexe, elle bouscule le principe selon lequel le criminel serait principalement mobilisé par l'opportunisme et le gain facile. Le SGDSN,[13], dans sa revue stratégique de cyber-défense (2018) précise : « D'origine étatique ou non, à visée universelle ou non, émanant d'organisations ou de simples individus, la principale caractéristique de la menace cyber est son caractère polymorphe ».

---

9 ***Organisations criminelles*** *: Elles sont attirées par le gain financier. L'avènement de ce type de menace mafieuse est caractéristique d'un phénomène d'effritement de la frontière entre criminalité traditionnelle et cybercriminalité.*
10 ***Insider*** *: Ces individus sont poussés par une volonté de nuire à l'organisation ciblée, et alimentés par des motivations qui peuvent être idéologiques ou parfois financières. Ils peuvent être internes à l'organisation (rogue employee), ou externes.*
11 ***Etats*** *: Organisations liées aux services de renseignements ou de sécurité des Etats. Ces attaquants s'inscrivent dans des logiques de sabotage, d'espionnage ou de déstabilisation. Les attaques commises par ce type d'organisation sont susceptibles d'être hautement ciblées et discrètes, mais aussi parfois ostentatoires et destructives.*
12 ***Hacktivistes*** *: Groupes plus ou moins organisés, motivés par des motifs idéologiques et qui agissent dans le but de dégrader l'image de marque ou la réputation des structures ciblées, notamment en perturbant la gouvernance de l'organisation.*
13 Secrétariat général de la défense et de la sécurité nationale en France

L'ARME DU CRIME

Les malwares[14] (« *maliciels* ») - c'est-à-dire des logiciels malveillants conçus pour infiltrer ou endommager un système informatique - atteignent des niveaux de sophistication et des capacités d'impact inédits leur permettant d'attaquer efficacement des systèmes d'information complexes abritant des services essentiels qui constituent autant de cibles de choix pour ceux qui souhaitent les attaquer.

Les mécanismes de propagation d'un logiciel malveillant sont devenus d'une redoutable efficacité. Certains paraissent conçus pour causer le maximum de dommages chez leurs cibles. Les plus sophistiqués utilisent des outils d'extraction de mots de passe et d'administration à distance qui les rendent difficiles à détecter. Selon les experts de Cisco Threat Response[15] : « La diversité et le nombre grandissant des types et familles de malwares réduisent la marge de manœuvre *et le temps d'anticipation des organisations face aux menaces* ».

LES COBAYES D'UN CYBER-CONFLIT

L'exemple du virus *NotPetya*[16] illustre particulièrement notre propos. Le 27 juin 2017, une puissante cyber-attaque frappe l'Ukraine et atteint de nombreux pays par rebonds. Lorsque le monde découvre le virus, il est trop tard : il a déjà infecté des dizaines de milliers d'ordinateurs et de nombreux systèmes dans le monde entier.

Ce rançongiciel (*Ransomware*) - c'est-à-dire un logiciel qui bloque un système jusqu'au paiement d'une rançon - s'est répandu au moyen de la mise à jour d'un programme de comptabilité édité en Ukraine. Extrêmement virulent *NotPetya* s'est faufilé à la faveur de nombreuses failles de sécurité jusqu'aux réseaux des plus grandes multinationales. L'opérateur maritime de porte-conteneurs *Maersk*[17], a bien failli y perdre son système informatique car à ne pas s'y tromper *NotPetya* a été conçu pour **détruire la capacité de traitement des données**. Il ne s'agissait pas d'un ransomware qui cherche à vous priver de vos données. L'objectif des concepteurs était bien de détruire la capacité à les traiter.

---

14 Confer l'analyse de Frédéric Fanuël susmentionnée.

15 Cisco Threat Response automatise l'intégration des solutions de sécurité Cisco et accélère les opérations clés comme la détection, l'analyse et la résolution des problèmes.

16 Lors de son apparition le 27 juin 2017, le virus est d'abord considéré comme une nouvelle variante de Petya. Peu après, cette hypothèse est démentie par les experts qui estiment qu'il s'agit d'un nouveau rançongiciel et le surnomme ainsi NotPetya ***afin de le différencier****. NotPetya touche toutes les versions de Microsoft Windows et utilise, pour se propager, la faille de sécurité qu'il exploite au même titre que WannaCry, c'est-à-dire External Blue, qui a été dérobée à la NSA par un groupe de pirates informatiques. Cette faille de sécurité de Windows a été corrigée par Microsoft* ***mais beaucoup d'entreprises n'ont pas mis à jour leur système d'exploitation, d'où cette cyber-attaque mondiale.***

17 NotPetya a gravement affecté différents services de Maersk. Du côté de l'informatique des utilisateurs finaux, 49 000 ordinateurs portables ont été rendus inopérants, toutes les capacités d'impression ont été détruites et les fichiers partagés se sont trouvés indisponibles. NotPetya ***a coûté à l'entreprise quelques 350 M$ en pertes de revenus.***

Pour Adam Banks, Directeur de la Sécurité de l'information, l'incident s'inscrit dans une tendance plus large, d'attaques conduites par des Etats en nombre sans cesse croissant : « en 2016, le *Pentagone a enregistré 15 attaques d'États, mais en 2017, ce nombre est passé à 180. La raison pour laquelle c'est important, c'est que les maliciels utilisés sont beaucoup plus destructifs que ceux qu'une entreprise criminelle utiliserait* ». Aujourd'hui, en dépit de lourds soupçons pesant sur la Russie, personne ne connaît l'identité de l'attaquant. Les auteurs de ce type d'attaques sont aussi multiples que leurs motivations sont nombreuses. Lorsqu'un Etat est impliqué, ses motivations seraient *a priori* géopolitiques ou économiques.


credentials {logged:# input.new(c
script src= address [statu
»access:denial // scri
t src= [true] {?unkno
e function logged:#
e function logged:#
unknown} m#4:80a?:
c= [true] local.config
= {d fg#6 mn4:h61l0
ess [status?] code<
// script src= [error]
unknown} m#4:80a?:/
c= [true] local.confi
d:# input false fun
edentials {logged:
cript src= address
»access:denial //
src= [true] {?unk
e function logged:#
e function logged:#
e function logged:# inp
unknown} m#4:80a?:/q.s statu
= [true] local.config = (245,23,
= {d fg#6 mn4:h61l04y} name<i
ess [status?] code< [true] # status (m#4:80a?:/q.s)
[error] malicious code logged
(245,23,068,789,a48) [lock.command]
name<img>=s
status. omm
(245,23,068,789,
n name<img>=spa
put.new(create)}
atus?] code< [tr
t src= [erro
ici
statu
onfig sc
onfig sc
onf sc
ue") add st
k.command]#
ress logged<[#]
ent.name[get]sc
tus (m#4:80a?:/q.s)
de logged (t
command if ("true") add string

CYBERSÉCURITÉ DES SYSTÈMES SPATIAUX, ÉMERGENCE DE NOUVEAUX RISQUES

La première partie du XXIème siècle est marquée par une nouvelle course à l'Espace. La maîtrise des technologies de l'Espace constitue, pour les Etats un intérêt fondamental dont l'importance n'a jamais été aussi grande. Dans un contexte de diffusion sans précédent des applications issues des services spatiaux à des champs d'activité inédits, les enjeux économiques et stratégiques gagnent constamment en importance. En d'autres mots, comme le précise le rapport 2019 de la Cour des comptes à Paris : « L'Espace fait l'objet d'une compétition stratégique entre les principales puissance ». Les capacités réservées, il y a quelques années encore, aux seules agences gouvernementales sont maintenant mobilisées par des entreprises commerciales et accessibles à de nombreux acteurs économiques. Cependant, les systèmes spatiaux sont devenus indissociables de la mise en œuvre d'infrastructures critiques[18] nationales et européennes ou d'opérateurs de services essentiels.

Les technologies se développent actuellement à toute vitesse et leur propagation, en corrélation avec une dépendance vis-à-vis des équipements spatiaux, ne fait donc que s'accélérer, avec pour résultat un espace extra-atmosphérique de plus en plus encombré, disputé et concurrentiel.

Plus encore que sa capacité à positionner ou à naviguer, la réelle fonction d'un satellite de navigation est de donner un signal temps utilisé pour synchroniser des échanges bancaires, des réseaux de production et de distribution électriques, les réseaux d'eau, des équipements d'aviation civile ou militaire (liste non exhaustive). Le développement et l'exploitation du domaine spatial, de même que la dépendance croissante vis-à-vis de ce dernier, sont porteurs de nouveaux risques dont nous devons prendre la mesure.

*18 Les **infrastructures critiques** constituent les piliers de la résilience de l'Etat. Elles comprennent les entités publiques et privées qui fournissent des biens et des services indispensables à l'exécution des fonctions régaliennes de l'Etat ou susceptibles de présenter un danger grave pour l'activité économique ou pour la population.*

LES SATELLITES, DES SYSTÈMES D'INFORMATION SPATIAUX CRITIQUES MAIS VULNÉRABLES

L'écosystème satellitaire est avant tout constitué de satellites artificiels, équipés de plateformes responsables de certaines fonctions : fourniture d'énergie, propulsion, orientation et communication. La charge utile (*payload*) est préparée et adaptée à la nature de la mission du satellite (observation de la terre, navigation, communication).

L'usage des satellites nécessite des moyens de support au sol. Ce segment « sol » est composé des centres de contrôle des opérations, des réseaux de stations terrestres et des centres de collectes et de traitement des informations.

Mais ces systèmes particulièrement complexes sont vulnérables. Les agressions de satellites ou des infrastructures du segment « sol » ne sont plus le fait de personnes isolées à l'imagination fertile : elles sont hélas devenues courantes. Un grand nombre de technologies critiques qui constituent la colonne vertébrale de l'architecture d'un système spatial sont vulnérables car elles ont été développées à un moment de l'histoire où les enjeux de cybersécurité étaient moindres et où l'ampleur des risques n'était pas encore connue.

JAMMING, SPOOFING, HIJACKING, ETC.

LE *JAMMING* OU LE BROUILLAGE

Parmi les attaques de satellites par hacking, figure le *jamming* ou le brouillage[19], comparable à une **attaque en déni de service** (**DDoS**: Distributed denial of service), c'est-à-dire une attaque qui permet d'encombrer ou de dégrader les flux d'informations de façon à ce que le signal ne puisse plus atteindre sa destination initiale.

Tous les systèmes de communication sans fil sont exposés et sensibles aux interférences électromagnétiques ou au brouillage. La seule considération pertinente en ce qui concerne la vulnérabilité est le degré de protection conçu dans le système de communication pour faire face à des scénarios d'interférence ou de brouillage. Dans le cas spécifique des services satellite, les signaux sont susceptibles d'être brouillés entre les satellites et les récepteurs ou, pour utiliser le jargon, ils peuvent être brouillés sur la « liaison descendante ». L'action malicieuse peut également affecter la « liaison montante », entre les stations du segment « sol » et les satellites.

LE *SPOOFING* OU USURPATION DE SIGNAUX

La masse importante d'information transmise par une constellation de satellites permet aux cybercriminels de corrompre l'exactitude, la précision et la fiabilité des données avec une faible probabilité de découverte. La technique du *spoofing* vise la manipulation de l'information échangée dans les communications et **réduit d'autant son intégrité**.

Le *spoofing* va bien au-delà du brouillage. En effet, il déforme et/ou remplace le signal utile par un faux signal. Une attaque par *spoofing* est susceptible de viser et donc d'endommager des infrastructures critiques telles qu'un réseau électrique en y introduisant des signaux horaires erronés. Une même attaque est susceptible de causer des dommages économiques considérables en ciblant des systèmes de *trading* à haute fréquence dans le secteur financiers.

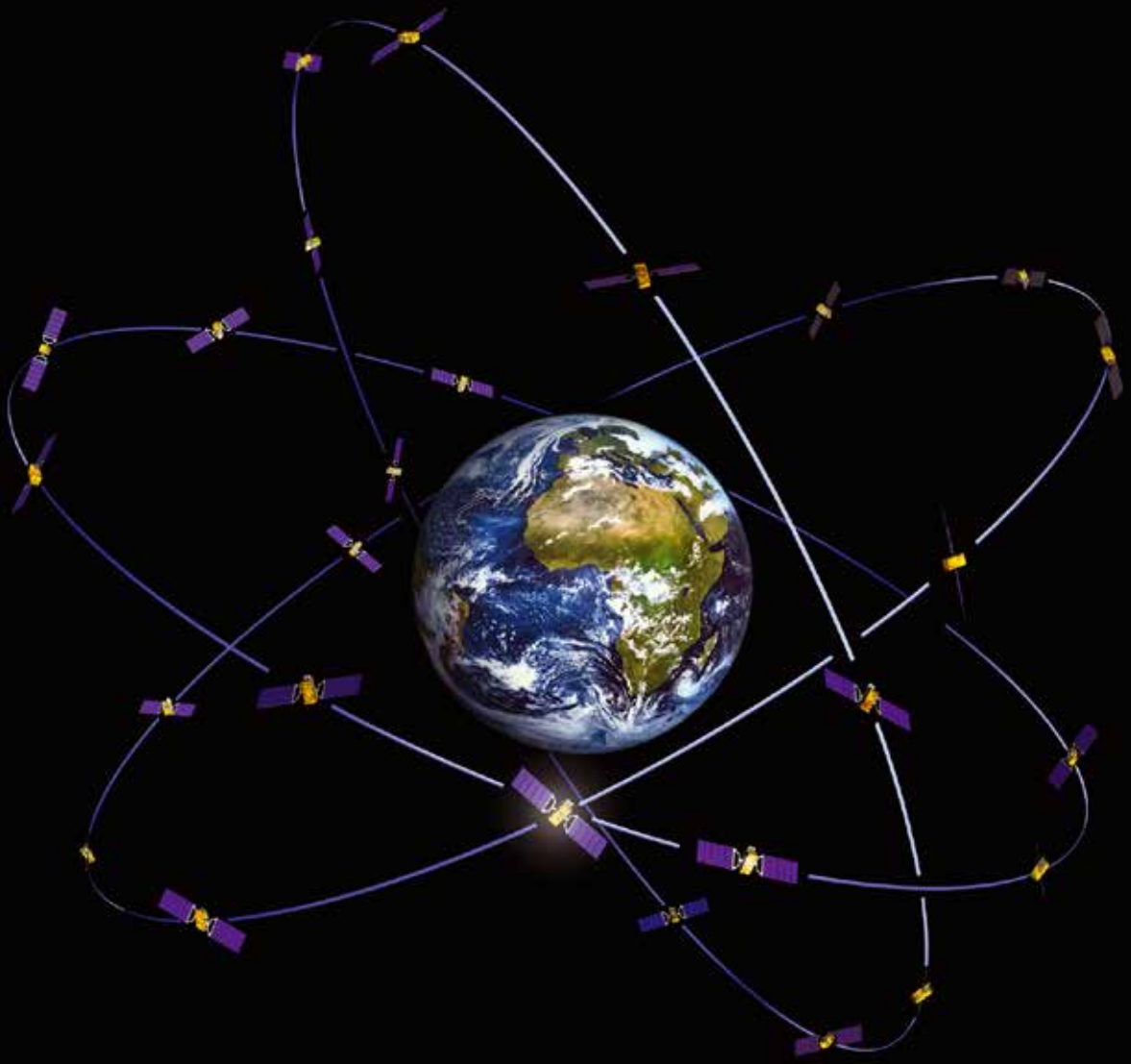
19 Un dispositif de brouillage transmet de l'énergie électromagnétique dans les mêmes bandes de fréquences radio que le signal transmis, ce qui perturbe la capacité d'un récepteur à récupérer avec précision le signal transmis. Les brouilleurs simples transmettent un « bruit », tandis que des dispositifs plus sophistiqués déploient des techniques conçues pour tirer parti des propriétés du signal, et peuvent bloquer simultanément une ou plusieurs fréquences.

LE *HIJACKING* OU DÉTOURNEMENT

Des cyber-attaques peuvent viser une station du segment « sol » avec pour objectif de modifier la trajectoire d'un satellite[20]. Contrôlé par l'adversaire, le satellite voit son orbite modifiée et abaissée afin de le faire entrer dans l'atmosphère terrestre et de le détruire. Ce type d'attaque sophistiquée ressort du sabotage.

La disponibilité sur le marché d'antennes de haute puissance peu coûteuses expose encore les satellites d'une autre manière. La multiplication des vecteurs d'attaque (et leur disponibilité), l'intégration tardive de principes de cybersécurité dans la conception des satellites confirment encore plus leur vulnérabilité. Ces services ont donné lieu à l'éclosion d'une multitude d'applications à haute valeur ajoutée pour le plus grand profit des Etats, des industries, de l'économie et des particuliers.

20 Selon le Centre de la sécurité des télécommunications du Canada, les services de renseignement russes sont capables de détourner des signaux de satellites afin de leur permettre de lancer des cyber-attaques furtives.



LA NAVIGATION PAR SATELLITE ET LE CAS DE GALILEO

Initiée à la fin des années 1950 par Ministère de la Défense américain, la navigation satellitaire constitue l'une des applications les plus lucrative que l'on doit à la conquête de l'Espace. Le déploiement de constellations de satellites de navigation, tous équipés d'horloges atomiques ultra-précises, permet de produire des services de position, de navigation et de synchronisation. Ces services ont donné lieu à l'éclosion d'une multitude d'applications à haute valeur ajoutée pour le plus grand profit des Etats, des industries, de l'économie et des particuliers.

Dans le cadre de la préparation de son Conseil des Ministres de novembre 2019, l'Agence Spatiale Européenne (ESA) a estimé que des activités générant plus de 800 milliards d'euros par an - soit l'équivalent de 6 et 7 % du PIB européen - dépendent directement de la navigation par satellite.

Prenons l'exemple de Galileo, programme phare de l'Union européenne. Galileo distribue ses services dont les applications couvrent de nombreux domaines de notre vie, à commencer par un transport sûr et efficace mais aussi par une très grande précision de la mesure du temps. Galileo est vital pour la stratégie, l'avenir de l'économie et de la haute technologie en Europe.

Grâce à la précision extrême de ses horloges atomiques, Galileo contribue à l'interconnexion de réseaux, de systèmes d'information, de télécommunication, de production et de distribution d'énergie et de services bancaires. Le système assure à l'Europe l'avance technologique critique lui garantissant sa compétitivité sur le plan mondial. La valeur ajoutée de Galileo ne se limite pas à l'économie et aux entreprises. Galileo est, à l'évidence, un outil précieux d'aide à la décision dans les activités régaliennes des Etats membres (gestion de crise, organisation des secours et de la sécurité, sauvetage des personnes, protection des infrastructures critiques).

CYBERSÉCURITÉ DE L'ESPACE ET LE SITE ESA/ESEC À REDU

Depuis 1968, un centre de l'Agence Spatiale Européenne (ESA) est établi à Redu en province du Luxembourg. Visionnaire, la Belgique, déjà très active au sein de l'Organisation européenne de recherche spatiale (CERS/ESRO) a proposé d'accueillir des installations au sol sur son territoire. Le site de Redu est opérationnel depuis le 1er janvier 1968. Les parties techniques comprennent des centres de contrôle, des salles d'équipements techniques et des bunkers pour les antennes.

En 2010, le site a fait l'objet d'un agrandissement et des travaux ont été entrepris afin de satisfaire aux normes de sécurité imposées aux différents sites de l'ESA. Depuis, le site héberge un centre de contrôle d'opérations de l'ESA, dont les satellites PROBA de conception belge. Le centre ESA de Redu a développé une expertise reconnue au niveau européen, tant pour le test en orbite de satellites de télécommunication que pour les satellites de navigation du programme Galileo de l'UE.

La Belgique s'est engagée à soutenir des activités de cybersécurité pour le centre ESA-ESEC de Redu à l'occasion du Conseil de l'Agence Spatiale Européenne (ESA) qui s'est tenu à Lucerne en 2016. La contribution de plusieurs millions d'euros visait à la création d'un pôle d'excellence dans le domaine.

En novembre 2017, assumant la pleine cohérence de l'engagement souscrit, le Ministre de la Mobilité, François Bellot a porté, au nom du Gouvernement Michel, la candidature de la Belgique à l'hébergement du centre back-up de cybersécurité du programme Galileo (GSMC Back-up). La qualité et la maturité du projet ont permis de positionner la Belgique et ses industriels sur l'échiquier cybersécuritaire de l'Union.[21]

Assurant la continuité de la contribution de la Belgique au développement de l'action opérationnelle de l'Agence Spatiale Européenne, le Ministre David Clarinval, en charge de la politique scientifique, a obtenu que le centre chargé de la cybersécurité des programmes de l'ESA soit installé à Redu. La décision a été prise par les Etats membres réunit à l'occasion du dernier Conseil ESA qui s'est tenu à Séville, les 27 et 28 novembre 2019.

Les deux implantations de l'ESA/ESEC (Redu et Transinne) comptent ensemble 250 emplois directs. La concrétisation de cette vision ambitieuse rencontre les priorités fixées dans le Plan national pour des investissements stratégiques du gouvernement fédéral.

21 Le Soir, édition du 03/01/2018 : « La sécurité du système satellitaire Galileo pourrait être bientôt assurée en partie en Belgique. Le GSM-C, c'est son nom, a pour tâche d'assurer la cyber-sécurité de l'ensemble du programme Galileo. Redondance oblige au vu de la nature de l'activité menée, un centre de secours vient en « back-up » du site « master » installé en France. Ce site back-up était situé dans le sud de l'Angleterre. Mais, par l'effet du Brexit, il doit déménager dans un pays membre de l'UE ».

GLOSSAIRE[22]

Attaque par déni de service : L'attaque par déni de service (DoS pour Denial of Service) consiste en une activité illicite visant à rendre un service inutilisable ou à ralentir l'exploitation et les fonctions d'un système donné.

Attaque par déni de service distribué : Attaque par laquelle une multitude de systèmes compromis visent une même cible. Le flux de messages envoyés est tel qu'il provoque une panne du système ciblé et l'interruption des services offerts aux utilisateurs légitimes.

Clé cryptographique : Valeur numérique employée dans des processus cryptographiques, notamment le chiffrement et le déchiffrement, la génération des signatures ou encore la vérification des signatures.

Compromission : Divulgation intentionnelle ou non intentionnelle d'information mettant en péril la confidentialité, l'intégrité ou la disponibilité de ladite information.

COMSEC : Ensemble des mesures visant à prévenir tout accès non autorisé à l'information de télécommunications sous forme lisible et à garantir la transmission de l'information aux destinataires prévus.

Confidentialité : Caractéristique de l'information sensible protégée contre tout accès non autorisé.

Cryptographie : Étude des techniques permettant de chiffrer l'information pour la rendre inintelligible ou de rendre lisible une information chiffrée.

Cyber-attaque : Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à scruter clandestinement un système informatique, un réseau ou un dispositif.

Exfiltration : Retrait non autorisé de données ou de fichiers d'un système par un intrus.

Hameçonnage : Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les mystifiant ou en imitant une marque commerciale connue dans le but de réaliser des gains financiers. En l'occurrence, les malfaiteurs incitent les utilisateurs à partager leurs renseignements personnels (numéros de carte de crédit, informations bancaires ou autres renseignements) afin de s'en servir pour commettre des actes frauduleux.

Intégrité : Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. L'intégrité s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel ainsi qu'au personnel.

22 Définitions données par le Centre canadien pour la cybersécurité

Malware (maliciel en français) : Logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie et les logiciels espions.

Rançongiciel : Type de programme malicieux qui empêche tout utilisateur légitime d'accéder à des ressources (système ou données), et ce, jusqu'à ce que les responsables desdites ressources aient payé une rançon.

Virus : Programme informatique qui se propage en se copiant par lui-même. Les virus informatiques se propagent d'un ordinateur à l'autre, souvent à l'insu de l'utilisateur, et causent des dommages de toutes sortes. Ils peuvent faire afficher des messages irritants, voler des données ou même permettre à d'autres utilisateurs de prendre le contrôle de l'ordinateur infecté.

Vulnérabilité : Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les biens ou les activités d'une organisation.

CONCLUSION & RECOMMANDATIONS

Depuis plusieurs années, les cyber-attaques font partie des risques auxquels sont exposés l'Etat, les organisations, les entreprises mais aussi les particuliers. Ces attaques, aux multiples facettes, visent la structure et le contenu de systèmes particulièrement complexes. L'examen du déroulé des dernières attaques démontre que c'est moins l'information contenue dans ces systèmes qui constitue l'objectif de ces attaques malveillantes que la capacité qu'ils ont de la produire ou de la traiter.

Si la prise de conscience de cette menace par l'Union européenne remonte déjà au début des années 2000 (comme en atteste ses premiers efforts normatifs), le développement d'une stratégie de la cybersécurité se heurte à des enjeux fondamentaux comme le rôle que l'Etat doit jouer dans la protection des systèmes d'information[23]. A ce titre, notons que le gouvernement a pris les dispositions nécessaires à la transposition de la directive NIS[24] en droit belge par la loi du 7 avril 2019 établissant *un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*. La loi est entrée en vigueur le 3 mai 2019.

La cybersécurité, au-delà de celle de l'Etat, des *infrastructures critiques* et des *opérateurs de services essentiels* passe impérativement par une élévation globale du niveau d'alerte dans les différents tissus qui composent notre société (organisations, entreprises et population). La réalisation de cet objectif passe par la promotion d'une culture partagée de la cybersécurité.

Comme le souligne très opportunément *Estelle Hoorickx*, dans Sécurité & Stratégie (février 2019) : « Evaluer la capacité d'un Etat à agir dans le cyberespace diffère selon les critères choisis et reste difficile (...). Le défi actuel des autorités belges consiste à ajuster les moyens juridiques, organisationnels et techniques existants afin de disposer d'une réponse appropriée face aux *cyber-menaces* ».

Nous souscrivons à cette assertion et y ajoutons quelques recommandations (à différents niveaux de pouvoir) :

- Intégrer les enjeux de cybersécurité dans les organisations, les entreprises et la population.
- Poursuivre la réalisation et la consolidation du Plan national pour des investissements stratégiques du gouvernement. Lequel fixe des domaines de cybersécurité prioritaires comme, par exemple, la création d'infrastructures critiques sécurisées, la protection de la population et des entreprises, le développement et l'entretien de capacités et expertises adéquates en cybersécurité et la garantie d'un niveau de formation adéquat.
- Ajuster les moyens juridiques, organisationnels et techniques afin de disposer d'une réponse appropriée face aux cybermenaces (moderniser et consolider l'organisation des capacités de cyber-protection).
- Renforcer significativement l'efficacité des réponses policières et judiciaires pour améliorer la lutte contre la cybercriminalité.

23 https://www.nvoans.be/fr/au-sujet-de-lans/organisation
24 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

Centre Jean Gol

Avenue de la Toison d'Or 84-86
1060 Bruxelles

02.500.50.40
info@cjg.be

www.cjg.be

FÉDÉRATION
WALLONIE-BRUXELLES

Mise en page : Maurane Ballez

Editeur responsable : Richard Miller, Avenue de la Toison d'Or 84-86, 1060 Bruxelles