Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: 6

Artikel: La souveraineté du renseignement : un besoin stratégique grandissant
Autor: David, Dimitri Percia / Mermoud, Alain
DOI: https://doi.org/10.5169/seals-823421

Entrée en vigueur il y a un peu plus d'une année, la LRens a permis de révéler l'ampleur considérable des activités d'espionnage contre la Suisse qui voit ainsi sa souveraineté renforcée.

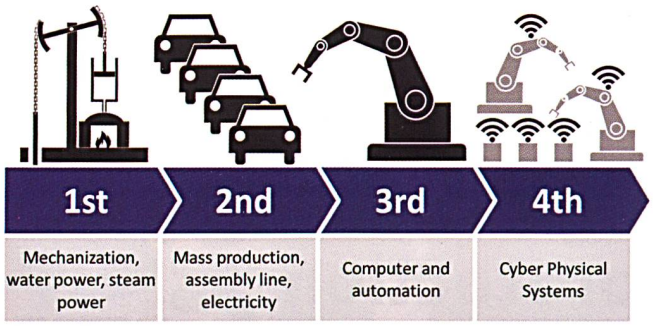
Renseignement

La souveraineté du renseignement : Un besoin stratégique grandissant

Cap Dimitri Percia David, cap Alain Mermoud
Doctorants en systèmes d'information à HEC Lausanne et collaborateurs scientifiques à l'ACAMIL à l'EPF de Zurich

Les nouveaux moyens de production économique liés aux technologies de la *société de l'information* réorganisent les modes opératoires de la guerre. La Révolution numérique, ainsi que la IVe Révolution industrielle, donnent à la *guerre de l'information* une importance sans précédent au travers de trois bouleversements. Premièrement, les menaces existantes telles que le sabotage, l'espionnage et les opérations d'influence prennent de l'ampleur. Deuxièmement, le précepte de Sun Tzu consistant à soumettre son adversaire sans combattre est favorisé. Et troisièmement, un floutage exacerbé des concepts-clés du pouvoir apparaît. Afin de contrer les menaces relatives à ces bouleversements, le renseignement et les moyens mis à disposition pour le produire prennent une importance inédite pour la sécurité nationale. Le cycle du renseignement fait appel à la maîtrise de ses moyens de production, désormais inséparables du contexte de la *société de l'information*. La nécessité d'établir une souveraineté du renseignement passe ainsi par le développement d'une souveraineté numérique, comprise comme une souveraineté au sein de la *société de l'information*. Cet article propose d'analyser l'impact que les bouleversements technologiques apportés par la *société de l'information* engendrent sur la façon de mener la guerre au sens large, ainsi que d'expliciter le rôle grandissant du renseignement en tant que mode opératoire. Des conclusions d'ordre stratégique sont explicitées, basées sur la nécessité de développer une souveraineté du renseignement.

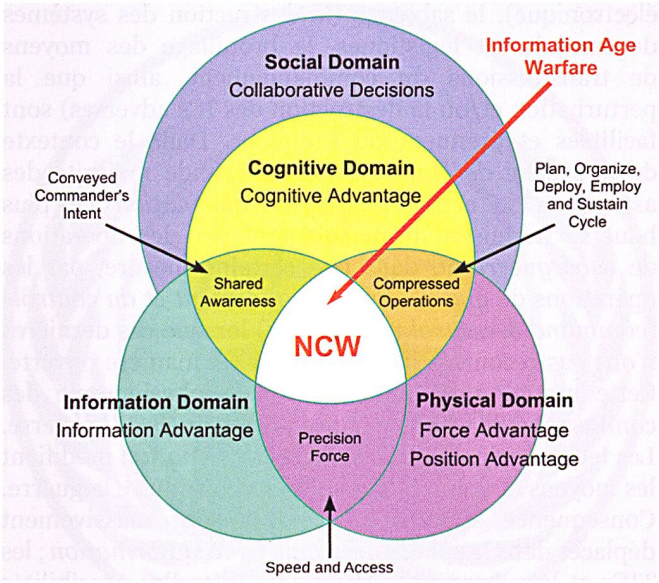
Cette illustration énumère les quatre Révolutions industrielles. La Révolution numérique (IIIe Révolution industrielle) donne naissance à la société de l'information, dont la IVe Révolution industrielle accélère les bouleversements. Dans ce contexte d'infobésité, le renseignement permet d'apporter de la clarté dans le brouillard informationnel.
Source © Wikimedia Commons.



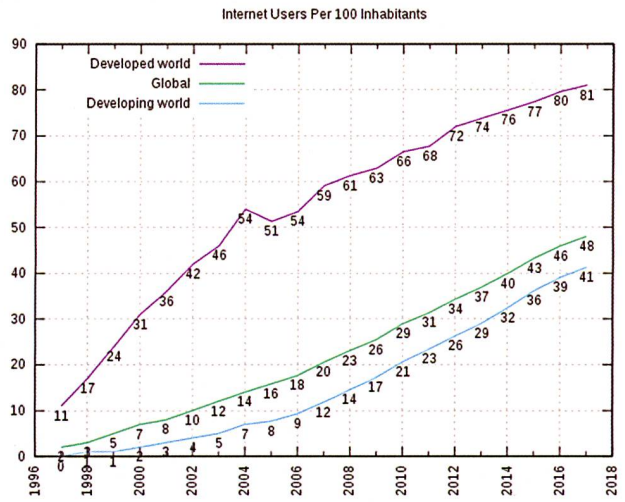
La guerre de l'information : Centre de gravité des manifestations du pouvoir

Au sens de Clausewitz, la guerre est envisagée comme un moyen d'imposition du pouvoir, dont l'effet final recherché est de soumettre son adversaire à sa volonté – et ce, qu'elle revête une composante militaire et/ou politique et/ou économique. Or, si cet effet final recherché reste inchangé après l'avènement et l'essor des technologies de l'information et de la communication (TICs), ces dernières tendent à réorganiser l'importance des facteurs-clés de la guerre et de l'imposition du pouvoir en général. Dans le domaine militaire, la naissance de la doctrine américaine du *network centric warfare* (guerre en réseau) illustre bien la réorganisation de ces facteurs-clés sur le plan opérationnel, distinguant les notions de *cyber war* et *cyber* in *war* (la guerre conventionnelle accompagnée de cyberopérations).

La *Révolution numérique* ainsi que la IVe Révolution industrielle déplacent la *guerre de l'information* au centre de gravité des manifestations du pouvoir. Qu'elles prennent la forme de conflits hybrides entre groupes politiques constitués, ou qu'elles se manifestent au travers de la guerre économique, les manifestations modernes du pouvoir donnent un rôle grandissant au renseignement, aspect indispensable à la *guerre de l'information*. Les fins militaro-stratégiques, économiques, ou plus récemment politiques, font appel au renseignement afin de soumettre son adversaire (ou concurrent) à sa volonté et d'imposer le pouvoir. « *L'information, c'est le pouvoir !* » disait déjà Thomas Hobbes au XVIIe siècle dans *Le Léviathan*. Ainsi,



Cette illustration représente la guerre au sein de la société de l'information ainsi que ses différents champs de batailles. Le network centric warfare (NCW) est une doctrine permettant de conduire les opérations militaires en exploitant les capacités des systèmes d'informations et des réseaux disponibles ; le bouleversement doctrinal principal résidant dans le renseignement produit grâce au partage d'informations. Source :s Département de la Défense des Etats-Unis.



Ce graphique représente l'évolution des usagers d'Internet par 100 individus. L'essor de l'usage d'Internet, couplé à l'interconnexion des systèmes d'information donnent une nouvelle dimension aux actions de sabotage, d'espionnage et d'influence. La croissance exponentielle des données, liée à la démocratisation d'Internet, offre de nouvelles possibilités pour le renseignement.
Source : Union Internationale des Télécommunications.

les prises de décisions stratégiques et l'exécution de l'action dans les environnements militaires, économiques et politiques ne sauraient se passer du renseignement et de sa composante civile: l'intelligence économique.

On fait la guerre et du renseignement comme on produit les richesses

Les bouleversements technologiques amenés par la *société de l'information* confèrent de nouvelles tournures aux actions militaires, à l'intelligence économique, et plus récemment au rôle grandissant de l'influence au sein d'élections politiques. Les TICs modifient la physionomie des manifestations du pouvoir – dont la guerre au sens large fait partie – en apportant trois bouleversements notables. Dans ce contexte, le renseignement joue un rôle-clé afin d'anticiper et maîtriser ces bouleversements. Les trois sous-chapitres suivants proposent d'analyser ces bouleversements en les appliquant au domaine militaire.

Un terreau favorable à de nouveaux acteurs *et à leurs moyens d'actions*

Le premier bouleversement sur la physionomie des conflits qu'apporte la *société de l'information* est lié à la création d'un environnement propice au déploiement d'acteurs tels que les *proxies* d'Etat, les groupes d'influence et les acteurs de la violence infraguerrière, ainsi qu'à l'amplification de leurs moyens d'actions (sabotage, espionnage, influence). Des acteurs qui auparavant étaient considérés comme possédant peu de pouvoir voient leurs capacités d'action considérablement renforcées. C'est au travers des TICs en général, de l'interconnexion des réseaux et de leur carence sécuritaire (manque de *security by design*) que ces acteurs et leurs actions prennent de l'importance. En termes de sécurité nationale, le manque de sécurité lors de la phase de conception (*security by design*) des technologies de la *société de l'information*, couplé à la place incontournable qu'occupent ces dernières dans le contrôle et la gestion des *infrastructures critiques* (ICs) – pour ne citer que cet exemple – créent les conditions favorables au développement, à l'amplification et au déploiement des actions de sabotage. Ces dernières sont de véritables défis pour la sécurité nationale depuis que les systèmes de gestion et de contrôle industriels – qui étaient autrefois basés sur des réseaux de communication dédiés – ont progressivement muté vers des réseaux interconnectés par Internet. Ces systèmes de contrôle et de gestion des ICs – apportés par la *société de l'information* – entraînent une interconnexion inévitable des ICs, et avec eux, les problèmes sécuritaires liés à l'interconnexion des risques. Cette dernière amène ce que l'on appelle le *risque systémique* : une défaillance sécuritaire sur un seul des systèmes provoque alors un effet de cascade sur tous les autres systèmes interconnectés. L'exemple du réseau électrique est édifiant : si le *smartgrid* est rendu inopérable, toutes les autres infrastructures dépendantes de l'énergie électrique se verront affectées, créant une situation que l'on peut appeler « *cyber subprime crisis* », en analogie avec la crise financière des *subprimes* de 2007/8. Un tel phénomène amènerait à un *black-out* sociétal généralisé, paralysant l'entier de la société. Cette tendance technologique d'interconnexion a conduit à considérer les problèmes de cybersécurité comme le principal défi sécuritaire des ICs. Les cyberattaques constituent ainsi la principale et la plus dangereuse menace asymétrique (sabotage) à laquelle sont confrontés les ICs.

Comme les actions de sabotage, les possibilités d'espionnage et de renseignement illégal se voient

également renforcées. L'exemple récent de l'espionnage visant le laboratoire de Spiez démontre que la Suisse n'est pas à l'abri. Le programme Prophylax du SRC fait d'ailleurs un travail remarquable afin de prévenir l'espionnage économique. Cependant, à l'instar de l'exemple des ICs, l'interconnexion des systèmes d'information, couplée au manque de conception sécuritaire de ces dernières, entraînent une interconnexion des risques. Si l'un des systèmes se voit pénétré par un acteur malveillant voulant espionner, tout le réseau interconnecté est vulnérable. Le cas RUAG (2016) le démontre bien: l'espionnage industriel a permis, de par la connexion du système de messagerie de la Confédération à RUAG, d'extraire des données stratégiques de plus de deux mille collaborateurs de l'administration fédérale. L'exemple de surveillance de masse de la NSA (dévoilé par Snowden) est également criant : en surveillant les ICs de télécommunication (câbles de télécommunication sous-marins), la grande majorité des intentions d'acteurs divers (Etats, entreprises privées, individus isolés) peut être mise sous écoute, ouvrant ainsi un boulevard sans précédent aux actions d'espionnage, qu'elles soient perpétrées par des acteurs publics ou privés.

De même, les actions et opérations d'influence prennent une ampleur sans précédent. La facilité de propagation des informations, les coûts réduits pour le faire, et l'anonymat permis par Internet, couplés à l'avènement des *mégadonnées* (*big data*) et de leur analyse (*big data analytics*) permettent de mettre les opérations d'influence « sous stéroïdes ». Le dénouement des dernières élections américaines a mis en évidence le rôle incontestable de l'influence comme mode opératoire afin de capter, récolter et renforcer le vote pro Trump, et que cela soit au travers de *Breitbart News* ou de l'implication supposée du gouvernement russe. Afin d'imposer l'effet final recherché, à savoir l'élection de Trump, les acteurs impliqués ont fait appel aux technologies du *big data analytics* et ont profité des effets des *echo chambers* et des *filter bubbles*.

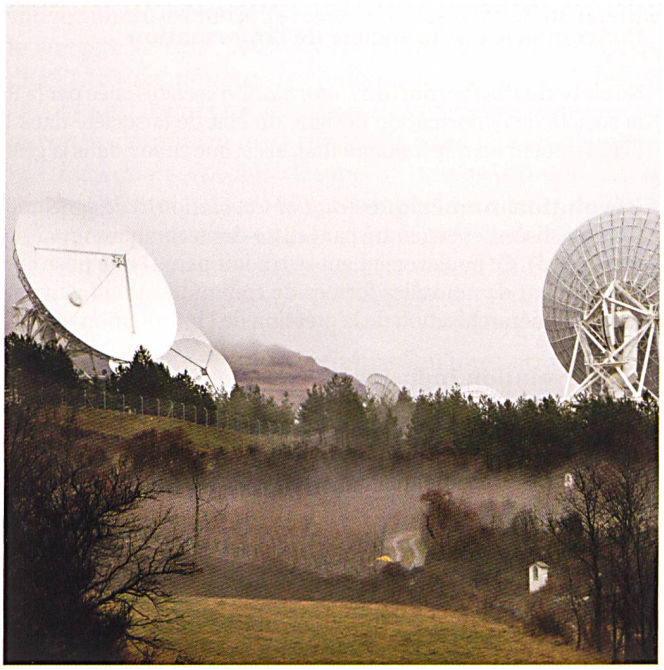
Soumettre l'adversaire sans combattre

L'un des principes-clés de Sun Tzu – soumettre l'adversaire sans combattre – est favorisé par la *Révolution numérique* et la *IVe* Révolution industrielle. Les opérations de P2C (*power to coerce*, ou pouvoir de coercition) prennent de l'ampleur et sont garanties par le déploiement des technologies de la *société de l'information*, notamment au travers de la *cyberguerre* (*cyber warfare*). Contraindre un adversaire en imposant sa volonté, sans pour autant officialiser un état de guerre, et ainsi éviter d'avoir recours à la force armée de manière ouverte, est un mode opératoire incontournable pour les acteurs dominants de la scène internationale. Cependant, les technologies de la *société de l'information* ont considérablement élargi les capacités à mener le P2C grâce à l'exploitation du manque de conception sécuritaire du *cyberespace*. Les opérations d'influence en général (la guerre psychologique, le dérèglement et l'exploitation des médias, la propagande, voire les opérations d'ingérence politique), l'espionnage, la déception (en termes de perturbation de l'exploration et du renseignement adverse menée par la guerre électronique), le sabotage (la destruction des systèmes de conduite et logistiques, le brouillage des moyens de transmissions du commandement, ainsi que la perturbation et/ou la destruction des ICs adverses) sont facilitées et prennent de l'ampleur. Dans le contexte de la *société de l'information*, la grande majorité des aspects du P2C et de la *guerre de l'information* cités plus haut se traduisent principalement par des opérations de *cyberguerre* et, dans une certaine mesure, par les opérations de *guerre du commandement et du contrôle* (*command & control warfare*, *W*) lorsque ces dernières n'ont pas recours à la force armée de manière ouverte. Cette mutation fondamentale de la physionomie des conflits modifie les paradigmes traditionnels de la guerre. Les technologies de la *société de l'information* modifient les moyens et donc les possibilités de conduire la guerre. Conséquence directe: les conflits sont massivement déplacés dans la sphère de la *guerre de l'information*; les TICs et le *cyberespace* offrent de nouvelles possibilités de combat et d'imposition du pouvoir, et élargissent les possibilités de recherche de renseignement. Ainsi, une victoire sans combattre devient une possibilité permettant à la fois d'éviter le recours à la force armée, et de réduire les coûts afin d'atteindre l'effet final recherché : soumettre l'adversaire à sa volonté.

Un floutage exacerbé des concepts-clés du pouvoir

Finalement, les technologies de la *société de l'information* ont un rôle prépondérant dans le floutage des frontières conventionnelles des concepts-clés du pouvoir. La distinction entre état de paix et état de guerre, la pertinence de la distinction entre ressortissants nationaux et étrangers, la différenciation entre actions militaires et actions criminelles (sous l'utilisation de *proxies*), ou encore la pertinence et la définition (parfois même légale) des frontières politiques et géographiques sont systématiquement caractérisées par des environnements VICA (volatile, incertain, complexe, ambigu). Dans ce contexte, les concepts-clés du pouvoir cités ci-dessus sont rendus vagues et confus par les difficultés d'attribution et de traçabilité des actions entreprises dans le *cyberespace*, par l'aspect immatériel et atopographique de ces mêmes actions, et finalement par la célérité de leur exécution. Ces attributs liés à la *guerre de l'information* constituent des bouleversements majeurs apportés par les technologies de la *société de l'information*. L'environnement dans lequel se développe et opère la *guerre de l'information* ne se limite ainsi plus au champ de bataille, mais intègre plusieurs éléments de la guerre dans la société à proprement parler. Par conséquent, la *guerre de l'information* est à la fois une affaire d'Etat et de société, lui conférant un aspect extramilitaire. L'importance de la sphère politique, l'aspect incontournable du pouvoir économique, le rôle que revêtent les acteurs infraguerriers, la possession privée des moyens de production des TICs, la dépendance que les sociétés et systèmes de défense ont développée envers les technologies de la *société de l'information*, ainsi que les vulnérabilités de ces dernières, apportent des mutations fondamentales dans la physionomie des conflits.

L'emblème du groupe d'activistes *Anonymous* représente bien la difficulté d'attribution des cyberattaques. Le renseignement peut contribuer à établir des responsabilités dans un environnement VICA où les frontières entre acteurs étatiques et non-étatiques sont brouillées.
Source © Wikimedia Commons.



Le système d'espionnage de satellites Onyx permet d'accroître notre souveraineté dans le domaine du renseignement. Toutefois, les antennes de Loèche appartiennent à une entreprise privée domiciliée au Luxembourg qui entretient des liens avec d'autres agences de renseignement. Par conséquent, la souveraineté du renseignement ne peut donc pas être totalement garantie. Source © Rama - Wikimedia Commons.

La souveraineté numérique : Condition *sine qua non* à la souveraineté du renseignement

Dans le contexte de la *société de l'information*, le concept de souveraineté – appréhendé comme le droit exclusif à exercer le pouvoir – se conçoit au-delà du champ strictement politique. Les technologies de la *société de l'information* transcendent désormais tous les aspects de notre société, appelant à développer une *souveraineté numérique*. Ces technologies transforment la sûreté des données des citoyens, la sécurité des ICs, ainsi que l'autonomie des moyens numériques en enjeux incontournables.

Notre dépendance aux TICs est désormais irréfutable. Constituant la colonne vertébrale de notre économie, les TICs sont devenus à la fois la charpente sur laquelle tous biens et services opèrent, et le vecteur de prospérité des économies développées. Pourtant, les enjeux sécuritaires des TICs ne semblent toujours pas être une priorité, éludant ainsi que l'interconnexion des réseaux implique également l'interconnexion des risques. La fragilité de notre monde en réseau se traduit en un risque systémique. Dans ce contexte, le manque d'emprise sur les TICs accélère l'érosion de la souveraineté nationale, qui n'est désormais plus envisageable sans souveraineté numérique.

Depuis les années Clinton, le gouvernement américain s'attelle à développer une stratégie numérique en partenariat avec les principaux acteurs de son industrie de produits et services de la *Révolution numérique* et de la *IVe Révolution industrielle*. Ainsi, les USA ont compris que dans une économie de la connaissance, l'information représente ce que le pétrole fut à la société industrielle : le principal carburant et relais de croissance. La suprématie numérique américaine s'est construite sur plusieurs décennies autour d'un partenariat public-privé (PPP) efficace. Cette stratégie numérique a pour objectif d'allier les intérêts économiques, les écosystèmes entrepreneuriaux de la *Silicon Valley*, les besoins des services de renseignement, et les intérêts militaro-stratégiques. N'oublions pas qu'Internet a une origine militaire (le réseau ARPANET lancé par la *Defense Advanced Research Projects Agency*, DARPA).

Dans le cas de la Suisse, le *Center for Digital Trust* lancé à l'EPFL en collaboration avec le DDPS et plusieurs entreprises privées va dans le sens d'une DARPA suisse. Cette « confiance numérique » permet de générer des opportunités commerciales, déjà exploitées par des sociétés telles que Threema (messagerie instantanée sécurisée), Protonmail (messagerie web sécurisée), et plus récemment Kaspersky (service de sécurité informatique) qui a entamé un important déménagement à Zurich pour rassurer ses clients américains, suite à la prohibition de l'installation de ses logiciels au sein de l'administration américaine. Toutefois, la comparaison avec la DARPA reste embryonnaire et les notions de souveraineté numérique et de renseignement restent à développer, comme le suggèrent les exemples suivants. Le Conseil fédéral a certes adopté en septembre 2018 la stratégie dite « Suisse numérique » fixant une ligne de développement, sans toutefois mentionner les notions de souveraineté numérique et de renseignement. Or, depuis 2010, les menaces provenant du *cyberespace* n'ont cessé de se multiplier contre les intérêts nationaux, qu'ils soient politiques, économiques

Concepts-clés de la société de l'information

Société de l'information *(information society)* : née par la Révolution numérique, et exacerbée par la IVe Révolution industrielle, la société de l'information désigne un état de la société dans lequel les technologies de l'information et de la télécommunication (TICs) jouent un rôle fondamental, et ce, que ce soit dans la gestion, le contrôle, ou encore la création de richesses (biens et services).

Révolution numérique *(digital revolution)* : désigne un bouleversement profond et globalisé, survenu dans les sociétés industrialisées, et engendré par l'essor des techniques numériques (principalement l'informatique, Internet, et finalement les TICs en général). Ce bouleversement se traduit par : 1) une mise en réseau planétaire des acteurs (Etats, sociétés privées, individus) ; 2) l'avènement de nouvelles formes de communication (courriels, réseaux sociaux) ; 3) une décentralisation dans la circulation des idées (déhiérarchisation de la création de l'information).

IVe Révolution industrielle *(industry 4.0)* : désigne un bouleversement dans les moyens de production économiques de la société de l'information. Cette nouvelle industrie 4.0 se conçoit comme la convergence du monde virtuel (le cyberespace) avec les objets, les produits et surtout les êtres humains du monde réel. La naissance de nouveaux moyens de production de cette révolution a permis de passer de l'intelligence à l'intelligence artificielle *(cognitive computing, AI)*, de l'Internet à l'Internet mobile (exemple des smartphones), de la programmation à l'auto-programmation (machine learning, deep learning), des données aux mégadonnées (big data), du système de stockage local au système de stockage à distance *(cloud computing)*, des systèmes physiques aux systèmes cyberphysiques (Internet of Things, IoT), des bases de données centralisées aux bases de données décentralisées (blockchain), et dans une certaine mesure de l'humain au transhumain.

Cyberespace : désigne l'ensemble des éléments permettant la création et l'exploitation de données numériques, constituant à la fois un champ d'information et de communication rendu possible par l'interconnexion globalisée des TICs (apportée par la Révolution numérique).

Cyberguerre *(cyber warfare)* : désigne l'utilisation des TICs et des réseaux informatiques pour mener une guerre dans le cyberespace.

Guerre de l'information *(information warfare)* : désigne l'ensemble des actions menées afin de garantir une supériorité et/ou infliger un dommage à un adversaire (ou concurrent). Le terme englobe : 1) l'acquisition d'informations stratégiques concernant l'adversaire (ou le concurrent) ; 2) la manipulation et l'influence (désinformation, subversion) de l'opinion de l'adversaire (ou du concurrent) ; 3) la dégradation (sabotage) des systèmes d'acquisition d'information et de communication de l'adversaire (ou du concurrent).

Pouvoir de contraindre *(power to coerce, P2C)* : né de la réticence de la société civile envers les coûts sociétaux et économiques qu'engendrent une guerre conventionnelle. Le gouvernement américain développa la stratégie du P2C afin d'imposer sa volonté politique. Le P2C est basé sur les principes du soft power, couplé au hard power (formant ainsi le *smart power*). Les outils du P2C se concentrent essentiellement sur les sanctions financières et commerciales (embargos, pressions commerciales comme dans le cas du secret bancaire suisse), sur le soutien implicite aux oppositions politiques à des régimes hostiles (exemple de la stratégie du Containment du communisme par Truman), et sur les cyberopérations offensives (sabotage, influence, déception ; exemple du sabotage du programme nucléaire iranien).

Guerre du commandement et du contrôle (*command and control warfare,* C^2W) : désigne l'engagement concerté de tous les moyens de destruction physique (armes), de la guerre électronique, des opérations psychologiques et de la déception, afin d'interdire à l'adversaire l'accès à l'information, de manipuler, d'interrompre ou de perturber ses activités de commandement, tout en protégeant ses propres capacités par des mesures de sécurité des opérations (mesures de protection) ; le C^2W s'applique à toutes les opérations militaires et à tous les échelons, et se base sur un élément-clé : le renseignement.

Infrastructures critiques, ICs (*critical infrastructures,* CIs) : désigne des systèmes ou des services essentiels au fonctionnement de la société. Ainsi, l'interruption prolongée (même partielle), et/ou la destruction des ICs affecterait fortement le fonctionnement de la sécurité, du système économique, de la santé ou de la sécurité publique, ou encore de toute combinaison de ces éléments.

Mégadonnées *(big data)* : désignent le phénomène de création massive de données de toutes sortes. Ce phénomène est une conséquence directe de la numérisation massive engendrée par la société de l'information. Des ensembles de données sont alors devenus si volumineux, complexes et rapides qu'ils dépassent l'intuition et les capacités d'analyse de l'être humain, et même des outils informatiques de gestion de base de données. Pour résoudre ce problème, les technologies du big data analytics (BDA) ont fait leur apparition. Au travers du BDA, une quantité d'information gigantesque et complexe peut être traitée dans des délais considérablement raccourcis (et parfois même en temps réel), et à un coût incrémental quasiment nul une fois que le coût fixe des systèmes et des algorithmes est investi.

Chambre d'écho médiatique *(echo chamber)* : désigne une situation dans laquelle l'information, les idées, ou les croyances sont amplifiées et/ou renforcées par la communication et la répétition dans un système défini. A l'intérieur d'une chambre d'écho médiatique, les sources ne sont généralement pas remises en question et les points de vue opposés sont censurés et/ou sous-représentés.

Bulle de filtre *(filter bubble)* : désigne à la fois le filtrage de l'information qui parvient à l'internaute par différents filtres, et l'état d'isolement intellectuel et culturel dans lequel l'internaute se retrouve quand les informations qu'il recherche sur Internet résultent d'une personnalisation mise en place à son insu. Couplées ensemble, les echo chambers et *filter bubbles* permettent d'orienter les opinions des citoyens (manipulation, influence des masses).

ou militaires. La « Stratégie nationale de protection contre les cyberrisques (SNPC 2017-2022) et son évolution (SNPC 2018-2022) prévoient plusieurs mesures visant à gérer les cybermenaces, notamment en créant un centre de compétence dans le domaine. Venant compléter ces deux textes, la « Stratégie nationale de protection des infrastructures critiques 2018-2022 » adopté par le Conseil fédéral en décembre 2017 promeut dix-sept mesures afin de préserver la sécurité d'approvisionnement et le bon fonctionnement des ICs – dépendant largement des systèmes d'informations et des TICs. Ces textes vont indirectement dans le sens d'une souveraineté numérique, mais leur implémentation, leurs retombées pratiques ainsi que leur efficacité restent encore à évaluer.

La cyberattaque de 2016 contre RUAG est un exemple démontrant l'importance d'acquérir une souveraineté du renseignement, incluant la capacité à échanger des renseignements avec d'autres agences étrangères afin de détecter et de prévenir les cyber-risques. Dans le cas d'école RUAG, le manque de moyens de nos services de renseignement a été compensé par les services de renseignement allemands. Ces derniers ont informé la Confédération que l'une de ses entreprises stratégiques faisait l'objet d'une cyberattaque depuis plus de 440 jours. En août 2018, le Ministère Public de la Confédération (MPC) a d'ailleurs suspendu la procédure pénale visant à identifier les auteurs de l'attaque. Cette décision démontre malheureusement que le MPC manque de moyens afin d'attribuer les cyberattaques, avouant ainsi publiquement notre faiblesse dans le domaine. Cette dépendance au renseignement étranger constitue un manque de souveraineté du renseignement devenant problématique, car elle expose la Suisse aux pressions et aux manipulations, voire à la déception. Cette dépendance pose également la question de la contrepartie réclamée en échange d'une information aussi stratégique. Grâce à la « Loi fédérale sur le renseignement » (LRens), la Confédération possède la base légale nécessaire pour augmenter son autonomie dans le domaine du renseignement. Toutefois, une année après son entrée en vigueur, tout le potentiel de cette loi reste à exploiter afin d'élargir son champ d'action pour produire son propre renseignement. En limitant sa dépendance au renseignement étranger, la Confédération augmente sa capacité de produire une monnaie d'échange informationnelle, renforçant ainsi sa crédibilité sur le marché international du renseignement.

Dans le cas de notre armée, la sûreté de la communication est cruciale. Le Chef du commandement des Opérations l'a justement rappelé durant le 2e « Forum Cyber-Souveränität » en septembre dernier : « *Le fonctionnement de l'armée dépend de systèmes-clés, lesquels sont fortement dépendants des fournisseurs de service étrangers* ». C'est pourquoi le DDPS développe ses propres compétences et essaie d'obtenir un aperçu dans le code source, afin de développer ses propres systèmes. Dans ce sens, Microsoft accepte, en cas de besoin, de fournir une transparence. Cependant, il semble que même si avec Microsoft une transparence est promise, il n'en reste pas moins que nous continuons à utiliser des systèmes d'information étrangers. La question de la souveraineté numérique reste ainsi toute relative, comme le suggère le Prof. Edouard Bugnion (Vice-Président de l'EPFL) : « *Le manque de confiance est un réel problème et les fournisseurs de service sont loin d'être capables de garantir un niveau de sécurité souhaité par les clients* ». Les *backdoors* (portes dérobées) ne constituent pas le seul problème : les *zero-days* sont également à considérer puisque « dans des millions de lignes de code, il est facile d'insérer des bugs, respectivement difficile de les détecter », déclare le Prof. David Basin (ETH de Zurich).

L'exemple américain démontre qu'une stratégie de maintien ou d'accroissement de puissance passe aujourd'hui obligatoirement par la maîtrise des systèmes d'information, des TICs et de leurs services. Toutes proportions gardées, la Suisse doit absolument se doter d'une véritable stratégie numérique et d'un partenariat public-privé (PPP) efficace, alliant la Confédération, ses hautes écoles possédant la compétence technique (EPFL, ETHZ), ainsi que les entreprises privées suisses possédant l'expérience et le savoir nécessaire (ELCA, Kudelski, etc.). Seule une approche ciblée de la souveraineté numérique – respectant le fédéralisme et le contexte helvétique – permettra de combler ce vide stratégique numérique. Un agenda numérique bien conçu pourrait même permettre l'émergence d'un Etat stratège capable de détecter les risques et les opportunités d'une manière proactive.

Le renseignement : Première ligne de défense contre les cyberattaques

Avec l'avènement de la *société de l'information* et de ses nouveaux moyens de production (liés aux TICs, à la *Révolution numérique* et à la *IVe Révolution* industrielle), la *guerre de l'information* tend à devenir le centre de gravité des conflits. Afin de contrer les menaces amplifiées et rendues possibles par les technologies numériques, le renseignement joue un rôle central et primordial dont l'ampleur n'a jamais été égalée dans le passé. La complexification de la guerre – due aux trois bouleversements de la physionomie des conflits cités plus haut – donne une importance sans précédent au renseignement. Ainsi, il devient primordial d'assurer un renseignement passant par la maîtrise des moyens de sa production. Afin de produire « les yeux de la défense » (le renseignement), il est nécessaire de maîtriser les moyens de production de la *société de l'information* afin de résister à une *guerre de l'information*. Cette nécessité passe inéluctablement par une souveraineté numérique solidement implantée et soigneusement ficelée afin d'accroître la souveraineté du renseignement, élément stratégique grandissant. Etant donné que les moyens de production de la *société de l'information* se concentrent essentiellement dans les mains du secteur privé, une stratégie de souveraineté du renseignement ne peut se passer d'un modèle basé sur un PPP.

A. M. et D. P.D.

A ce sujet lire : Metzger, P., Schneider, T. (2018). *Cybersouveränität, Digital Selbstbestimmung der Schweiz.* www.digma.info