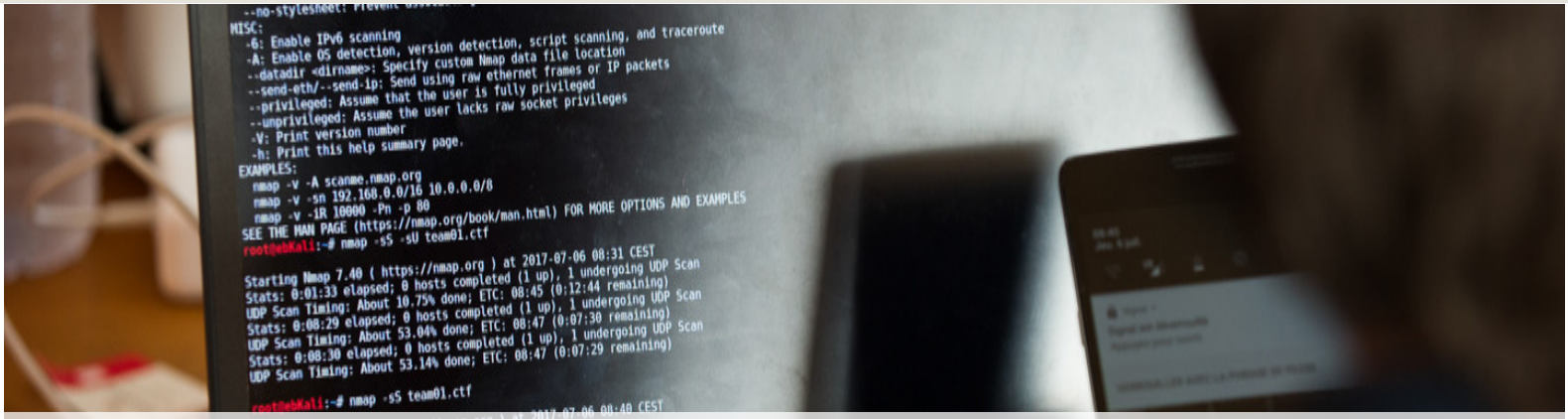

De la souveraineté numérique

cahier de la pensée mili-Terre

Chef de bataillon Frédérick ZIMMERMANN

publié le 06/11/2018

Histoire & stratégie

Les évolutions dans le domaine des technologies de l'information et de la communication se sont répandues si vite qu'elles ont été adoptées sans en mesurer l'intégralité des enjeux. L'actualité récente nous a démontré les risques liés à l'utilisation non maîtrisée de ces systèmes. Pour les Etats, le risque majeur lié à ces technologies peut aller jusqu'à une perte sensible d'indépendance. L'objet de cet article est de vulgariser cette problématique afin de sensibiliser le lecteur de la nécessité des efforts humains et financiers à consentir dans la cyberdéfense.

Le 23 mars dernier, Le Monde publiait, dans son édition web matinale, le récit du "casse" de la banque centrale du Bangladesh[1]. Contrairement à l'imagerie populaire, d'un gang agissant cagoulé pour braquer une banque ou un fourgon blindé, ni arme ni violence n'avait alors été utilisée. Encore plus surprenant, la somme dérobée, 81 millions de dollars, provenait d'un compte que la banque centrale détenait auprès de la Réserve fédérale de New-York. Et les braqueurs seraient de nationalité Nord-Coréenne…On croirait lire le scénario du dernier film d'action produit par les studios d'Hollywood, il n'en est rien. Ce vol a bien eu lieu mais il s'est déroulé sur le réseau numérique du système de transfert bancaire internationale SWIFT[2].

Cet exemple illustre que désormais, l'espace numérique, "le cyberespace" constitue une extension du citoyen, de l'entreprise, et de l'Etat. Alors que l'Etat, au nom du peuple français, possède la maîtrise de son espace terrestre, maritime et aérien, la question de la maîtrise de son cyberespace demeure ouverte. Toutefois, il peut sembler incongru d'utiliser le terme de maîtrise lorsque le cyberespace est évoqué. En effet, le cyberespace, même s'il ne se résume au seul réseau Internet, en partage certaines caractéristiques notamment l'absence de frontières. Ce paradoxe souligne la difficulté à définir l'objet et les limites d'une souveraineté dans le cyberespace. En prenant comme référence l'amendement n°cl129 du projet de loi "pour une République numérique"[3], la souveraineté dans le cyberespace y est définie de la manière suivante: "la souveraineté numérique consiste à continuer la République et ses droits dans la dimension des

réseaux numériques". L'essor prodigieux de l'informatique et des réseaux numériques bouleverse les modèles de société et catalyse de nouvelles forces émergentes : GAFA, ONG, groupes terroristes. Néanmoins, les acteurs traditionnels de la géopolitique, les Etats, réagissent et prennent la mesure des potentialités liées à ce développement technologique inédit par sa vitesse de propagation.

La souveraineté numérique est donc devenu un enjeu majeur pour les décennies à venir. Pour s'en convaincre, il suffit d'observer la place prise par le cyberespace dans les sociétés humaines, telle est la première partie de cet exposé. Après avoir établi ce constat, il s'agira de comprendre les risques et opportunités du cyberespace pour saisir l'enjeu de la souveraineté dans cet espace. Enfin, seront présentées les voies envisageables pour rendre crédible l'expression de la souveraineté dans le numérique.

Comme évoqué précédemment, le développement du cyberespace modifie les rapports entre individus mais aussi entre les individus et les institutions dans le sens où il est presque devenu un intermédiaire incontournable dans la vie quotidienne.

Ainsi, selon l'étude annuelle "DATA NEVER SLEEPS 5.0"[4] de la société américaine DOMO, spécialisée dans l'analyse des données et l'intelligence d'entreprise, pour chaque minute d'une journée en 2017, AMAZON vend pour 258 millions de dollars de marchandises, 4 millions de vidéos sont vues sur YOUTUBE, UBER "transporte" 45000 passagers et 103 millions de courriers indésirables sont envoyés. Ces quelques chiffres non exhaustifs démontrent comment se sont insérés les réseaux numériques chez l'individu. Cette tendance se retrouve également au sein de la société française, en premier lieu chez les personnes. D'après une étude de l'ARCEP[5], 74% de la population française utilise désormais internet quotidiennement, un internaute sur deux déclarant ne pas pouvoir s'en passer plus de deux ou trois jours et 70% des moins de 60 ans estime qu'internet est important pour se sentir intégré dans la société". Tendance, qui sauf cataclysme, n'est pas prêt de s'inverser, et ce pour trois principales raisons: les utilisateurs les plus jeunes en sont les plus consommateurs, "la transition numérique des entreprises françaises, la digitalisation, est encore loin d'être accomplie" dixit le même rapport[6] et enfin la connexion aux réseaux des objets, dénommée généralement comme l'IoT, débutent seulement.

Cette tendance dépasse donc le cadre de l'individu même, car des administrations et des entreprises réalisent ou ont déjà réalisé leur transformation digitale. Effet de mode ou enjeu de survie à moyen ou long terme, c'est un phénomène que nul ne peut ignorer. Sans développer plus longuement sur ce qu'est la digitalisation, il s'agit de revoir les organisations et les processus au filtre des technologies issues de l'informatique et des réseaux et de les adapter en conséquence afin d'améliorer l'expérience utilisateur/client ou encore de gagner un avantage concurrentiel. D'ailleurs, cette vision est également partagée par l'armée de Terre qui accélère elle-aussi sa transformation digitale. Le "Monsieur transformation digitale de l'armée de Terre", à la question "quels sont les enjeux de la transformation digitale?", y répond de la manière suivante: "Il y a deux grands enjeux. Celui de proximité vise à améliorer à court terme, la vie des soldats de l'armée de Terre au quotidien [...]. Le deuxième enjeu, de plus long terme et stratégique, est celui de la supériorité opérationnelle grâce à un meilleur contrôle de données beaucoup plus nombreuses."[7]

Parallèlement à la digitalisation et venant la renforcer, la connectivité des objets se généralise et permet à la fois de mesurer, contrôler et commander à distance voire d'automatiser. L'un des exemples les plus emblématiques est symbolisé par la voiture connectée et autonome dont le déploiement généralisé est prévu pour 2020 ou 2040 selon les scénarii développés par France Stratégie[8]. Non seulement, une multitude

d'objets de tous les jours (réfrigérateurs, jouets, tondeuse, dispositifs médicaux) se voit ajouter une couche de numérique et de réseau mais également les systèmes industriels. Le gouvernement français, considérant le secteur de l'IoT comme un levier de croissance majeur, a dévoilé, en décembre 2016, une feuille de route "Internet des objets"[9] pour développer l'offre des entreprises françaises dans ce domaine.

A l'instar de la révolution scientifique et sociale engendrée par l'invention de l'imprimerie au XV^{ème} siècle, cette révolution engendrée par l'ordinateur et les réseaux informatiques offre de nouvelles opportunités de développement des sociétés humaines. Toutefois, elle comporte aussi son revers de la médaille à travers les risques et dangers inhérents à l'utilisation de ces technologies.

L'extension du cyberespace va donc se poursuivre dans les décennies à venir et s'intégrer davantage au monde physique. VA-t-il contribuer à faciliter le travail des êtres humains ? Cela semble évident lorsque sont évoquées la robotisation des tâches pénibles et dangereuses ou encore l'automatisation de tâches administratives répétitives. Néanmoins, les outils et procédés du cyberespace peuvent être plus ou moins facilement détournés et servir à des fins moins heureuses.

Dans le registre des communications et de l'espionnage, les révélations successives d'Edward Snowden en 2013 puis du site d'information wikileaks en 2017 ont une nouvelle fois illustré cette citation attribuée au général de Gaulle:"les Etats n'ont pas d'amis, ils n'ont que des intérêts." Ces révélations ont, en effet, montré comment les Etats-Unis d'Amérique espionnent alliés et ennemis grâce à leur puissance technologique afin d'assurer leur sécurité voire d'avantager leurs grandes industries. Certes, déjà à la fin des années 1990, les américains étaient également pointés du doigt à cause du système Echelon. De plus, l'espionnage n'est pas l'apanage unique des Etats-Unis. Ces exemples doivent résonner comme des avertissements supplémentaires de la nécessité d'assurer la confidentialité, l'intégrité et l'authentification des communications et données stockées. Ce qu'offre aujourd'hui, entre autres, le cyberespace à nos adversaires, c'est l'interconnexion toujours plus nombreuses de systèmes d'information et de communication.

Cette interconnexion élargit la surface d'attaque et multiplie les possibilités de neutraliser voire de détruire des systèmes clés d'entreprises, d'administrations ou encore de la défense. Ainsi, les 15 et 16 janvier 2009, des avions de chasse Rafale de la force d'action navale ont été cloués au sol suite à l'infection du système de contrôle aérien par le ver informatique Win32/Conficker[10]. Lorsque sont mises en parallèle les avancées technologiques et les vulnérabilités informatiques découvertes chaque jour par des chercheurs, cela ouvre des perspectives effrayantes comme la prise de contrôle à distance de véhicules connectés[11]. Les modes d'action n'ont de limites que l'imagination de leurs concepteurs : quelles seraient les conséquences du non-versement des allocations chômage en France ? Les actions envisageables sur les réseaux numériques peuvent donc être aussi élaborées, de manière à atteindre leur cible indirectement.

L'utilisation du cyberespace pour modifier les perceptions, déstabiliser les opinions est également retrouvée et reconnue dans le concept militaire d'influence[12]. Cette considération souligne que seules les mesures purement techniques ne peuvent suffire pour protéger sa propre appréciation de situation et celle de ses citoyens dans le cas d'un Etat. L'exemple des dernières élections américaines en constituent une démonstration. En effet, Facebook, Google et Twitter, plateformes incontournables d'internet ont reconnu la multiplication de comptes d'origine russe pendant la dernière campagne présidentielle devant le congrès américain.

Les évolutions du cyberespace, espace virtuel, viennent redistribuer les cartes dans le monde physique. Le leadership des Etats y est contesté et la régulation y est encore faible car non unifié. Face à ce constat pessimiste, il convient donc de poursuivre les efforts entrepris pour conserver notre indépendance stratégique dans le cyberespace à l'instar des choix effectués pour posséder l'arme nucléaire ou encore développer nos capacités de renseignement à la fin de la première guerre du Golfe.

Notre dépendance à la technologie constitue désormais une telle source de fragilité, qu'une atteinte majeure sur les systèmes informatiques pourrait bouleverser la vie de la Nation. Dès lors, quelles sont les voies qui permettront de faire face à ces menaces dans l'avenir ? Il s'agit pour la France de se doter de ses propres solutions afin de conserver la maîtrise de ses espaces numériques. Les facteurs pour y parvenir sont autant d'ordre technologique qu'humain.

Dans le chapitre technologique et scientifique, la physique quantique pourrait détenir certaines clés de cet enjeu. Deux applications de ce domaine de la physique, l'ordinateur quantique et la distribution quantique de clés de chiffrement, mobilisent de nombreuses énergies. Depuis le début des années 2000, une véritable course à l'ordinateur quantique a démarré mêlant grands groupes industriels et Etats. L'une des raisons de cet engouement réside dans le fait qu'un tel ordinateur sera en mesure de casser les systèmes de chiffrement asymétrique. Or c'est sur ces systèmes que repose en grande partie la sécurité des échanges sur internet. Même si de véritables calculateurs quantiques ne devraient voir le jour que dans une décennie, le problème est pris au sérieux et le NIST[13] a organisé un concours international pour développer les prochains standards cryptographiques post quantique. En parallèle, a été lancé le projet RISQ[14] qui a pour but de faire de la France un acteur international majeur de la transition post-quantique. Une autre alternative est d'utiliser la deuxième application de la physique quantique, la distribution quantique de clés. Cette technologie est déjà disponible et la Chine semble avoir pris de l'avance: le 29 septembre 2017, elle a réalisé la première vidéoconférence entre Vienne et Pékin par cryptage quantique par le biais d'un satellite[15]. Bien que des sociétés privées commercialisent dès à présent des solutions de distribution quantique, l'expérience menée par la Chine représente un saut technologique majeur par la distance parcourue et le médium utilisé.

Parmi les autres possibilités pour garantir la maîtrise du cyberespace, la conception et la production des matériels et logiciels peuvent être évoqué. D'ailleurs, dans l'amendement précité en introduction figure l'étude de la mise en place d'un système d'exploitation souverain. Mais cette dernière idée a été rapidement retoquée par Guillaume Poupard, directeur général de l'ANSSI[16] lors du forum international de la Cybersécurité à Lille en 2016. En effet, l'ANSSI propose dès à présent pour les besoins de l'administration un système d'exploitation sécurisé, basé sur Linux dénommé CLIP OS. En revanche, une autre voie plus prometteuse s'appuie les développements de l'intelligence artificielle. Ses applications dans la cybersécurité pourrait permettre de pallier les carences des pare-feux et antivirus traditionnels. Ces derniers ne peuvent traiter que des menaces connues et peuvent être facilement contournés car prévisibles. Or, l'utilisation de l'intelligence artificielle dans ce domaine met en œuvre des mécanismes d'analyse du comportement des utilisateurs et des machines pour déceler les attaques et autres logiciels malveillants[17].

Si les algorithmes sont destinés à prendre de plus en plus la main dans la sécurité informatique, l'humain n'est pas pour autant écarté de la boucle. La réalisation de tels programmes informatiques nécessite un capital scientifique donc humain important. Prenant acte de cette nouvelle donne, le ministère de la Défense sous Jean-Yves Le Drian a adopté le pacte Défense Cyber[18] pour atteindre le niveau d'excellence nécessaire

pour être crédible face aux adversaires. Ce pacte contient notamment un volet formation, recherche et développement avec la création du pôle d'excellence Cyber en Bretagne. Cette approche par le haut est complétée par le bas par le développement d'une culture de la sécurité numérique dans l'ensemble de la société. Cet aspect est quant à lui repris dans la stratégie nationale pour la sécurité numérique[20]. Cependant, en 2012, un rapport du Sénat[19] pointait les lacunes du dispositif français en insistant sur notre retard vis à vis de nos partenaires majeures, Etats-Unis, Grande-Bretagne et Allemagne. Le rapport fait également référence au précédent rapports sur le même thème de 2006 et 2008, qui font état d'une prise de conscience tardive. Si aujourd'hui en 2017, la prise en compte de cette problématique est bien réelle, la vue des attaques récentes (Wannacry, Notpetya) ayant impacté des entreprises françaises et les menaces futures, démontrent qu'il est nécessaire de poursuivre le renforcement de nos capacités dans ce domaine et la sensibilisation de tous.

La France dispose d'atouts dans le cyberespace: une véritable expertise dans les télécommunications avec un tissu industriel développé ou encore une recherche académique de grande qualité. Il s'agit donc d'en éviter l'érosion. Il n'est pas anodin que partout dans le monde soient créés des unités militaires pour agir dans le cyberespace. Si nos armées veulent faire partie du cercle des grandes armées qui maîtrisent les données, elles doivent poursuivre l'investissement dans les capacités numériques. A l'instar de ce qu'a connu la France au début de l'aviation, nous assisterons peut-être à une réorganisation en profondeur des armées pour que le militaire soit capable de défendre la nation aussi bien sur la terre, les mers, l'air, l'espace et le cyberespace. La France et ses armées se doivent d'adopter leur propre voie dans le cyberespace en gardant à l'esprit l'avertissement du général Beaufre: « cependant, cet intense mouvement d'idées pénètre à peine en Europe, où l'on se contente en général après quelques lectures distraites d'adopter le vocabulaire et le matériel américains parce que l'on croit encore sans le dire à la suprématie du matériel sur les idées »[21].

Saint-Cyrien de la promotion général Vanbremeersch (01-04), le chef de bataillon Zimmermann choisit de servir au sein de l'arme des Transmissions. Il effectue ses premières années de chef de section au sein de la 4ème Compagnie de Commandement et de Transmissions. En 2007, il rejoint la Brigade de Sapeurs-Pompiers de Paris où il commandera la 6ème Compagnie d'Incendie et de Secours de 2011 à 2013. Affecté au CRR-FR de 2013 à 2015, il sert en qualité d'officier traitant au sein de la branche génie. Il a été projeté en République Démocratique du Congo en tant qu'adjoint opération de l'état-major de la MONUSCO. Breveté de l'Ecole de Guerre, le CBA Zimmermann suit actuellement une scolarité à Télécom ParisTech.

[1] http://www.lemonde.fr/pixels/article/2016/04/26/comment-des-pirates-informatiques-sont-parvenus-a-derober-81-millions-de-dollars_4909101_4408996.html, lu le 10 décembre 2017

[2] Society for Worldwide Interbank Financial Telecommunication

[3] Assemblée Nationale, 6 janvier 2016,projet de loi pour une République numérique, amendement n°129 présenté par Mme Batho et M. Grandguillaume

[4] https://www.domo.com/learn/data-never-sleeps-5, lu le 12 décembre 2017

[5] ARCEP, rapport sur l'état d'internet en France en 2017, mai 2017 (ARCEP, autorité de régulation des communications électroniques et des postes)

[6] IoT, Internet of Thing, internet des objets

[7] Terre Information Magazine, dossier la transformation digitale, novembre 2017

[8] France Stratégie, la voiture sans chauffeur bientôt une réalité, note d'analyse n°47, avril 2016

[9] Ministère de l'économie et des finances, direction générale des entreprises, feuille de route "internet des objets", 14 décembre 2016

[10] BAUD Michel, La cyberguerre n'aura pas lieu mais il faut s'y préparer, revue Politique étrangère, février 2012

[11] Le Monde.fr, Deux chercheurs parviennent à pirater une voiture à distance, 22 juillet 2015, consulté le 14 décembre 2017

[12] L'environnement informationnel est « l'espace virtuel et physique dans lequel l'information est reçue, exploitée et diffusée ». Il englobe le cyberespace et les réseaux sociaux. Il est plutôt du niveau stratégique en raison de la mondialisation de l'information et de ses techniques. Y agir vise en temps réel à identifier les opportunités, les tendances et les possibilités pour faciliter la réalisation de la mission.

RDIA-2012/008 L'influence en appui aux engagements opérationnel, Centre interarmées de concept, de doctrine et d'expérimentation

[13] NIST: National Institute of Standards and Technology, agence du département du commerce des Etats-Unis d'Amérique dont le rôle est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie.

[14] RISQ: Regroupement de l'Industrie française pour la Sécurité post-Quantique comprenant industriels et chercheurs

[15] La première communication inviolable a été réussie, Sciences et Avenir n°850, novembre 2017

[16] ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information

[17] Intelligence artificielle et Cybersécurité, CDEC/PEP, lettre de la prospective n°3-4ème semestre 2017

[18] Pacte Défense Cyber, ministère de la Défense, février 2014

[19] Stratégie nationale pour la sécurité numérique, secrétariat général de la défense et de la sécurité nationale, octobre 2015

[20] Rapport d'information sur la cyberdéfense, commission des affaires étrangères, de la défense et des forces armées du Sénat, juillet 2012

[21] BEAUFRE André, Introduction à la stratégie, Hachette, Paris 1963

Titre : Chef de bataillon Frédérick ZIMMERMANN

Auteur(s) : Chef de bataillon Frédérick ZIMMERMANN

Date de parution 22/10/2018