Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2016)
Heft: 4

Artikel: La LRens : réduire le vide stratégique numérique suisse
Autor: Percia David, Dimitri / Mermoud, Alain
DOI: https://doi.org/10.5169/seals-781442

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 29.03.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Le Service de renseignement de la Confédération (SRC) joue un rôle essentiel dans le suivi de la situation et l'appréciation des risques et menaces.

Renseignement

La LRens : réduire le vide stratégique numérique suisse

Dimitri Percia David, Alain Mermoud

Doctorants UNIL et collaborateurs scientifiques à l'Académie militaire de l'EPFZ

Que peut faire la Suisse pour garantir sa souveraineté dans une société du tout numérique? La nouvelle loi sur le renseignement (LRens) permet d'accroître notre souveraineté dans le domaine du renseignement. Une première étape – insuffisante mais nécessaire – pour combler le vide stratégique numérique suisse.

Pas de souveraineté nationale sans souveraineté numérique

La notion de souveraineté démocratique, comprise comme le droit exclusif du peuple à exercer le pouvoir, se décline désormais au-delà du champ strictement politique. Le champ du cyberespace n'échappe pas à cette tendance. Le numérique transcende désormais tous les aspects de notre société, y compris la souveraineté étatique. La sûreté des données des citoyens, la sécurité informatique des infrastructures critiques, ainsi que l'autonomie de l'infrastructure numérique sont devenus des enjeux incontournables pour notre société de l'information encore émergente. Les gouvernements ainsi que la société civile commencent à saisir l'ampleur du problème, projetant sur le cyberespace les tendances souverainistes qui ont le vent en poupe – à l'instar de l'exemple récent du Brexit.

La fragilité de notre monde en réseau est le nouveau risque systémique

Notre dépendance aux technologies de l'information et de la communication (TIC) se développe de manière exponentielle. Colonne vertébrale de notre économie, les TIC sont devenus à la fois la structure sur laquelle tous biens et services s'appuient, et le vecteur sur lequel une économie développée continue à prospérer. Pourtant, les enjeux et la sécurité des TIC ne semblent toujours pas être une priorité, l'interconnexion des réseaux impliquant également l'interconnexion des risques. La fragilité de notre monde en réseau est le nouveau risque systémique. Dans ce contexte, le manque d'emprise sur les TIC accélère l'érosion de la souveraineté nationale. Condition *sine qua non* de la maîtrise de notre destin, la souveraineté nationale n'est désormais plus envisageable sans souveraineté numérique.

La souveraineté numérique ne se décrète pas: le contre-exemple français et européen

En janvier 2016, le gouvernement français créa un commissaire et un service de l'information stratégique et de la sécurité économique. Cette politique publique relative à l'intelligence économique vise en particulier à renforcer la protection et la promotion des intérêts économiques, industriels et scientifiques fondamentaux de la nation, ainsi qu'à assurer les moyens de sa souveraineté économique. Dans le cadre du projet de loi pour une *République numérique*, le gouvernement français a évoqué le concept de souveraineté numérique. Appliquant le principe de souveraineté aux TIC et aux réseaux informatiques, ce concept vise notamment à favoriser le développement d'un système d'exploitation français. Un *cloud* souverain basé sur des logiciels libres pourrait également voir le jour afin de permettre la conservation et le rapatriement des données stratégiques sur le territoire national. Malheureusement, la souveraineté numérique, à l'instar de la souveraineté politique, ne peut pas se réaliser sur ordre de l'Etat. Pour preuve, les tentatives bureaucratiques de l'UE visant à réduire l'hégémonie numérique américaine ne furent pas concluantes. Abandonné en 2014, le projet de «Google européen» (Quaero) est un exemple de fiasco retentissant.

La suprématie numérique américaine n'est pas un hasard

Les Etats-Unis ont compris depuis les années Clinton que dans une économie de la connaissance, l'information serait ce que le pétrole était à la société industrielle: le principal carburant et relais de la croissance.
La suprématie numérique américaine s'est construite sur plusieurs décennies autour d'un partenariat public-privé efficace. Cette stratégie vise à allier les intérêts économiques, les investissements, les écosystèmes entrepreneuriaux de la *Silicon Valley*, les besoins des services de renseignement, et les intérêts militaro-stratégiques. De plus, n'oublions pas que l'Internet a une origine militaire (réseau *ARPANET*). Le développement symbiotique entre l'Internet et la défense de la souveraineté est donc un atavisme. Les révélations Snowden n'ont fait que de confirmer l'importance du pouvoir

de l'information pour la sécurité nationale. « *L'information c'est le pouvoir !* » écrivait Thomas Hobbes dans le *Léviathan* au XVII[e] siècle déjà.

Le secteur privé commence à exploiter les atouts numériques suisses

Sur le papier, la Suisse présente un cadre idéal pour l'éclosion d'une société de l'information florissante : stabilité et neutralité politique, système d'éducation performant et capital humain de haute qualité, culture de la confidentialité, et surtout un cadre juridique garantissant la protection des données. Cette prise de conscience s'est matérialisée par la récente création de VIGISWISS, une association qui regroupe les sociétés actives dans le stockage et la protection des données en Suisse. Avec la fin du secret bancaire, pourquoi ne pas proposer la sécurité des données comme nouveau modèle d'affaire ?

L'extension de la neutralité et des bons offices au cyberespace

Le Geneva Center for Security Policy (GCSP), une fondation internationale regroupant 45 Etats membres, s'est montrée comme précurseur de la cyber diplomatie, tirant partie de la Genève internationale afin de développer une gouvernance de l'Internet en Suisse. Autre atout pour la Suisse : notre neutralité pourrait permettre d'accompagner la résolution de cyber conflits, en étendant les bons offices au cyberespace. Mieux : avec ses nombreuses institutions internationales, la Suisse est idéalement positionnée pour favoriser et accompagner l'émergence d'un premier traité du cyberespace.

La Confédération n'a pas suffisamment conscience des enjeux numériques

Le secteur public et la sphère politique continuent à sous-estimer les opportunités et les risques liés à la société de l'information. Berne a certes adopté en avril dernier une stratégie *Suisse numérique* fixant des idées cohérentes, sans toutefois y allouer le budget nécessaire. Depuis 2010, les cyber attaques n'ont cessé de se multiplier contre les intérêts nationaux, qu'ils soient politiques, économiques ou militaro-stratégiques. Bien que la *Stratégie nationale de protection contre les cyber-risques* (SNPC) prévoit plusieurs mesures visant à gérer les cyber-risques, l'ampleur et la fréquence des cas de cyber attaques observées depuis remettent en cause son efficacité. L'Hebdo du 16 juin résumait bien la situation : « *la stratégie de cyberdéfense suisse n'est qu'un fromage percé de trous, une ligne Maginot numérique aussi inefficace et mal conçue que les casemates de Verdun en leur temps.* »

Le renseignement, première ligne de défense contre les cyber attaques

La récente cyber attaque contre RUAG est un cas d'école qui démontre l'importance du renseignement et de l'échange d'information pour détecter et prévenir les cyber attaques. Dans cette affaire, le manque de moyens de nos services de renseignements ont heureusement (sic !) été compensés par les services de renseignement allemands. Ils ont informé la Suisse que l'une de ses entreprises stratégiques faisait l'objet d'une cyber attaque depuis plus d'une année. Cette dépendance au renseignement étranger est problématique, car elle expose aux pressions et aux manipulations, voire à la déception.

La LRens est nécessaire pour réduire notre vide stratégique numérique

Cette dépendance pose surtout la question de la contrepartie réclamée en échange d'une information aussi stratégique. La Suisse doit impérativement augmenter sa capacité à produire son propre renseignement, afin de limiter cette dépendance. Cela permettra également à la Confédération de générer une monnaie d'échange informationnelle, renforçant ainsi sa crédibilité sur le marché international du renseignement. La LRens apportera une bouffée d'air frais et des nouvelles ressources au Service de renseignement de la confédération (SRC). C'est une première étape – insuffisante mais nécessaire – vers une souveraineté dans le domaine du renseignement.

Les cyber attaques sont un épiphénomène

Les cyber attaques ne sont qu'un épiphénomène, comparable aux attaques répétées contre la place financière suisse. Depuis trop longtemps, notre gouvernement attend passivement les attaques et cherche ensuite à recoller les pots cassés à posteriori. La cause : une vision trop « confédérale, » étalant les responsabilités entre diverses unités, et alimentée par une suspicion envers la centralisation des pouvoirs ainsi que par la volonté de ménager la liberté de ses diverses unités. Conséquence : aucune entité ne se voit responsable d'agir et surtout de prévenir. Si différents organes, décrets et commissions fédérales portant sur la sécurité du cyberespace et de ses infrastructures numériques existent en Suisse, la dilution des responsabilités entre entités compétentes n'est qu'un symptôme d'une maladie plus grave : le vide stratégique numérique suisse.

La souveraineté numérique, prélude à un Etat stratège ?

L'exemple américain démontre qu'une stratégie de maintien ou d'accroissement de puissance passe aujourd'hui obligatoirement par la maîtrise des systèmes d'informations et de leurs services. Toute proportion gardée, la Suisse doit absolument se doter d'une véritable stratégie numérique et d'un partenariat public-privé efficace. Seule une approche holistique de la souveraineté numérique - respectant le fédéralisme et le contexte helvétiques - permettra de combler ce vide stratégique numérique. Un agenda numérique bien conçu pourrait même permettre l'émergence d'un Etat stratège avec une véritable vision stratégique à long terme, capable d'anticiper afin de cesser de se faire surprendre. Un tel Etat serait doté d'un outil de pilotage stratégique capable de détecter de manière proactive les risques et les opportunités. A l'instar de Fathi Derder, on pourrait alors se mettre à rêver que le prochain Google sera Suisse.

Rappelons que le droit à l'autodétermination est un principe reconnu par le droit international. Ce principe doit aujourd'hui également s'appliquer au cyberespace. Chaque peuple doit pouvoir disposer librement de son destin, y compris de son destin numérique. Heureusement, la défense de la souveraineté transcende aujourd'hui les clivages politiques classiques. La *LRens* permet d'accroître notre souveraineté dans le domaine du renseignement. C'est un premier pas en direction d'une souveraineté numérique, désormais indissociable de la souveraineté nationale. Elle mérite donc d'être soutenue. Nous recommandons de voter oui le 25 septembre.

D. P. D. ; A. M.