Pour une approche économique de la cybersécurité

La cybersécurité ne se limite pas aux sciences informatiques. Une approche holistique et multidisciplinaire est nécessaire pour renforcer notre souveraineté numérique. Deux recherches scientifiques adoptant une approche économique de la cybersécurité sont présentées. La première se concentre sur les incitations au partage de l'information sur les cybermenaces. La deuxième porte sur l'efficience des technologies de rupture pour la cyberdéfense. Ces deux études visent à augmenter la résilience des forces armées et des infrastructures critiques.

Marcus M. Keupp, Alain Mermoud[1], Dimitri Percia David

Renforcer notre souveraineté numérique

La souveraineté nationale – condition *sine qua non* pour maîtriser notre destin politique, économique et social – est désormais étroitement liée à la souveraineté numérique.[2] Certains auteurs, comme Pierre Belanger, estiment que : « sans souveraineté numérique, la mission de défense ne sera à terme plus exécutable. La souveraineté numérique est la condition de la sécurité nationale et de la défense ».[3] La Confédération doit donc agir pour assurer notre souveraineté dans le cyberespace. Elle doit prolonger l'existence et la défense de la Suisse dans cette quatrième dimension, comme elle le fait pour la terre, l'air et ses intérêts maritimes. La sûreté des données des citoyens, la sécurité des infrastructures critiques, ainsi que l'autonomie de l'infrastructure numérique, sont devenues des enjeux incontournables pour la confiance générale dans notre société de l'information encore émergente. La notion de souveraineté démocratique, comprise comme le droit exclusif du peuple d'exercer le pouvoir, transcende désormais les clivages politiques classiques.[4] Le champ du cyberespace n'échappe pas aux tendances souverainistes, favorisées par l'émergence d'une ère post-vérité[5] et d'un monde de plus en plus volatile, incertain, complexe et ambigu (VICA).[6]

La souveraineté numérique est la condition de la sécurité nationale et de la défense.

La couche physique du cyberespace[7] est avant tout une ossature matérielle composée d'infrastructures interconnectées: câbles sous-marins, antennes, satellites, etc. Ces infrastructures sont réparties sur les territoires de différents États qui ont leurs propres intérêts stratégiques et géopolitiques.[8] La majorité des câbles sous-marins de fibres optiques (au nombre de 366) appartiennent à des opérateurs privés. Ils sont exploités en collaboration avec les États et assurent 99 % du trafic mondial des données. Ils sont posés directement sur le fond marin et évitent la lenteur et le coût plus élevé des transmissions par satellites. La maîtrise de ces câbles intercontinentaux représente aujourd'hui un enjeu stratégique majeur.

La carte des câbles sous-marins (Fig. 1) indique que le Royaume-Uni est une plaque tournante des télécommunications mondiales.[9] Le service de renseignements électroniques du Royaume-Uni (*Government Communications Headquarters:* GCHQ) profite de cet avantage grâce à son programme Tempora. En effet, ce programme lui permet d'intercepter massivement les données transitant entre l'Europe et les États-Unis. Le GCHQ et son homologue américain, la *National Security Agency* (NSA), peuvent ainsi surveiller les échanges transatlantiques et partager les informations récoltées avec leurs partenaires des «*Five Eyes*».[10] La surveillance des câbles est devenue un élément central de la stratégie de surveillance

1 Auteur correspondant : alain.mermoud@vtg.admin.ch
2 La souveraineté numérique désigne l'application des principes de la souveraineté aux technologies de l'information et de la communication (TIC). Elle est un enjeu majeur pour la gouvernance d'Internet, c'est-à-dire l'élaboration et l'application conjointes par le secteur privé, la société civile et les États, de normes visant à réguler les usages dans le cyberespace.
3 Bellanger, P. 2014. *La souveraineté numérique.* Stock.
4 Citons par exemple l'initiative pour la souveraineté alimentaire déposée par le syndicat paysan *Uniterre*. Le Conseil national soutient actuellement un contre-projet visant à inscrire la sécurité alimentaire dans la Constitution.
5 Le néologisme *post-truth politics* a été consacré mot de l'année 2016 par le dictionnaire d'Oxford. Celui-ci en donne la définition suivante : « la post-vérité fait référence à des circonstances dans lesquelles les faits objectifs ont moins d'influence pour modeler l'opinion publique que les appels à l'émotion et aux opinions personnelles ».
6 Valla, P. 2004. *Sommes-nous aptes à gérer un monde volatile, incertain, complexe et ambigu (VICA)?* Military Power Revue.
7 Le cyberespace est à la fois physique (serveurs, routeurs, câbles), logiciel (protocoles, programmes), et cognitif (le sens de l'information portée par les réseaux).
8 Huyghe, F-B., et al. 2016. *Gagner les cyberconflits : au-delà de la technique.* Economica.
9 Cette supériorité remonte au XIXe siècle, lorsque les britanniques dominaient déjà le marché du câble sous-marin télégraphique dans l'océan Atlantique.
10 Le terme *Five Eyes* (Cinq Yeux) désigne l'alliance entre les services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Ces pays sont liés par le traité *UKUSA,* un accord qui règle la coopération pour la collecte de renseignements électromagnétiques. Ce traité signé en 1946 est resté secret jusqu'aux révélations liées au réseau Echelon (système mondial d'interception SIGINT) à la fin des années 1990.

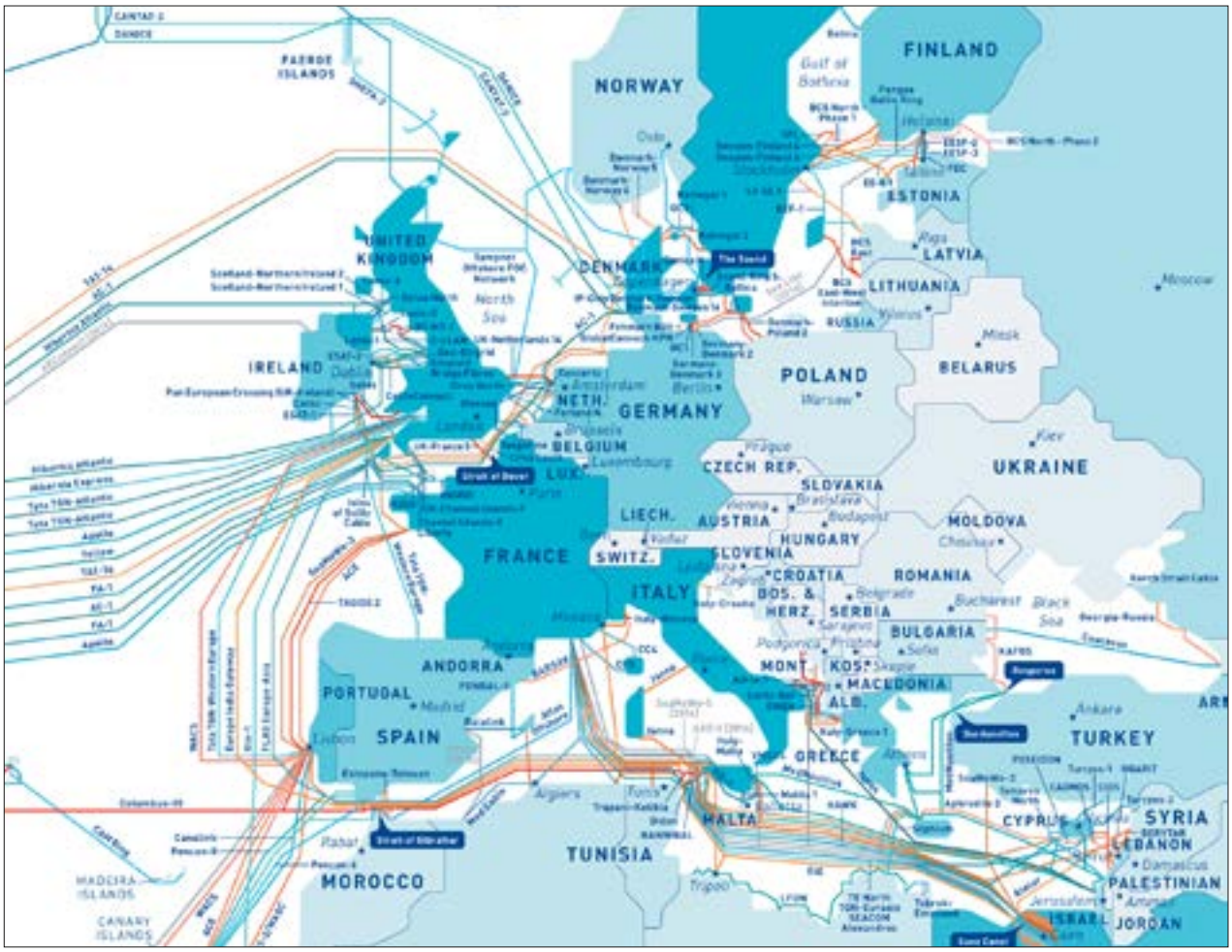

Figure 1 Le Royaume-Uni concentre un grand nombre de câbles sous-marins, ce qui lui permet de surveiller à large échelle le trafic Internet passant sur son territoire. (telegeography.com)

de la NSA, car elle sert à la sécurité nationale, mais aussi au renseignement économique et à l'espionnage industriel.[11] Pour maintenir et accroitre sa souveraineté, un État doit maîtriser la surveillance qui s'exerce sur et depuis son territoire.

Figure 2 Le sous-marin nucléaire d'attaque *USS Jimmy Carter* (SSN-23) a la capacité de mettre sur écoute la fibre optique sous-marine. (Wikipedia)

11 Cette surveillance n'est toutefois pas un phénomène nouveau. Au XIXe siècle la communauté du renseignement s'intéressait déjà à la collecte de données issues des câbles sous-marins. Lors de la première guerre mondiale, les Britanniques et les Allemands cherchaient à interrompre systématiquement les communications en sectionnant ces câbles. Durant la Guerre froide, l'opération *Ivy Bells* (menée conjointement par la *NSA* et l'*US Navy*) permettait de placer les câbles sous-marins soviétiques sur écoute.

Pour maintenir et accroitre sa souveraineté, un État doit maîtriser la surveillance qui s'exerce sur et depuis son territoire.

Le réseau Internet est devenu le symbole de la globalisation et des échanges internationaux. Cependant, ce réseau a une origine militaire – le réseau *ARPANET* – et constitue ainsi un lien direct avec la défense de la souveraineté.[12] Les *révélations Snowden* n'ont fait que confirmer l'importance de l'information pour la sécurité nationale, comme précédemment défendu par Thomas Hobbes au XVIIe siècle dans son Léviathan : *« L'information c'est le pouvoir ! »*.

Dès les années 1990, les États-Unis ont compris que dans une économie de la connaissance, l'importance de l'information pourrait être comparée à celle du pétrole dans la société industrielle : le principal carburant et le relais de la croissance. Les données sont donc la principale matière

12 Suite à la crise des missiles de Cuba, la *Defense Advanced Research Projects Agency* (DARPA) développa en 1969 le premier réseau de téléinformatique à transfert de paquets, baptisé *ARPANET*. La *DARPA* est une agence du département de la Défense des États-Unis et elle est chargée de la recherche et du développement destinés aux usages militaires.

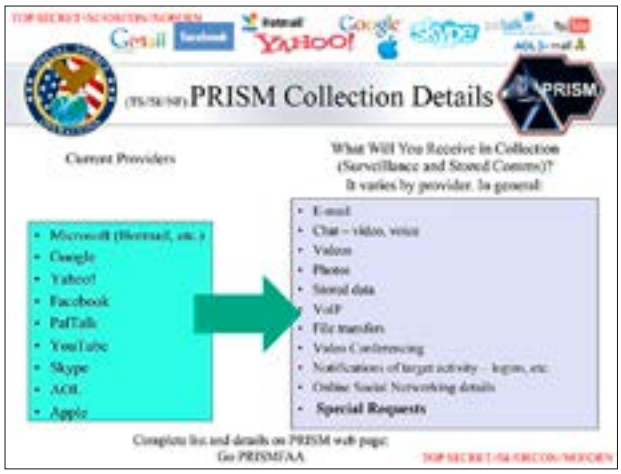

Figure 3 Le programme de surveillance électronique PRISM révélé par Edward Snowden en 2013. Ce programme a pour but de collecter des données sur le réseau Internet, en collaboration avec les grandes sociétés high-tech américaines. Certaines entreprises stratégiques américaines utilisent les informations collectées pour se créer un avantage compétitif. (NSA)

Figure 4 L'ancien secrétaire américain à la défense, Leon Panetta, a mis en garde son pays contre la possibilité d'un « Cyber Pearl Harbor ». (istockphoto.com)

première de la quatrième révolution industrielle.[13] Comme le pétrole, elles doivent d'abord être extraites, puis raffinées pour devenir utilisables. Elles sont réparties d'une manière inégale et représentent donc un intérêt géoéconomique pour les États. La technologie n'est pas neutre. Elle s'inscrit dans un contexte géopolitique et dans les idéologies. Les GAFA (Google-Apple-Facebook-Amazon) forment aujourd'hui les premières capitalisations boursières mondiales et dépassent le produit intérieur brut (PIB) de certains États. Cette suprématie numérique américaine s'est construite sur plusieurs décennies autour d'un partenariat public-privé efficace.[14] La stratégie consiste 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. Cette alliance forme aujourd'hui un véritable complexe militaro-numérique qui permet d'assurer l'hégémonie américaine dans le cyberespace et de consacrer l'extraterritorialité du droit américain.[15]

La technologie n'est pas neutre. Elle s'inscrit dans un contexte géopolitique et dans les idéologies.

Notre dépendance aux technologies de l'information et de la communication (TIC) se développe de manière exponentielle. Par conséquent, les États, les entreprises et les individus sont la cible de cyberattaques de plus en plus fréquentes et sophistiquées. Le développement rapide de l'informatique dématérialisée en nuage et de l'Internet des objets (dont la sécurité de base est très limitée) amplifie encore cette perte d'autonomie. Les forces armées et les infrastructures critiques[16] n'échappent pas à la datafication et dépendent de plus en plus du réseau Internet pour accomplir leurs mandats respectifs. L'interruption (même partielle et éphémère) de certaines infrastructures critiques pourrait entraîner des effets en cascade. Si l'interconnexion des réseaux engendre de nombreuses opportunités, elle implique également l'interconnexion des risques. Ceux-ci sont encore trop souvent mesurés et gérés de façon isolée. Par analogie à la crise des *subprimes*[17] en 2008, cette cyber-interconnexion des risques est appelé cyber-apocalypse ou cyber-subprime par certains experts. *L'Autorité bancaire européenne* (ABE) prévoit d'ailleurs d'élargir ses stress tests au domaine de la cybersécurité des banques *too big to fail* (trop grandes pour faire faillite). La fragilité de notre monde interconnecté représente donc un nouveau risque systémique dont les conséquences restent trop peu étudiées.

13 La quatrième révolution industrielle désigne les nombreuses innovations de ruptures bouleversant actuellement les économies développées. Ces innovations s'appuient sur les technologies numériques et transforment radicalement les moyens de production, de distribution et d'accès aux biens et services. Le réseau Internet est au cœur de cette révolution et permet l'interconnexion de ces technologies (robotique, impression 3D, biotechnologie, etc.) avec la société et le corps humain (on parle alors de transhumanisme).

14 L'entreprise *Palantir Technologies* symbolise parfaitement cette alliance. Cette société spécialisée dans la science des données développait à ses débuts des logiciels d'analyses pour la communauté américaine du renseignement. Elle s'est ensuite diversifiée dans les secteurs de l'assurance, de la finance, de la santé et s'exporte désormais à l'international. Cette entreprise a été financée dès sa fondation par *In-Q-Tel*, un fonds de capital-investissement géré par la *Central Intelligence Agency* (CIA).

15 L'accord transatlantique *Privacy Shield* qui règle la protection des données personnelles est remise en cause par le nouveau gouvernement américain. Officialisé en juillet 2016, cet accord était censé garantir aux citoyens la protection des données stockées dans le cloud et collectées par les GAFA, et qu'elles ne feraient pas l'objet d'une surveillance massive.

16 Dans cet article, nous définissons une infrastructure critique comme un actif vital et essentiel pour le bon fonctionnement de l'État, de la société et de l'économie.

17 La crise des *subprimes* désigne la crise financière qui a touché le secteur des prêts hypothécaires à risque en 2007. Cette crise est partie des États-Unis et a débouché sur une crise bancaire mondiale, entraînant la plupart des pays industrialisés dans la Grande Récession, soit la pire crise économique depuis la Grande Dépression de 1929.

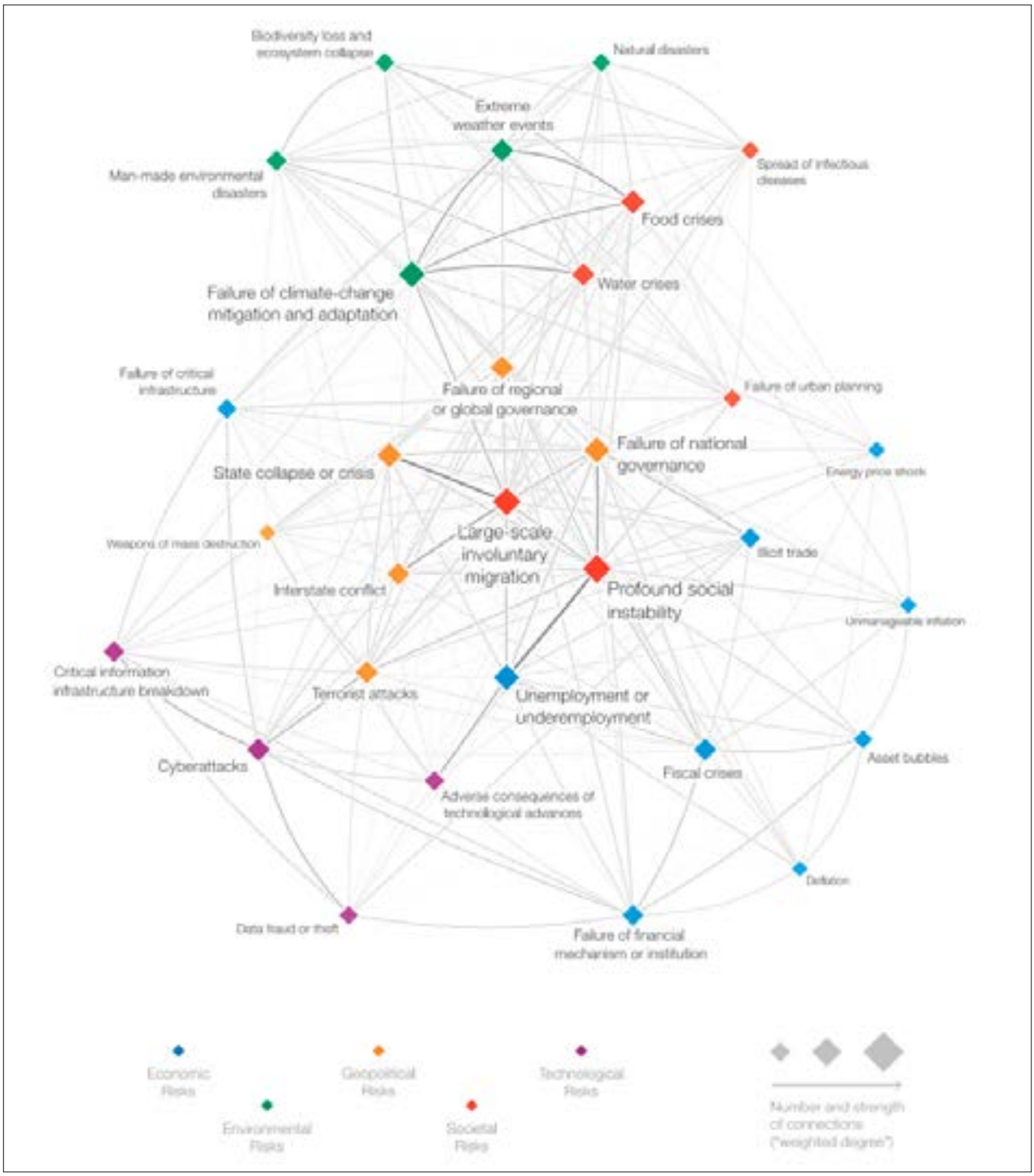

Figure 5 Chaque année le *World Economic Forum* (WEF) établi son *Global Risks Report*. La carte ci-dessus montre les interconnexions des risques globaux en 2017. Le risque technologique (en violet) est surtout corrélé avec le risque économique et le risque géopolitique. (WEF)

Si l'interconnexion des réseaux engendre de nombreuses opportunités, elle implique également l'interconnexion des risques.

Colonne vertébrale de notre économie, les TIC sont devenues la structure sur laquelle tous les biens et les services s'appuient, mais aussi un relais de croissance pour les économies développées. Cette concentration de richesses et de savoirs dans le cyberespace rend celui-ci économiquement attractif pour mener des opérations de guerre économique,[18] de guerre de l'information ou des actions cybercriminelles. Le quasi-anonymat et la difficulté d'attribuer une cyberattaque renforcent encore cette attractivité.

18 La chaire *Economie de Défense* de l'ACAMIL a organisé une grande conférence sur la guerre économique – défis et stratégies – en septembre 2016. La doctrine Gerasimov est analysée dans les actes de la conférence disponibles sur le site www.milak.ch (consulté le 31.03.17).

Le cyberespace transcende désormais tous les aspects de notre société, y compris la souveraineté étatique. Celle-ci se trouve compromise par notre manque d'emprise sur le réseau Internet, ses données et ses services.[19] Si les infrastructures critiques venaient à être sévèrement touchées par une cyberattaque, les citoyens seraient dépossédés de leurs données et l'État ne serait plus capable d'accomplir ses missions régaliennes. Deux des trois conditions de la formation de l'État moderne (citoyens, pouvoir, territoire) ne seraient alors plus réunies. Depuis deux décennies, des plans gouvernementaux de défense des infrastructures critiques se développent. Paradoxalement et parallèlement, les infrastructures critiques connaissent une dérégulation, une privatisation et une libéralisation. L'interaction entre ces deux développements antagonistes posent des questions doctrinales non résolues pour les forces armées. De plus, certaines données nécessaires à l'accomplissement de leurs mandats sont aujourd'hui détenues par des sociétés ou des opérateurs privés.

L'ère de post-vérité et les réseaux sociaux offrent une caisse de résonnance sans précédent à la désinformation et aux opérations de déceptions.[20] Les bulles de filtres et les chambres d'échos[21] viennent encore amplifier la portée des « faits alternatifs », souvent diffusés par des « usines à trolls ».[22] Ce type de propagande inspirée de *l'astroturfing*[23] est le cœur de la stratégie d'ingérence de la Russie dans les dernières élections américaines.[24] Dans son concept de guerre de quatrième génération, William Lind[25] avait déjà théorisé l'apparition de ces phénomènes. Ils permettent de gagner du pouvoir coercitif (P2C) sans utiliser de moyens conventionnels et brouillent les frontières traditionnelles entre guerre et paix, national et étranger, civil et militaire. Dans ce contexte, une victoire sans combat devient possible, réalisant ainsi le vieux rêve du général et stratège chinois *Sun Tzu*.

L'érosion de la souveraineté numérique créé des conditions favorables à la guerre hybride, aux violences infra-guerrières, aux attaques indirectes et non linéaires, théorisées par le Général Gerasimov en 2013 et mises en pratique lors de la crise de la Crimée en 2014.[26] Selon la doctrine Gerasimov, les cyberattaques ne sont qu'un épiphénomène à replacer dans le contexte plus général de la guerre de l'information et de la guerre économique.[27] L'absence de souveraineté numérique crée des conditions favorables aux attaques sur la couche sémantique du cyberespace. Dès lors, la guerre de l'information tend à devenir le centre de gravité des conflits contemporains.[28] La maîtrise du réseau Internet, de ses données et de ses applications devient donc la mère des batailles.

L'absence de souveraineté numérique crée des conditions favorables aux attaques sur la couche sémantique du cyberespace.

L'économie de la cybersécurité, de quoi s'agit-il ?

L'économie de la cybersécurité est un champ de recherche multidisciplinaire qui existe depuis une quinzaine d'années. Cette discipline est issue des sciences informatiques et a ensuite évolué dans de multiples champs de recherche comme la stratégie, la science militaire, les sciences de la complexité, la psychologie sociale, ou encore l'économie comportementale. La majorité des chercheurs sont anglo-saxons et proviennent de prestigieuses universités. Cette communauté de recherche se réunit chaque année au sein du *Workshop on the Economics of Information Security* (WEIS).[29]

L'idée de base de cette discipline est de transférer des modèles et concepts économiques dans les sciences informatiques.

L'idée de base de cette discipline est de transférer des modèles et concepts économiques dans les sciences informatiques. D'autres disciplines ont également participé au décloisonnement de la cybersécurité, comme par exemple : la psychologie avec son concept de résilience[30], la géopolitique qui permet de mieux comprendre les motivations et les conflits qui précèdent les cyberattaques, et la stratégie et la polémologie qui permettent de replacer les cyber-conflits au cœur de la dialectique des volontés. Le droit et les relations internationales sont également des disciplines importantes pour réguler le cyberespace. Le renseignement peut, quant à lui, permettre d'anticiper une cyberattaque ou d'aider à son attribution. Cette approche holistique et multidisciplinaire de la cybersécurité est un changement de paradigme indispensable pour la sécurité numérique.

La cybersécurité a trop longtemps été associée uniquement à la sécurité informatique, se limitant ainsi exclusivement à des mesures techniques de sécurité. Les antivirus, la cryptographie et autres pare-feu – pour ne citer que

19 La présence massive de portes dérobées dans les *firmwares* de nos smartphones, téléviseurs et véhicules intelligentes renforcent encore cette perte d'autonomie.
20 Volkoff, V. 1999. *Petite histoire de la désinformation.* Editions du Rocher.
21 Les *filter bubbles* désignent la personnalisation de contenu informationnel, par des algorithmes, à l'insu de l'internaute. Celui-ci se retrouve alors isolé dans une echo chamber médiatique où ses idées et croyances sont constamment amplifiées et répétées.
22 La notion *d'usine à trolls* qualifie une stratégie de propagande visant à contrôler de nombreux comptes en ligne dans le but de simuler des mouvements de masse, principalement sur les sites et forums des médias de référence.
23 L'*astroturfing* est une technique de propagande utilisée dans les campagnes de relations publiques, publicitaires ou politiques. Elle consiste à simuler un mouvement citoyen, venu de la société civile, dans le but de donner l'impression d'un comportement spontané ou d'une opinion publique dominante.
24 Cette stratégie vise à avantager des candidats favorables à la Russie. Dès lors, il est probable que cette même stratégie soit utilisée lors de l'élection présidentielle française ce printemps et lors des élections générales en Allemagne cet automne.
25 Lind, W., et al. 1989. *The changing face of war: into the fourth generation.* Marine Corps Gazette.
26 En février 2017, le ministre russe de la Défense a confirmé la création, il y a quatre ans, d'une entité consacrée à la guerre de l'information. Ce département, inspiré par la doctrine Gerasimov, est spécialisé dans la contre-propagande, le piratage informatique et la diffusion de fausses nouvelles.
27 Mermoud, A. 2013. *La place financière suisse au cœur de la guerre économique.* Infoguerre.fr
28 Vernez, G. 2009. *L'information, zone de conflit et risque stratégique majeur.* Military Power Revue.
29 Les résultats de nos recherches seront également présentés dans cette conférence scientifique http://weis2017.econinfosec.org/ (consulté le 31.03.2017).
30 En sciences informatiques, la résilience désigne la capacité d'un système à s'adapter et à continuer à fonctionner en mode dégradé pendant une attaque, puis à revenir rapidement à son état initial.

les plus connus – ont longtemps été considérés comme les moyens les plus pertinents pour protéger le cyberespace. Pourtant, des chercheurs de renom ont empiriquement démontré que de nombreux défis liés à la cybersécurité pouvaient être rendus intelligibles, expliqués et résolus en utilisant une approche économique. Des experts affirment même que certains défis en cybersécurité ne peuvent être résolus sans une approche économique. A titre d'exemple, les faiblesses d'un système informatique sont souvent causées par des motivations divergentes des acteurs, formulées par la théorie de l'agence[31], dont la compréhensibilité dépasse les sciences informatiques.

En employant le cadre analytique de cette même théorie à la sécurité du cyberespace, Anderson et Moore[32] ont démontré que les organisations fournissant de la cybersécurité ne supportent pas elles-mêmes les coûts et les pertes d'une cyberdéfaillance. Dès lors, les systèmes de sécurité alloués ne peuvent produire un service à la hauteur des attentes. L'économiste Adam Smith utilise le concept d'aléa moral pour désigner cet effet.[33] Dans le domaine de la cybersécurité, l'aléa moral est accentué par le phénomène croissant de l'externalisation informatique et de l'informatique en nuage.[34]

Les externalités négatives d'une cyberattaque contre une infrastructure critique peuvent être extrêmement élevées.

Les externalités[35] négatives d'une cyberattaque contre une infrastructure critique peuvent être extrêmement élevées,[36] en raison de l'interconnexion des risques et des effets en cascade subséquents. En revanche, les investissements sont forcément limités et ne peuvent compenser que partiellement les externalités. Selon une étude de 2015 de la compagnie d'assurance *Zurich*[37], les risques liés au réseau Internet pourraient supplanter les bénéfices dès 2020, ce qui pourrait engendrer le retour du low-tech volontaire dans certains secteurs stratégiques et un ralentissement du développement de la quatrième révolution industrielle.

Pour une organisation, une cyber-assurance permet de transférer le risque financier d'une cyberattaque. Toutefois, il est peu probable que le marché de la cyber-assurance se développe pour les infrastructures critiques dont le coût des externalités est par définition difficilement quantifiable. Par conséquent, le prix de la prime pour assurer un cyber-risque systémique serait trop élevé, même pour une réassurance. Il convient alors de gérer le risque en appliquant les concepts connus du plan de continuité des activités (PCA)[38] et les méthodes de gestion de crises bien connues des militaires. C'est dans cet esprit que *l'Office fédéral de la population* (OFPP) a rédigé son guide[39] pour la protection des infrastructures critiques en 2015. Ce guide classe les infrastructures critiques par secteurs et sous-secteurs, en évaluant à chaque fois le niveau de criticité selon : « *l'importance relative du sous-secteur par rapport à la dépendance, à la population et à l'économie* ».

Le guide de l'OFPP applique la théorie des coûts marginaux[40] pour identifier les mesures de protection optimales sur le plan économique, selon la méthode suivante : « *l'approche basée sur les coûts marginaux vise un rapport optimal entre les dommages résultant des défaillances ou des dérangements des infrastructures critiques et les coûts des mesures à mettre en œuvre. La quantité de mesures optimales est celle qui donne le total des coûts le plus bas selon le schéma ci-dessous* ».

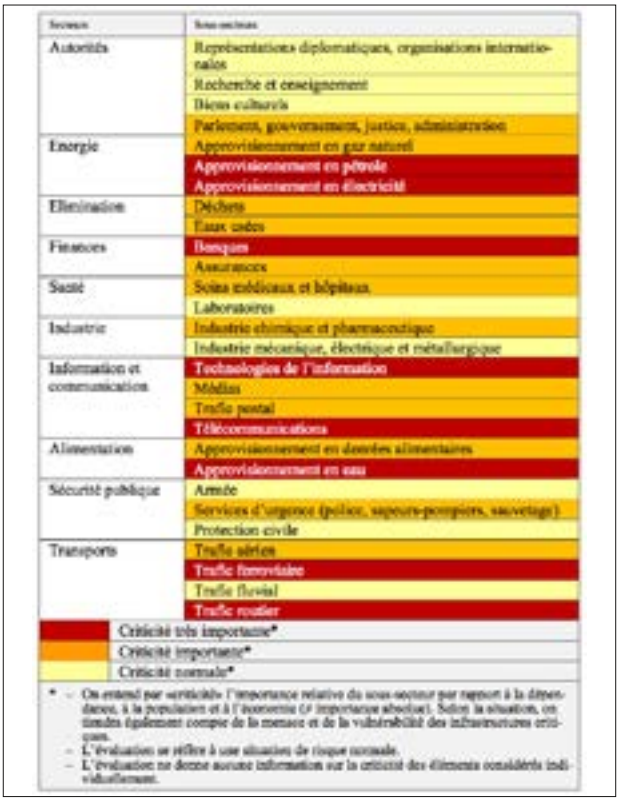

Figure 6 Extrait du guide pour la protection des infrastructures critiques. En rouge les huit sous-secteurs dont la criticité est très importante en Suisse. (OFPP)

31 La théorie de l'agence est une branche de l'économie qui étudie les conséquences du problème *principal-agent*. Ce problème apparaît lorsque l'action d'un acteur économique *(le principal)* dépend de l'action ou de la nature d'un autre acteur (l'agent) sur lequel le principal est imparfaitement informé.

32 Anderon, R., Moore, T. 2006. *The Economics of Information Security.* Science.

33 Un aléa moral *(moral hazard)* peut apparaître dans certaines situations à risque lorsqu'un agent se comporte différemment selon son degré d'exposition au risque. L'aléa moral est, par exemple, observable dans le domaine des assurances, lorsqu'un assuré augmente sa prise de risque, par rapport à la situation où il supporterait seul les coûts d'un sinistre.

34 Le *cloud computing* consiste à exploiter la puissance de calcul et du stockage de serveurs distants via le réseau Internet.

35 Une *externalité* se caractérise par le fait qu'un agent économique crée, de par son activité, un effet externe négatif ou positif en procurant à autrui, et sans contrepartie monétaire, un avantage ou un dommage.

36 Gordon, L., Loeb, M., Lucyshyn, W., Zhou, L. 2015. *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model.* Journal of Information Security.

37 Zurich Insurance Group, Atlantic Council. 2015. *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures.* http://publications.atlanticcouncil.org/cyberrisks/ (consulté le 31.03.2017).

38 Un *PCA* a pour but de garantir la survie d'une organisation après un sinistre important. Ce plan stratégique permet à l'organisation de continuer à fonctionner en mode dégradé, puis de redémarrer l'activité le plus rapidement possible.

39 Le guide complet est disponible sur le site http://www.babs.admin.ch/fr/aufgabenbabs/ski.html (consulté le 31.03.2017).

40 Le coût marginal de production est le coût supplémentaire induit par la dernière unité produite. Le coût marginal joue un rôle fondamental dans l'analyse des décisions de production.

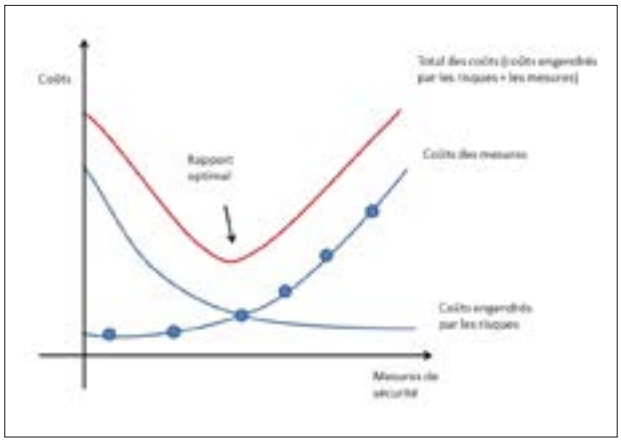

Figure 7 Principe des coûts marginaux. Les points bleus représentent les différentes mesures. Chaque mesure implémentée réduit le coût des dommages résultant d'une défaillance ou d'une perturbation d'une IC. La combinaison est optimale lorsque les coûts totaux (c.-à-d. la somme des coûts des mesures et des dommages résultant de défaillances ou de dérangements des IC) sont au point le plus bas. (OFPP)

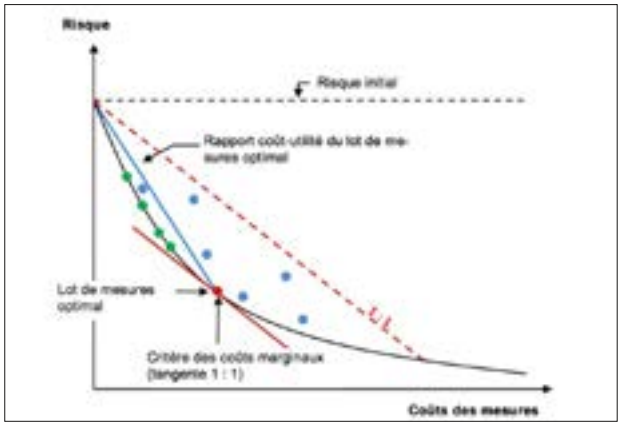

Figure 8 Procédure pour déterminer la combinaison optimale de mesures sur le plan économique. La courbe noire représente la limite inférieure de l'ensemble des mesures. Sur cette courbe, les mesures atteignent une utilité maximale (réduction des risques) avec des coûts minimaux. Toutes les mesures situées au-dessous de la ligne rouge en pointillé (points bleus) ont bien un rapport coût-utilité supérieur à 1 mais elles ne sont efficaces ou optimales que si elles se trouvent sur la ligne noire avant le point de tangente (point rouge) = coûts marginaux des mesures (points verts). (OFPP)

L'économie de la cybersécurité aborde également des problèmes importants à propos des investissements en cyberdéfense. Ceux-ci ne sont pas forcément corrélés avec les bénéfices produits. Il convient donc de trouver le montant optimal d'investissement en cyberdéfense et de mesurer la productivité des mesures choisies. La méthode des coûts marginaux décrite ci-dessus est nécessaire, mais insuffisante. De nombreuses contributions empiriques sont encore attendues par la communauté de recherche en économie de la cybersécurité. Il existe par exemple un besoin important de tester les modèles théoriques développés à ce jour. Afin de contribuer à ce champ de recherche, la chaire *Économie de Défense à l'académie militaire* (ACAMIL) à l'*EPF de Zurich* (EPFZ) mène actuellement deux études scientifiques qui seront présentées dans les sections suivantes. La première se concentre sur les incitations au partage volontaire des informations concernant les cybermenaces. La deuxième porte sur les gains d'efficience engendrés par les technologies de rupture pour la cyberdéfense. Ces deux recherches scientifiques contribuent à renforcer notre souveraineté numérique et la résilience des infrastructures critiques avec des coûts réalistes. Elles répondent aux besoins stratégiques de la défense, de l'industrie et de la recherche académique.

L'humain, ce maillon faible

Cette étude scientifique, menée par Alain Mermoud dans le cadre de sa thèse de doctorat, se focalise sur les incitations au partage volontaire des informations concernant les cybermenaces.[41] Un cadre théorique issu de l'économie comportementale est appliqué dans le contexte de la protection des infrastructures critiques. Un nouveau modèle détaille le mécanisme incitatif qui permet d'orienter les comportements humains vers l'échange volontaire d'informations et qui permet ainsi d'optimiser l'efficience de la cybersécurité. Ce modèle, peu coûteux et relativement simple à mettre en place, permet d'abaisser le coût optimal d'investissement dans la cyberdéfense et contribue à renforcer notre souveraineté numérique. Il permet également de lutter contre les phénomènes de rétention d'information entre les différents acteurs de la chaîne sécuritaire.

L'opération *Olympic Games*[42] restera probablement dans l'histoire comme la première grande campagne de cyberguerre. Le ver informatique utilisé, baptisé *Stuxnet*, a exploité des vulnérabilités *Zero day*.[43] Son inhabituelle complexité en a fait une cyber-arme redoutable pour perturber et dégrader les centrifugeuses iraniennes. Il est intéressant de relever que le virus a été inoculé par ingénierie sociale, c'est-à-dire que les failles humaines des ingénieurs iraniens ont été utilisées pour les inciter à connecter des clés USB infectées sur le réseau interne des centrifugeuses. Cet exemple démontre que la manipulation psychologique humaine joue un rôle important même dans le cas d'attaques techniquement complexes. Les comportements humains inadéquats sont souvent le maillon faible de la chaîne sécuritaire.

Les comportements humains inadéquats sont souvent le maillon faible de la chaîne sécuritaire.

Par conséquent, les techniques d'ingénierie sociale ont fortement progressé ces dernières années. Une tendance a émergé dans la littérature scientifique selon laquelle les

41 L'échange d'information sur les cybermenaces consiste à partager des informations pertinentes pour la cybersécurité entre agents économiques. Ces informations peuvent porter sur une faille, une vulnérabilité, un maliciel, des techniques de hameçonnages (*phishing*), une fuite de données, etc. Un agent peut également partager des informations à propos des bonnes pratiques (résolution d'un incident), une compétence particulière, des avis et conseils d'experts, ou encore des renseignements pertinents pour la cybersécurité.

42 L'opération *Olympic Games* est une série de cyberattaques secrètes, menées en 2010 par les États-Unis et Israël, contre le programme nucléaire iranien.

43 *Zero day* (jour zéro) désigne une vulnérabilité informatique inconnue du public et qui ne dispose pas d'un correctif connu. La partie adverse peut exploiter cette asymétrie de l'information à son avantage.

problèmes de cybersécurité sont souvent liés à de mauvais comportements humains.[44] Ceux-ci sont généralement engendrés par un mauvais design des systèmes d'information et de mauvaises incitations. L'exemple typique est celui du mot de passe inscrit sur un post-it à côté de l'ordinateur. L'utilisateur sait qu'il s'agit d'un mauvais comportement qui peut mettre en danger sa propre sécurité. Cependant, la mémorisation d'une quantité exponentielle de mots de passe complexes n'est pas gérable pour un utilisateur lambda, ce qui l'incite à de mauvais cybercomportements. Cet exemple démontre l'importance d'une approche multidisciplinaire de la cybersécurité et qu'il est donc essentiel de mener la recherche académique au-delà du domaine traditionnel de la sécurité informatique.

La politique de sécurité du WEF a réuni de nombreux experts scientifiques en cybersécurité lors de sa dernière édition. Les experts présents, en collaboration avec *Interpol* et *Europol*, ont démontré que l'échange d'informations entre le secteur public et le secteur privé permettait d'aboutir à des systèmes de protection efficaces. Toutefois, cet échange nécessite une importante confiance entre les régulateurs, l'industrie et le secteur public. Cette confiance doit se construire sur le long terme. Elle est particulièrement difficile pour les multinationales qui opèrent dans des juridictions différentes et complexes. Il est donc essentiel de clairement définir les responsabilités des différents acteurs. Si les experts s'accordent sur la nécessité de partager des compétences et des informations, ils divergent cependant sur le type de modèle à déployer pour favoriser la confiance réciproque.

Les experts s'accordent sur la nécessité de partager des compétences et des informations.

Du point de vue du renseignement, le partage d'informations sur les cybermenaces permet de produire du *Cyber Threat Intelligence* (CTI). Le CTI est une discipline basée sur le cycle du renseignement (analyse des besoins, collecte, analyse et diffusion des informations) qui est bien connue des militaires. Elle a pour finalité la production du renseignement lié aux cybermenaces, par exemple dans le but d'alimenter les systèmes de détections précoces ou les CERTs.[45] Ce renseignement sur et depuis le cyberespace est la première ligne de défense contre les cyberattaques. Il permet d'anticiper les attaques, de s'adapter et de contribuer à l'attribution d'une cyberattaque en identifiant son origine ou son auteur, ou en détectant des tendances sur les méthodes utilisées et les secteurs touchés. Il existe donc un lien indissociable entre le renseignement et la cybersécurité.

Ce renseignement sur et depuis le cyberespace est la première ligne de défense contre les cyberattaques.

Plusieurs économistes et actuaires ont proposé des modèles quantitatifs pour pallier au manque d'investissement chronique dans le domaine de la cybersécurité. Ces modèles d'investissements ont théoriquement démontré le potentiel de l'échange d'informations entre infrastructures critiques. Pour une organisation, le partage d'informations permet de réduire le niveau optimal d'investissement en cybersécurité. D'un point de vue économique, l'échange d'informations permet – entre autres – de réduire l'asymétrie d'information,[46] les externalités négatives et surtout d'anticiper les menaces afin d'augmenter la résilience des systèmes d'information. Cependant, les problèmes de rétention d'information et du passager clandestin[47] sont persistants, ce qui ne permet pas d'exploiter tout le potentiel de l'échange d'informations pour prévenir les cybermenaces.

Ainsi, certains régulateurs proposent de contraindre les infrastructures critiques au partage d'informations.[48] Cette contrainte serait similaire à l'obligation d'annonce pour les médecins et les hôpitaux pour certaines maladies transmissibles à déclaration obligatoire.[49] Les premiers résultats montrent toutefois que la régulation ne peut pas fonctionner sans incitations. La Suisse semble plutôt suivre une tendance régulatrice basée sur l'adhésion volontaire. Depuis 2004, la *Centrale d'enregistrement et d'analyse pour la sûreté de l'information* (MELANI) facilite le partage d'informations entre les infrastructures critiques.[50]

Il est important d'identifier les incitations économiques et sociales qui peuvent permettre aux infrastructures critiques de partager des informations spontanément et volontairement.

Plusieurs études ont démontré que l'échange délibéré d'informations concernant les cybermenaces, au sein d'un partenariat public-privé, était plus performant que la contrainte. Dès lors, il est important d'identifier les incitations économiques et sociales qui peuvent permettre aux infrastructures critiques de partager des informations spontanément et volontairement. Un nouveau modèle est donc nécessaire pour comprendre le mécanisme incitatif permettant d'orienter les comportements vers l'échange volontaire d'informations. La confiance demeure une condition primordiale, mais pas suffisante, à

44 Ghernaouti, S. 2013. *Cyber Power : Crime, Conflict and Security in Cyberspace.* EPFL Press.

45 Les CERT *(Computer Emergency Response Team)* sont des centres d'alertes dotés de personnels prêts à réagir aux cyberattaques.

46 En sciences économiques, l'*asymétrie d'information* désigne un échange dans lequel certains des participants disposent d'informations pertinentes que d'autres n'ont pas. La présence d'asymétrie d'information conduit au problème du risque moral.

47 Le problème du passager clandestin *(free-rider)* désigne le comportement d'un agent qui profite d'un avantage sans y avoir investi autant d'efforts (en argent ou en temps) que les autres agents d'un groupe.

48 En 2015, les États-Unis ont adopté le *Cybersecurity Information Sharing Act* (CISA) et l'Union Européenne (UE) le *Network and Information Security Directive* (NIS).

49 Art.12 *de la loi fédérale sur la lutte contre les maladies transmissibles de l'homme.* Selon cette loi, l'*Office fédéral de la santé publique* (OFSP) est contraint d'exploiter, en collaboration avec d'autres services fédéraux et avec les services cantonaux compétents, les systèmes de détection précoce et de surveillance des maladies transmissibles.

50 L'échange d'informations entre MELANI et les exploitants d'infrastructures critiques sera régi par la *Loi fédérale sur la sécurité de l'information* (LSI).

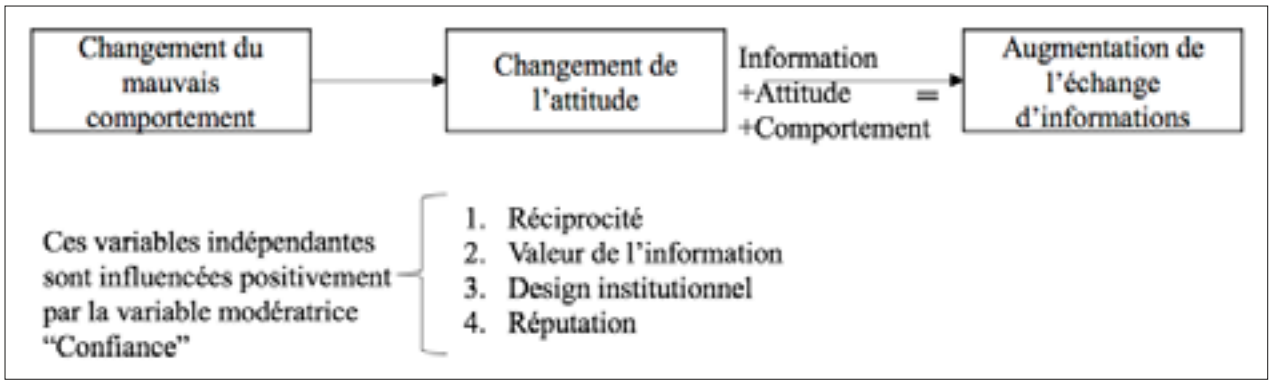

Figure 9 Notre mécanisme théorique permet d'inciter les acteurs de la cybersécurité à échanger des informations. Ce modèle est inspiré de l'économie comportementale et de la théorie des perspectives. (Kahneman & Tversky)

l'échange d'informations. Par conséquent, nous avons défini la confiance comme une variable modératrice dans notre modèle théorique présenté ci-dessous. Ce modèle a été validé par un comité scientifique international et présenté lors d'une conférence scientifique.[51]

Notre recherche a pour but de confirmer ou d'infirmer les impacts de facteurs clés dans le partage de l'information cybernétiquement pertinente. Les quatre variables indépendantes étudiées sont les suivantes : la réciprocité dans l'échange d'informations, la valeur de l'information, la réputation et le design institutionnel des plateformes d'échanges. Lors d'études précédentes, ces quatre « effets » ont été identifiés comme des éléments précurseurs au partage de l'information.[52] Nos résultats devraient permettre d'investiguer les facteurs pertinents à développer afin d'atténuer les problèmes de rétention d'information et du passager clandestin.

Nos résultats devraient permettre d'investiguer les facteurs pertinents à développer afin d'atténuer les problèmes de rétention d'information et du passager clandestin.

Notre modèle incitatif est compatible avec une vision libérale et décentralisée de la cyberdéfense. Cette vision se base sur l'idée que, pour bien fonctionner, un système doit reposer sur la responsabilité individuelle et la motivation intrinsèque de ses membres, plutôt que sur la contrainte juridique. Cette vision, similaire à celle du système de milice, repose donc fondamentalement sur la confiance et une collaboration forte entre le secteur public et le secteur privé. Ce modèle a été développé dans le cadre de la protection des infrastructures critiques, mais il peut aussi être utilisé dans d'autres domaines (par exemple : le partage d'informations entre agences de renseignement). La Suisse offre un cadre idéal au déploiement de ce modèle grâce à sa stabilité politique et son haut degré de confiance envers les institutions.

Technologies de rupture et cybersécurité

Cette étude scientifique, menée par Dimitri Percia David dans le cadre de sa thèse de doctorat, vise à déterminer les effets des technologies de rupture[53] sur la dynamique des investissements en cybersécurité et des gains d'efficience subséquents. L'avènement de technologies de rupture comme les systèmes d'analyses et de traitement des mégadonnées (*Big Data Analytics;* BDA)[54] ou la chaîne de blocs[55] – pour ne citer que celles-ci – implique un retour sur investissement disruptif vis-à-vis des mesures de cybersécurité conventionnelles. Le succès de ces mesures restant limité, le marché de la sécurité informatique commence à s'adapter. Cette étude scientifique se déroule dans le contexte de la protection des infrastructures critiques et vise à délivrer des recommandations politiques afin d'optimiser les investissements dans le domaine de la cyberdéfense. La partie théorique de cette thèse a été validée par un comité scientifique international et présentée lors d'une conférence scientifique.[56]

Le modèle présenté précédemment vise à réduire le problème de la rétention d'information et des mauvais comportements humains. D'un point de vue théorique, une autre solution serait de supprimer ou diminuer les interactions humaines (par exemple en automatisant le processus du partage d'informations). D'un point de vue pratique, cette solution n'a encore jamais été appliquée. Cependant, la chaîne de blocs pourrait remettre en question les modèles développés à partir de l'économie comportementale. En effet, cette technologie permet de supprimer les intermédiaires et de

51 Mermoud, A., Keupp M.M., Ghernaouti, S., Percia David, D., 2016. *Using incentives to foster security information sharing and cooperation: a general theory and application to critical infrastructure protection.* The 11th International Conference on Critical Information Infrastructures Security, Paris. http://www.critis2016.org/ (consulté le 31.03.2017).

52 ENISA. 2010. *Incentives and challenges for information sharing in the context of network and information security.* https://www.enisa.europa.eu (consulté le 31.03.2017)

53 Une technologie de rupture *(disruptive technology)* est une innovation radicale qui remplace à terme une technologie existante. Par opposition, les technologies de continuité améliorent par incréments successifs une technologie existante.

54 Le terme mégadonnées *(Big Data)* se réfère aux données dont la complexité rend leur traitement (extraction, gestion, sollicitation et analyse) irréalisable par les technologies quantitatives classiques. La complexité des mégadonnées est définie par trois aspects: 1) le volume (téraoctets, pétaoctets, ou même exaoctets (1000^6 octets) ; 2) la vitesse (à laquelle les données sont générées) et 3) la variété (liée aux mélanges de données structurées et non structurées).

55 La chaîne de blocs *(blockchain)* est une base de données distribuée qui fonctionne d'une manière décentralisée. Les monnaies cryptographiques, comme le *bitcoin* (système de paiement pair à pair), utilisent cette technologie. Toutes les transactions sont transparentes, vérifiées par les nœuds du réseau et enregistrées dans un registre public théoriquement infalsifiable.

56 Percia David, D. Keupp, M. M., Ghernaouti, S., Mermoud, A., 2016. *Cyber Security Investment in the Age of Big Data: Reassessment of Gordon-Loeb Model and Application to Critical Infrastructure Protection.* The 11th International Conference on Critical Information Infrastructures Security, Paris.

générer automatiquement de la confiance entre les utilisateurs. De plus, son mode de fonctionnement décentralisé est parfaitement compatible avec le fédéralisme helvétique et elle pourrait permettre d'automatiser le partage d'informations. Réputée inviolable, cette technologie balbutiante est promise à un bel avenir et les débouchés pour la cybersécurité sont nombreux.

Les systèmes d'analyse des mégadonnées sont susceptibles de devenir la prochaine génération de technologies de l'information. Certains experts pensent que le futur des *Information Sharing and Analysis Centers* (ISACs)[57] réside dans l'émergence des Fusion Centers. Ces centres ont été créés aux États-Unis après les attentats du 11 septembre 2001, pour favoriser le partage d'informations entre les différentes agences de renseignement, le *Département de la Sécurité intérieure* et le *Département de la Justice*. Ils permettent de collecter, d'agréger et de fusionner des informations provenant de différentes sources hétérogènes. Contrairement à la chaîne de blocs, cette solution centralisatrice et bureaucratique semble moins bonne dans le contexte helvétique.

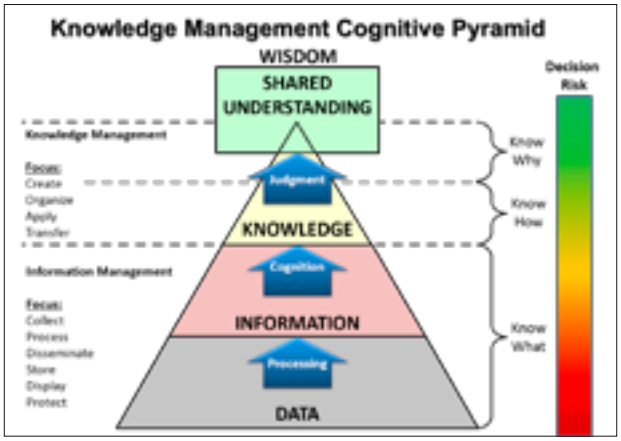

Figure 10 La pyramide de DIKW (Data, Information, Knowledge, Wisdom) adaptée par l'*US Army*. Le but du BDA est en fait de générer du Small Data. Cette pyramide montre le processus nécessaire pour transformer et contextualiser des données non structurées (matière première) en sagesse, voire en Smart Data. (Wikipedia CC BY-SA 4.0)

Ces technologies de rupture sont essentielles pour renforcer notre souveraineté numérique et investir d'une manière optimale dans la cyberdéfense.

Dans tous les cas, ces technologies de rupture sont essentielles pour renforcer notre souveraineté numérique et investir d'une manière optimale dans la cyberdéfense. En développant un modèle actuariel basé sur les coûts liés à la cybersécurité, *Gordon et Loeb*[58] ont proposé d'investiguer le niveau optimal d'investissement en cybersécurité, *ceteris paribus*. En partant du principe que la préoccupation principale de chaque organisation est de maximiser son bénéfice net provenant de ses dépenses en cybersécurité, les deux chercheurs déterminent une fonction permettant d'établir un niveau optimal d'investissement en cybersécurité. Ce dernier correspond à la minimisation du coût total, c'est-à-dire à la somme de la valeur de la perte générée par des failles cybersécuritaires et de la valeur du montant investi afin d'acquérir des technologies ayant pour but de se prévenir de telles failles.

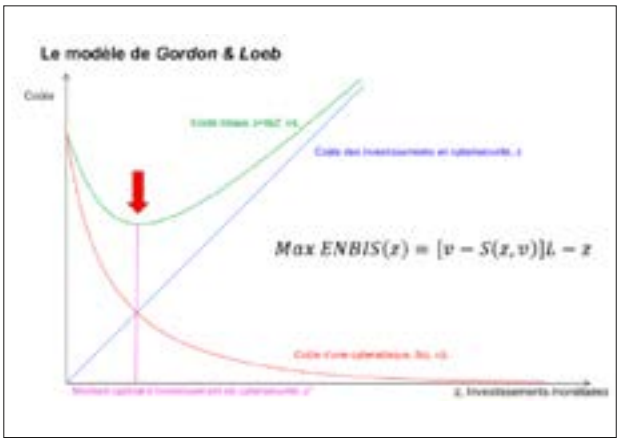

Figure 11 Ce modèle permet de calculer le montant optimal d'investissement en cybersécurité (flèche rouge) en fonction de la vulnérabilité des systèmes et de la perte potentielle dûe à une cyberdéfaillance. (Gordon & Loeb, 2002)

Ce modèle permet par exemple de calculer une prime pour une cyber-assurance. Il permet ainsi de conclure que le montant investi par une organisation pour sa cybersécurité ne devrait pas dépasser 37 % des pertes potentielles engendrées par une cyberattaque. Les pertes liées aux risques cybersécuritaires, ainsi que le montant investi dans les technologies de protection informatique, sont intrinsèquement liés à l'efficacité des produits et services du marché de la sécurité numérique. Depuis une trentaine d'années, ce dernier propose de nombreux moyens techniques conventionnels basés sur l'analyse des signatures, pour accroître la sécurité informatique. Les mécanismes de contrôle d'accès, les systèmes de détection d'intrusion, les techniques de cryptage, pare-feu et logiciels anti-virus ont ainsi vu le jour. Or, le succès de ces mesures est toutefois limité.

Les technologies actuelles basent leur stratégie essentiellement sur la détection des menaces qui ont déjà été observées dans le passé.

Les technologies actuelles basent leur stratégie essentiellement sur la détection des menaces qui ont déjà été observées dans le passé. Une telle approche devient de moins en moins appropriée face à une cybercriminalité grandis-

57 Les *ISACs* sont des plateformes, qui s'appuient généralement sur un partenariat public-privé et à but non lucratif, dont l'objectif est de favoriser l'échange d'informations entre les infrastructures critiques privées et publiques.
58 Gordon, L.A., Loeb, M.P. 2002. *The economics of information security investment*. ACM Transactions on Information and System Security (TISSEC).

sante. La complexité et la rapidité d'exécution deviennent des défis colossaux. Un écart grandissant se fait ressentir entre les moyens de la cybercriminalité et le retard de détection des signatures inappropriées. De plus, les vulnérabilités dites *Zero day* ne peuvent pas être prises en considération par une telle approche. Par conséquent, les techniques conventionnelles peuvent être facilement rendues inefficaces par les cybercriminels. Ce constat d'échec devient davantage alarmant à l'ère des mégadonnées. En effet, des exaoctets d'informations sont transférés tous les jours, ce qui donne de nombreuses possibilités aux cybercriminels pour accéder à des réseaux en dissimulant leur présence et en infligeant des dégâts difficilement détectables.

Afin de répondre à une cybersécurité défaillante, le marché de l'informatique commence à s'adapter en donnant moins d'importance à l'approche conventionnelle et en développant une approche novatrice de détection d'actions inappropriées. La récente discipline académique que les Anglo-Saxons nomment *Security Analytics* permet d'opérer ce changement de vision. En employant les technologies dérivées du BDA, des procédés de détection précoce (basés sur la prospection active de menaces en temps réel) permettent la création de renseignements ciblés afin de prévenir les cybercrimes. Ces méthodes sont susceptibles de devenir la prochaine génération de technologies de l'information et permettront un retour sur investissement disruptif par rapport aux mesures conventionnelles. Cette rupture fondamentale permettrait ainsi de passer du principe clé de résilience des infrastructures (élément réactif) au principe d'anticipation (élément actif) des infrastructures. L'avènement d'une telle technologie et ses conséquences disruptives sur le niveau optimal d'investissement en cybersécurité, ainsi que l'étude des nouvelles dynamiques d'investissements, sont des éléments qui méritent d'être investigués. Quels que soient les résultats d'une telle recherche académique, les apprentissages délivreront de multiples indices sur la façon d'optimiser les investissements en cybersécurité et permettront ainsi d'augmenter l'efficience des mesures envisagées.

Passer du principe clé de résilience des infrastructures (élément réactif) au principe d'anticipation (élément actif) des infrastructures.

Nous proposons d'étendre le modèle de *Gordon et Loeb* à plusieurs périodes et de relaxer l'hypothèse de continuité de la fonction de probabilité de défaillance sécuritaire. Ces adaptations permettent de capturer les aspects dynamiques des investissements tels que l'avènement d'une technologie radicalement innovante (le BDA ou la chaîne de blocs). Nous proposons ainsi d'étudier théoriquement et empiriquement les conséquences d'une telle technologie sur les investissements.

En basant la conceptualisation d'une expérience sur la théorie des jeux et sur les systèmes de sécurité interdépendants, les données récoltées seront utilisées par un modèle économétrique afin de corroborer ou infirmer nos hypothèses d'efficience et leurs conséquences pour la cybersécurité. Nous illustrerons notre approche dans le contexte de la protection d'une infrastructure critique représentée par les forces armées. Bien que les technologies du BDA soient considérées comme prometteuses pour la protection des infrastructures critiques, leurs effets concrets n'ont à notre connaissance jamais été investigués dans le milieu académique. Cette étude devrait permettre de répondre à ce besoin.

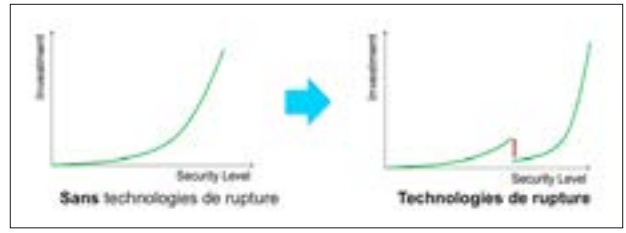

Figure 12 Le but de cette recherche est d'analyser l'impact des technologies de rupture sur le modèle de Gordon et Loeb. (ACAMIL)

État stratège et Intelligence Economique

En conclusion, la cybersécurité ne se limite pas aux aspects techniques des sciences informatiques. Les études présentées dans cet article contribuent au développement d'un nouveau champ de recherche : l'économie de la cybersécurité. Elles fournissent des pistes pour renforcer notre souveraineté numérique et augmenter l'efficience de la cyberdéfense. Les deux recherches présentées sont complémentaires, puisque la deuxième bénéficie directement des résultats de la première. Les résultats scientifiques détaillés des deux thèses de doctorat seront publiés dans des périodiques scientifiques spécialisés.

Depuis 2010, les cyberattaques n'ont cessé de se multiplier contre les intérêts nationaux.

Nos recherches présentent des conséquences politiques pour la Suisse, sa souveraineté numérique, sa sécurité économique et ses forces armées. Depuis 2010, les cyberattaques n'ont cessé de se multiplier contre les intérêts nationaux. Le cas américain démontre qu'une stratégie de maintien et d'accroissement de puissance passe aujourd'hui obligatoirement par la maîtrise des systèmes d'information, de leurs services et usages incontournables. Toute proportion gardée, la Suisse doit donc se doter d'une stratégie numérique pragmatique et d'un partenariat public-privé efficace. Seule une approche holistique de la souveraineté numérique – respectant le fédéralisme et le contexte helvétique – permettra de combler notre vide stratégique numérique.[59]

A ce titre, la stratégie « *Suisse numérique* » adoptée en 2016 fixe des idées cohérentes. Cette stratégie est une première base indispensable permettant de produire de la valeur liée aux données, nouveau pétrole de l'ère numérique. La Suisse doit créer et maintenir des conditions favorables

59 Baumard, P. 2012. *Le vide stratégique.* CNRS Editions.

pour bénéficier de la quatrième révolution industrielle, renforçant ainsi ses atouts : stabilité et neutralité politique, système d'éducation performant et capital humain de haute qualité, culture de la confidentialité, et surtout le développement d'un cadre juridique garantissant la protection des données. Cette prise de conscience se matérialise déjà par la récente création de *VIGISWISS*[60], une association qui regroupe les sociétés actives dans le stockage et la protection des données en Suisse.[61] A titre d'exemple, avec la fin du secret bancaire, la Suisse pourrait ainsi proposer la sécurité des données comme nouveau modèle d'affaire.[62]

Avec la fin du secret bancaire, la Suisse pourrait ainsi proposer la sécurité des données comme nouveau modèle d'affaire.

La première *Stratégie nationale de protection contre les cyber-risques* (SNPC)[63] 2012 – 2017 a permis d'implémenter 15 des 16 mesures prévues. Le Conseil fédéral a néanmoins décidé de mettre en place une deuxième stratégie pour les années 2018 – 2023. Ces nouvelles mesures pourraient intégrer une réflexion stratégique sur la souveraineté numérique. Si une autarcie numérique helvétique semble impossible sur la couche physique du cyberespace[64], il convient toutefois de tendre vers une souveraineté numérique sur les couches logiques et sémantiques. La création d'un *cloud souverain*, basé sur des logiciels libres permettant de rapatrier des données stratégiques sur notre territoire, serait par exemple une mesure intéressante concernant la couche logique.[65] A titre d'exemple, Swisscom propose désormais un cloud suisse dans son offre de base. La souveraineté numérique tend donc à devenir un argument commercial.

La Suisse pourra ainsi augmenter sa capacité à produire son propre renseignement, afin de réduire sa dépendance aux services étrangers.

Concernant la couche sémantique, la nouvelle loi sur le renseignement *(LRens)* entrera en vigueur en septembre 2017. Elle apportera des nouvelles ressources au *Service de renseignement de la confédération* (SRC). La Suisse pourra ainsi augmenter sa capacité à produire son propre renseignement, afin de réduire sa dépendance aux services étrangers. La *LRens* permettra au SRC et à la Confédération de disposer d'une monnaie d'échange informationnelle, renforçant ainsi leur crédibilité sur le marché international du renseignement.[66]

Ces différentes mesures sont un premier pas en direction d'une souveraineté numérique, mais cela est insuffisant par rapport aux enjeux civilisationnels liés à la quatrième révolution industrielle. Selon de nombreux experts cette révolution est d'ordre structurel : « la blockchain n'est pas la révolution tant annoncée, elle n'est que l'outil d'un monde lui-même entré en révolution ».[67] La chaîne de blocs ressemble au modèle suisse : décentralisation, sécurité, confiance. Les monnaies cryptographiques (systèmes de paiement pair à pair) remettent par exemple en question le monopole de l'État sur la création monétaire. Les forces armées n'échapperont évidemment pas à cette révolution. Par conséquent, il est nécessaire de revoir la traditionnelle appréciation de la situation pour y ajouter un sixième facteur « information » (liée à la guerre de l'information) et relativiser l'importance du facteur milieu (géographique).

Inspirée du renseignement, l'Intelligence Economique offre une grille d'analyse permettant de décrypter le dessous des cartes.

Un agenda numérique soutenu par une politique publique d'Intelligence Economique (IE)[68] pourrait permettre l'émergence d'un « soft power ». Cette puissance d'influence est aujourd'hui indispensable pour former un « smart power suisse », soutenu par le « hard power ». L'IE peut permettre l'émergence d'un État stratège capable de mieux anticiper, pour moins se laisser surprendre. Un tel État doit se doter d'un outil de pilotage stratégique capable de détecter de manière proactive les risques et les opportunités. Inspirée du renseignement, l'IE offre une grille d'analyse permettant de décrypter le dessous des cartes et d'armer intellectuellement l'Etat pour comprendre les forces à l'œuvre, décrypter les alliances et les stratégies d'actions. L'IE permet également d'optimiser le transfert de connaissances et de méthodologies entre la sphère militaire et la sphère économique.[69] L'IE est également une méthode permettant de créer de la sécurité économique pour nos entreprises. Par ailleurs, une telle politique permettrait d'augmenter notre emprise sur nos réseaux informatiques, colonne vertébrale de notre économie. Car « si l'on fait la guerre comme on produit des richesses »[70] les conflits futurs se cristalliseront autour de l'information, de ses systèmes et de ses réseaux. Il est toutefois nécessaire de rappeler que les nouvelles cybermenaces viennent s'ajouter aux menaces conventionnelles (sans les remplacer) et que la majorité des conflits finissent par devenir territoriaux.

60 https://www.vigiswiss.ch/fr/ (consulté le 26.02.17).
61 La nouvelle loi sur la protection des données est toutefois jugée insuffisante par les organisations de protection des consommateurs car elle n'attribue pas le contrôle des données aux citoyens. Ceux-ci sont privés de deux éléments essentiels de la législation européenne : le droit à la portabilité et le droit à l'oubli.
62 La société *Swiss Data Safe SA* rachète et rénove des anciens bunkers de l'Armée suisse. Cette société utilise la sécurité associée à la Suisse pour vendre un coffre-fort de données privées.
63 https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html (consulté le 28.02.2017).
64 Le développement du dernier *Smaky* autonome a complètement cessé en 1995. Ce micro-ordinateur helvétique avait été développé à l'EPFL par le Prof. Nicoud et vendu par la société *EPSITEC SA*.
65 En 2014, la France s'est dotée d'un *Institut à la souveraineté numérique* (ISN) dont le but est de faire connaître les enjeux de la souveraineté numérique au grand public et aux élus.
66 Mermoud, A., Percia David, D. 2016. *La LRens : réduire le vide stratégique numérique suisse.* Revue Militaire Suisse.
67 Leloup, L. 2016. *Blockchain, la révolution de la confiance.* Eyrolles.
68 L'Intelligence Economique (IE) peut se résumer en une formule : la bonne information, à la bonne personne, au bon moment, et d'une manière sûre. L'IE repose sur trois piliers fondamentaux : la veille stratégique, la protection de l'information, l'influence. L'IE fait partie du renseignement de défense et du renseignement d'intérêt militaire avec, pour ne citer qu'un exemple, le renseignement scientifique.
69 Mermoud, A., Percia David, D. 2016. *L'Intelligence Economique : du renseignement militaire au renseignement privé.* Revue Militaire Suisse.
70 Wicht, B. 2013. *Europe Mad Max demain ? Retour à la défense citoyenne.* Favre.

Figure 13 Une équipe suisse de milice a gagné l'édition 2015 du Cyber Challenge. (Atlantic Council, GCSP)

La majorité des conflits finissent par devenir territoriaux.

A ce titre, la République et canton de Genève fait figure de pionnier avec sa stratégie économique 2030 qui fait explicitement référence à l'IE. Avec l'entrée en vigueur de sa nouvelle *Loi sur la police* (LPol), le canton s'est doté d'un conseil consultatif de sécurité qui a rédigé une stratégie sécuritaire 2030.[71] Ce document stratégique réitère l'importance de développer une capacité de veille stratégique et d'IE. Fin 2017, le canton prendra également part à un exercice de conduite stratégique. Ces exercices sont essentiels et permettent de développer une réflexion stratégique, ainsi que de tester la coordination entre les différents acteurs de la chaîne sécuritaire. Dès lors, il est essentiel que le prochain exercice du Réseau national de sécurité (ERNS 19) adopte une approche holistique et multidisciplinaire de la cybersécurité.

Sur le plan international, les exercices de conduite politico-stratégique adoptent de plus en plus une approche publique-privée, dans le but d'intégrer l'ensemble des parties prenantes. Les risques ne peuvent plus être gérés en silo et l'interopérabilité est une condition nécessaire à la réussite. Organisée pour la première fois en Europe, l'édition 2015 de la compétition internationale *Cyber 9/12 Student Challenge*[72] est à ce titre un bon exemple. Les participants à ce concours de référence avaient pour but de présenter des mesures de gestion de crise à des décideurs politiques, économiques et militaires, afin de trouver une réponse appropriée à une cybercrise internationale. Soudés par leur solide formation militaire, les participants suisses ont rapidement appliqué les méthodes d'activités de conduite. La Suisse a brillé non seulement comme pays hôte grâce à l'organisation du *Geneva Center for Security Policy* (GCSP), mais également grâce à son équipe qui a décroché la médaille d'or.[73]

Les équipes professionnelles spécialisées dans la cyberdéfense n'ont pas mieux performé que l'équipe de milice.

Cette première place confirme la force de notre modèle de milice qui a permis de réunir une équipe de quatre étudiants aux profils éclectiques (ingénieur, juriste, militaire, économiste), parlant différentes langues et provenant de

71 http://www.ge.ch/dse/doc/news/170315_DSE-Brochure_strat_securitaire.pdf (consulté le 31.03.2017).

72 http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12 (consulté le 31.03.2017)

73 Mermoud, A. 2015. *La Suisse championne du monde de cybersécurité.* Le Temps.

diverses institutions : *ACAMIL, Center for Security Studies* (CSS) et *HEC Lausanne*. Contrairement à ce qu'on l'on pourrait penser, les équipes professionnelles spécialisées dans la cyberdéfense n'ont pas mieux performé que l'équipe de milice. L'équipe de milice a naturellement adopté une approche multidisciplinaire face à un scénario dont l'intensité a rapidement dépassé celui d'une cybercrise de basse intensité. Cet exemple démontre que notre système de milice est adapté à la cyberguerre. Nos deux écoles polytechniques fédérales *(EPF)* forment parmi les meilleurs spécialistes en sécurité informatique du globe. Il convient maintenant d'optimiser le transfert de connaissances, via le système de milice, entre la sphère académique et la sphère militaire. Dans cette optique, l'idée récemment évoquée d'une « cyber école de recrues » nous semble pertinente. Le détachement de cryptologues mis en place au sein de la *Brigade d'aide au commandement 41* est également une initiative intéressante pour favoriser le transfert de connaissances.[74]

La Suisse est idéalement positionnée pour favoriser et accompagner l'émergence d'un Traité International du Cyberespace.

Le *GCSP* est une fondation internationale regroupant 45 États membres. Il est précurseur dans le domaine de la cyberdiplomatie et profite de la Genève internationale pour développer une gouvernance technique du réseau Internet en Suisse.[75] Autres atouts : notre neutralité pourrait permettre d'accompagner la résolution de cyber-conflits en étendant les bons offices au cyberespace[76] Avec ses nombreuses institutions internationales, la Suisse est idéalement positionnée pour favoriser et accompagner l'émergence d'un Traité International du Cyberespace.[77] Celui-ci pourrait offrir une base juridique pour réguler le cyberespace et pour poursuivre les auteurs d'infractions opérant dans différentes juridictions, ce qui n'est pas possible actuellement. *Microsoft* a appelé en février 2017 les États à signer une « convention digitale de Genève » (basée sur la *Convention de Genève* de 1949 relative à la protection des civils en temps de guerre) pour protéger l'usage civil du réseau Internet. En l'absence de souveraineté numérique, des multinationales risquent de se poser en gendarme du cyberespace et de dicter des régulations aux politiques. 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. La maîtrise des données sur le plan individuel est une première étape vers une souveraineté collective. La souveraineté numérique doit donc être considérée comme un droit fondamental, car elle symbolise la maîtrise de notre destin sur les réseaux informatiques et *in fine* de nos libertés politiques, économiques et sociales.

74 Schmidlin, M. 2016. *Mit angewandter Mathematik zu mehr Sicherheit.* ASMZ.
75 Le cyberespace est un espace non régulé. En 2013, un groupe d'experts mandatés par l'*OTAN* a publié le *Manuel de Tallinn*. Ce manuel propose une transposition du droit international aux cyber-conflits et formule des recommandations non contraignantes. Il est disponible à cette adresse: https://ccdcoe.org/tallinn-manual.html (consulté 31.03.17).
76 La *Stratégie de politique étrangère 2016 – 2019* considère la cybersécurité comme un instrument de paix et de stabilité internationale.
77 Ghernaouti, S. 2017. *Pourquoi il faut une Déclaration de Genève du cyberespace.* Le Temps.

Marcus M. Keupp

Dr. oec., Dipl.-Kfm., Privat-docent Economie militaire
Titulaire de la chaire Economie de Défense à l'Académie militaire à l'EPF de Zurich (EPFZ)
E-mail: marcus.keupp@vtg.admin.ch

Alain Mermoud

Doctorant en systèmes d'information à HEC Lausanne et collaborateur scientifique à la chaire Economie de Défense à l'Académie militaire à l'EPF de Zurich (EPFZ)
Capitaine, officier de renseignement
E-mail: alain.mermoud@vtg.admin.ch

Dimitri Percia David

Doctorant en systèmes d'information à HEC Lausanne et collaborateur scientifique à la chaire Economie de Défense à l'Académie militaire à l'EPF de Zurich (EPFZ)
Capitaine, commandant de compagnie
E-mail: dimitri.perciadavid@vtg.admin.ch