Observatoire de la prospective internationale de défense

Cybersécurité et prospective

Par Cécile Wendling, directrice d'études à Futuribles

Note d'analyse n° 1 - Juillet 2013

Délégation aux Affaires Stratégiques

DAS

Un projet réalisé par l'Institut de relations internationales et stratégiques (IRIS), la Compagnie européenne d'intelligence stratégique (CEIS) et Futuribles, pour la Délégation aux affaires stratégiques (DAS)

futuribles
Veille, prospective, stratégie

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

CEIS

SOMMAIRE

Les risques cyber sont identifiés comme une menace émergente majeure dans plusieurs des rapports répertoriés par l'Observatoire prospectif de la défense. L'objectif de cette note d'analyse est de faire une analyse croisée des rapports concernés pour identifier les grandes tendances, les ruptures et les recommandations qui en ressortent, mais aussi pour en souligner certaines limites. Par ailleurs, d'autres sources ou rapports complémentaires ont été ajoutés afin d'avoir un panorama prospectif sur les questions de cybersécurité le plus exhaustif possible, sur la base des publications sorties au cours des années 2012 et 2013.

Les méthodes employées dans les rapports à caractère prospectif

Il faut souligner que les documents analysés ici sont très variés, allant de rapports parlementaires à des productions de *think-tanks* ou d'universitaires. Le vocabulaire employé n'est pas toujours le même et par conséquent les concepts ne recouvrent pas toujours les mêmes champs. D'ailleurs, certains rapports eux-mêmes font mention des décalages entre le vocabulaire des informaticiens, des militaires, des stratèges, etc. Ces divergences de terminologie ne facilitent pas les comparaisons ni les négociations sur les enjeux de cybersécurité [1].

Les rapports à caractère prospectif analysés s'appuient le plus souvent sur de la veille documentaire (rapports, articles de presse, articles académiques, etc.). Ce sont souvent des documents qui synthétisent des études prospectives publiées par des organismes publics et privés [2]. D'autres s'appuient sur des entretiens ou des auditions d'experts, voire sur des enquêtes par questionnaires, au-delà de l'étude documentaire [3]. Enfin, certains travaux s'appuient sur des ateliers prospectifs, réunissant différents *leaders* pour échanger de façon collective et coconstruire ainsi des visions du futur [4].

On peut distinguer des rapports adoptant une vision systémique de la cybersécurité, incluant des données technologiques mais aussi culturelles, au-delà des données purement liées à la cyberdéfense [5], et des rapports à *focus* plus étroit se concentrant sur la menace cyber dans le champ de la défense uniquement [6]. Certains rapports se concentrent exclusivement sur le sujet de la cybersécurité [7] ; dans d'autres, la cybersécurité n'est qu'un chapitre ou un thème parmi d'autres sujets prospectifs comme le réchauffement climatique, la robotisation… [8]

---

1. GRAUMAN Brigid, *Cyber-security: The Vexed Question of Global Rules. An Independent Report on Cyber-preparedness around the World,* Bruxelles : Security & Defence Agenda's (SDA), 2012.

2. DUPONT Benoît, *L'Environnement de la cybersécurité à l'horizon 2022. Tendances, moteurs et implications,* Montréal : Chaire de recherche du Canada en sécurité et technologie, université de Montréal, Note de recherche n° 14, septembre 2012.

3. HOUSE OF COMMONS DEFENCE COMMITTEE, *Defence and Cyber-Security: Sixth Report of Session 2012-13,* vol. 1 « Report, together with formal minutes, oral and written evidence », Londres : The Stationery Office, janvier 2013, 99 p. ; GRAUMAN Brigid, *op. cit.*

4. WEST Darell M., *A Vision for Homeland Security in the Year 2025,* Washington, D.C. : Brookings Institution, *Governance Studies,* juin 2012.

5. DUPONT Benoît, *op. cit.*

6. HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.*

7. DUPONT Benoît, *op. cit.* ; HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.*

8. WEST Darell M., *op. cit.* ; GORE Albert A., *The Future: Six Drivers of Global Change,* New York : Random House, janvier 2013.

Tableau 1 — Géographie, temporalité et méthode de production des rapports

Titre du rapport / pays d'origine	Horizon temporel	Champ géographique couvert	Données sur lesquelles le rapport s'appuie
European Cyber Security Policy / Allemagne	Non communiqué	Europe	Les rapports de la Commission européenne, les législations nationales, etc.
L'Environnement de la cybersécurité à l'horizon 2022 / Canada	2022	Monde	Riche revue de la littérature prospective
Distributed Security as Cyber Strategy / Canada	Non communiqué	Canada	Articles académiques, rapports
The Canadian Forces in 2025 / Canada	2025	Canada	Exemples de faits passés
A Vision for Homeland Security in 2025 / États-Unis	2025	États-Unis	Atelier prospectif avec un groupe d'experts de la sécurité
The Future / États-Unis	Non communiqué	États-Unis	Articles de presse, rapports, articles académiques
Cyber Security and Global Interdependence: What Is Critical? / Royaume-Uni	Non communiqué	Monde	Rapports, articles académiques
Defence and Cyber-Security / Royaume-Uni	Non communiqué	Royaume-Uni	Rapport parlementaire qui s'appuie sur des auditions

Enfin, certains rapports sont centrés sur un État [9] et d'autres ont une vision européenne [10] ou encore plus large au niveau international [11].

Globalement, l'horizon temporel fixé est plutôt à court ou moyen terme (maximum 2025). Il semble difficile sur un sujet tel que la cybersécurité de pouvoir produire des analyses prospectives à 2030 ou 2050 en raison de la rapidité des avancées technologiques. On peut regretter le fait que certains rapports (comme l'ouvrage d'Al Gore) évoquent le futur sans indiquer précisément à quel horizon ils se situent. Cela crée des confusions entre des changements qui pourraient survenir à court terme et des évolutions qui seront beaucoup plus lentes à émerger et à être adoptées. Une des difficultés méthodologiques de l'analyse prospective sur les questions de cybersécurité réside bien toutefois en la mise en cohérence complexe d'horizons temporels divers. Par exemple, les évolutions technologiques évoquées ne se développeront pas toutes à la même vitesse. Le *cloud computing* existe déjà, tandis que l'informatique quantique n'en est qu'à ses balbutiements. Par ailleurs, le temps de la technique et de la technologie n'est pas toujours le même que celui des décisions politiques ou des adaptations du droit.

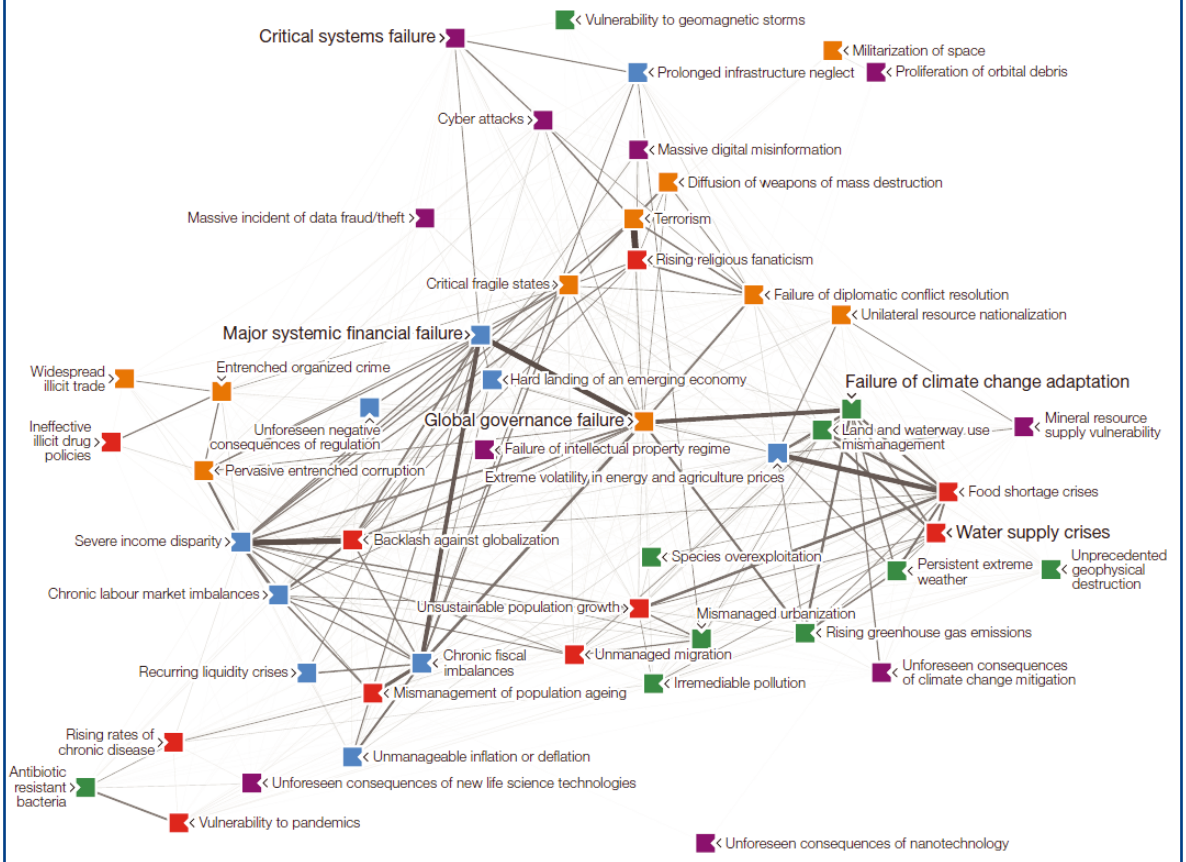
Une autre difficulté méthodologique est de savoir comment l'évolution des risques cyber est interconnectée à d'autres évolutions de risques, avec potentiellement des effets multiplicateurs. Le graphique 1 est une tentative d'explicitation des liens qui peuvent exister entre les cyberrisques et les autres risques d'après le World Economic Forum (WEF).

9. HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.* ; DEIBERT Ron, *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*, Calgary : Canadian Defence & Foreign Affairs Institute (CDFAI), août 2012 ; WEST Darell M., *op. cit.*

10. BENDIEK Annegret, *European Cyber Security Policy*, Berlin : Stiftung Wissenschaft und Politik (SWP, German Institute for International and Security Affairs), *SWP Research Paper*, octobre 2012.

11. DUPONT Benoît, *op. cit.*

Graphique 1 — Carte de l'interconnexion des risques 2013 selon le World Economic Forum



Source : Global Risks 2013: Eighth Edition. An Initiative of The Risk Response Network, Genève : WEF, 2013, p. 53.

Il faut aussi mentionner le fait que la plupart des données sur lesquelles s'appuient les rapports viennent d'entreprises vendant des solutions de sécurité informatique. Il est donc difficile de savoir dans quelle mesure s'appuyer sur ces informations quand elles viennent d'organisations qui pourraient avoir intérêt à vendre le plus de solutions de protection possible, ou bien les solutions pour lesquelles elles ont des positions dominantes sur le marché.

Pour faire face aux difficultés de l'anticipation prospective dans le domaine du cyber, certains pays ont pris des initiatives particulières. C'est le cas du Royaume-Uni avec la « Cyber Future Force », qui se concentre sur les opportunités pour l'avenir, et les ressources à garantir, couplées avec la mise en place d'indicateurs de suivi de performance [12]. C'est le cas aussi aux États-Unis où D. West suggère, dans son rapport de synthèse du *workshop* prospectif, « d'institutionnaliser un mode de pensée orienté vers le futur [13] ».

Les tendances identifiées dans les rapports

Huit tendances lourdes émergent à la lecture des rapports. Elles font l'objet de consensus, quels que soient les pays ou les auteurs.

12. HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.*
13. WEST Darell M., *op. cit.*

1. Augmentation du nombre de connexions fixes et mobiles

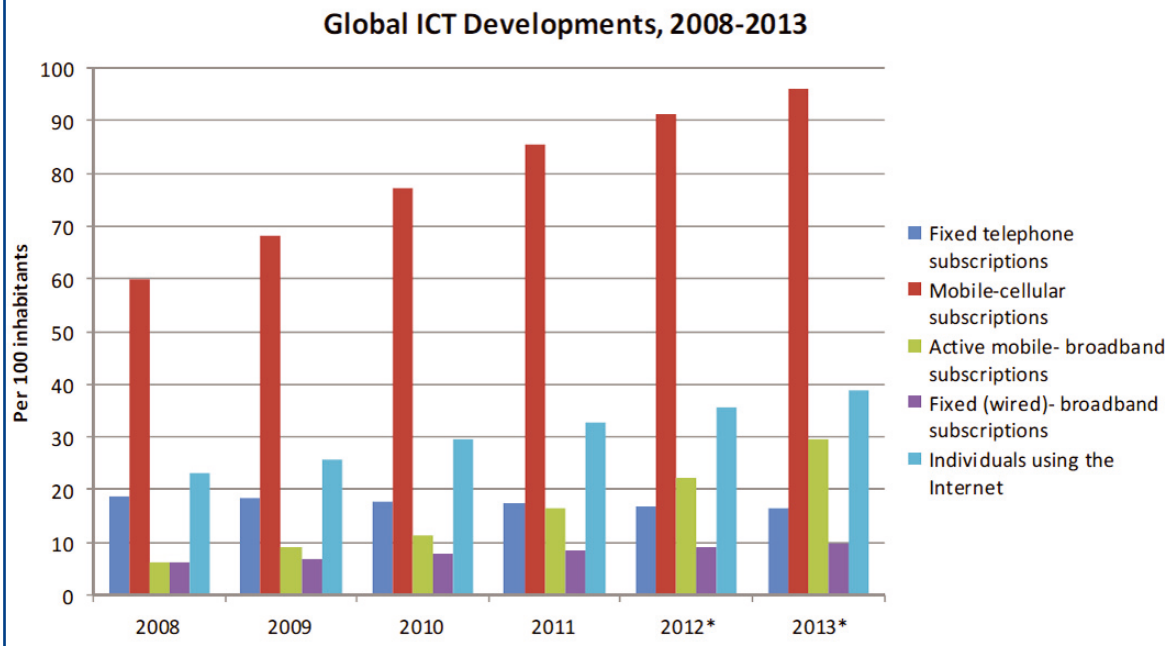
Tous les rapports partent d'une analyse rétrospective soulignant l'augmentation du nombre de connexions fixes ou mobiles et prévoyant la poursuite de cette tendance dans les prochaines années. Le trafic IP (*Internet Protocol*) est en augmentation d'année en année et les chiffres donnés par l'Union internationale des télécommunications (UIT) pour 2013 annoncent une prévision d'augmentation de 14 000 petabytes (10^{15} bytes) par mois, en lien avec le plus grand nombre d'individus et de machines connectées à l'Internet. Les graphiques 2 et 3, issus du dernier rapport de l'UIT, illustrent cette tendance en chiffres.

En lien avec cette augmentation, les rapports mentionnent l'augmentation de la quantité de données stockées sur Internet, le « *big data* » (graphique 4).

2. Augmentation du nombre de cibles potentielles par la mise en réseau croissante des objets et des individus

Comme l'écrivent S. Dutta et B. Bilbao-Osorio, « notre monde hyperconnecté de demain sera construit sur la base des fonctionnalités rendues possibles par la convergence des réseaux de nouvelle génération et de l'ouverture de ces mêmes réseaux, mais il dépassera aussi en un sens ces réseaux de nouvelle génération car il inclura des systèmes d'intelligence ambiants, des connexions automatiques entre machines, et une dimension décuplée de l'Internet des objets. En pratique, il nous faudra être capables de composer avec un très fort degré de connectivité de notre environnement, évoluant avec agilité de réseau en réseau, peu importe où nous allons, peu importe l'heure ou l'objet que nous utilisons [14]. »

Graphique 2 — Tendances mondiales des TIC et pénétration 2008-2013

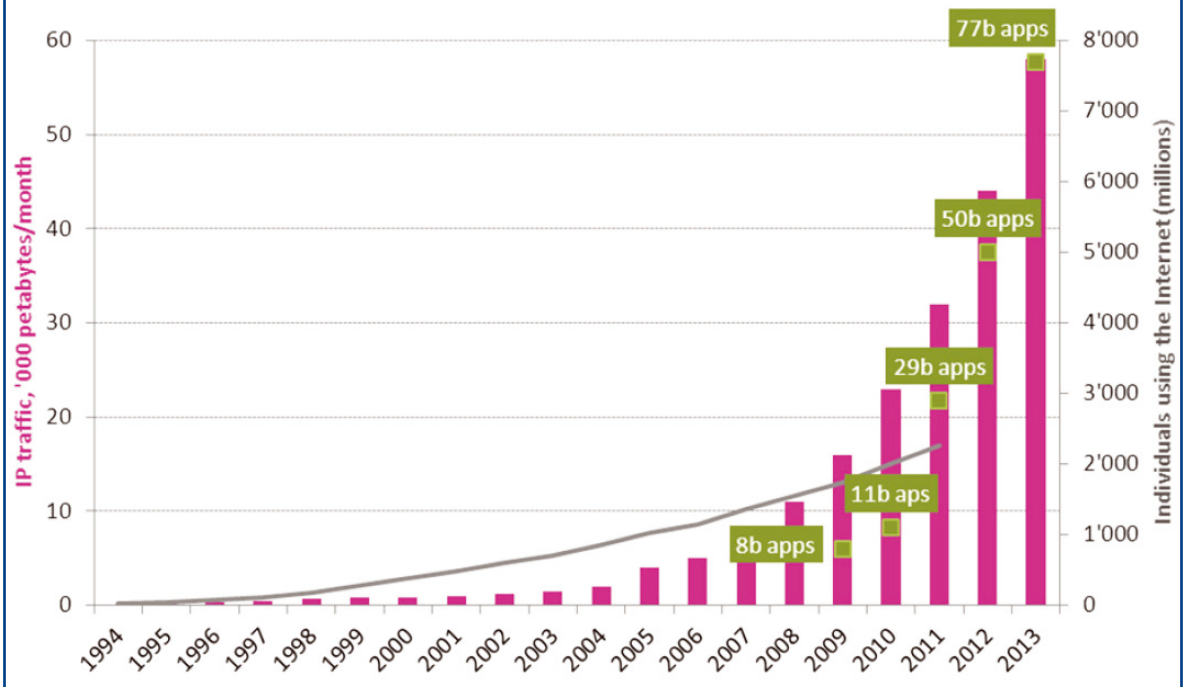


*Estimations.

Source : UIT, base de données World Communication/ICT Indicators.

14. DUTTA Soumitra et BILBAO-OSORIO Beñat (sous la dir. de), *The Global InformationTechnology Report 2012: Living in a Hyperconnected World*, Genève : World Economic Forum, 2012, p. XIV : « *Our future hyperconnected world will build on the functionality made possible by converged next-generation networks (NGN) and*

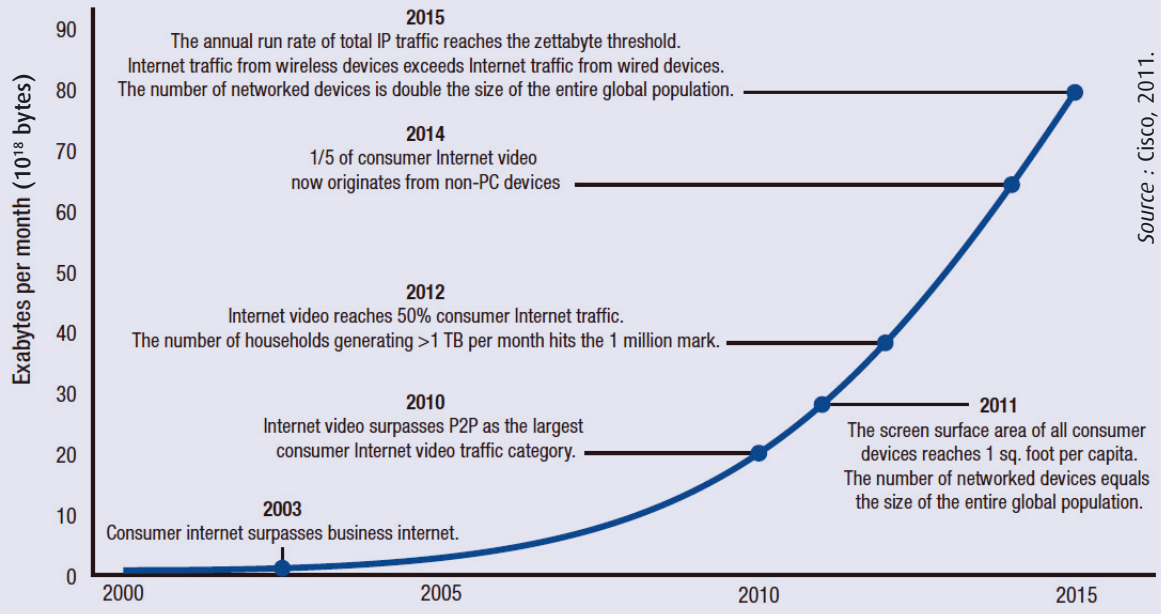
Graphique 3 — Croissance du trafic IP, du nombre d'utilisateurs d'Internet et du téléchargement d'applications 1994-2013



N.B. : « b apps » = milliards d'applications ; les chiffres du trafic IP et des téléchargements d'applications sont des estimations pour les années 2010 à 2013.

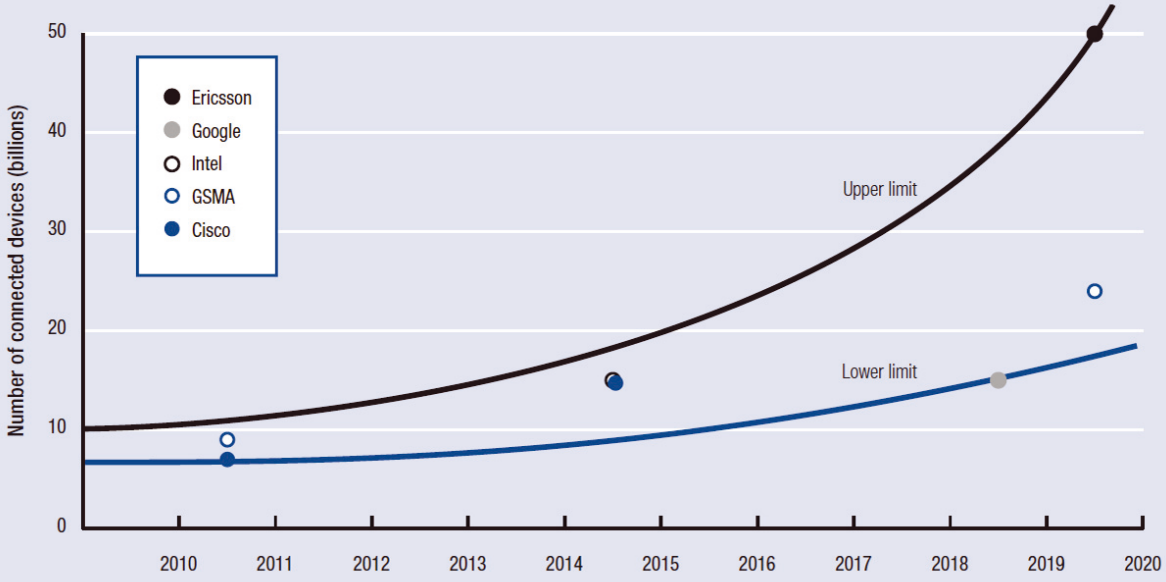
Source : UIT, à partir de données UIT, Cisco VNI, Andrew Odlyzko, RHK, Telegeography, IDC, ABI Research et Cheta Sharma Consulting.

Graphique 4 — Croissance explosive du volume de données



open access networks, but extends the concept of NGN in several ways —through embedded ambient intelligence, automated machine-to-machine traffic, and the sheer size and scale of the Internet of Things. In practice, we should be able to enjoy super-fast connectivity on the move, always-on, roaming seamlessly from network to network, wherever we go —anywhere, anytime, via any device. »

Graphique 4 — Croissance explosive du volume de données



Source : données compilées par l'UIT (pour Intel : Higgenbotham 2009 ; pour Google : Malas 2011 ; pour Cisco : Cisco 2010 ; pour GSMA : Mobile World Live 2011).

En effet, les rapports mentionnent les voitures, les instruments médicaux, les *smart grids,* entre autres, comme pouvant entraîner des problèmes physiques et des effets sur les personnes en cas de cyberattaque, du fait de la plus grande connexion des objets à l'Internet. Al Gore, dans son livre *The Future*, écrit : « Avec autant d'objets connectés, contrôlant la distribution d'eau, d'électricité, les centrales, les industries, le transport et bien d'autres infrastructures stratégiques, il n'est pas difficile d'imaginer des scénarios dans lesquels des attaques cyber auraient des effets physiques concrets sur nos sociétés [15]. » Certains rapports font aussi le lien avec la robotique mobile connectée, comme possible faille de sécurité [16].

Il n'est plus possible de distinguer le domaine de la défense du domaine de la sécurité, les menaces externes et internes, lorsque l'on parle de l'Internet des objets et des cyberattaques qui y seraient liées, comme l'écrit A. Bendiek [17]. Il faut donc développer de nouvelles façons de concevoir la sécurité des réseaux et des flux, et aller au-delà des organisations en silo pour faire face [18].

Un cas particulier d'augmentation de vulnérabilité est celui dit des SCADA, acronyme de l'anglais *Supervisory Control And Data Acquisition* (télésurveillance et acquisition de données), très souvent utilisé dans l'industrie (énergie, eau, déchets). D'après l'*Open Source Vulnerability Database*, le nombre d'attaques sur des SCADA révélées serait en augmentation, ce que confirme un rapport de HP [19].

15. GORE Albert A., *op. cit.*, p. 77 : « *With so many Internet connected computerized devices now controlling water, and electric systems, power plants and refineries, transportation grids and other crucial systems, it is not difficult to conjure scenarios in which a coordinated attack on a nation's vital infrastructure could do real physical arms.* »

16. DUPONT Benoît, *op. cit.*

17. BENDIEK Annegret, *op. cit.*, p. 6.

18. WEST Darell M., *op. cit.*

19. HP (Hewlett-Packard), *HP2012 Cyber Risk Report*, 2012, accessible en ligne http://www.hpenterprisesecurity.com/collateral/whitepaper/HP2012CyberRiskReport_0313.pdf. Consulté le 4 juillet 2013.

3. Augmentation du nombre et de la diversité des attaquants potentiels

Les attaquants potentiels augmentent en nombre, avec d'un côté plus d'attaquants étatiques qui s'arment, et de l'autre plus de cyberterroristes, cybercriminels, individus isolés, cyberactivistes, cyberespions, etc. [20] Internet devient un champ d'attaque asymétrique avec la montée en puissance d'individus isolés mais compétents et capables d'attaques [21]. On peut aussi observer une complexification du champ avec des liens nouveaux entre les acteurs [22]. Une des tendances en 2012 est l'augmentation des intrusions perpétrées par des acteurs étatiques. La Chine, la Roumanie, les États-Unis et la Bulgarie seraient les États d'où proviendraient le plus d'attaques d'après le rapport Verizon 2013 [23].

4. Faible prise en compte par les individus et les entreprises des risques cyber

Les rapports analysés soulignent combien les individus et les entreprises tardent à prendre en compte l'ampleur de la menace cyber et des impacts potentiels. En conséquence, ils relèvent qu'il existe très peu de réflexes de protection, ce que l'on peut qualifier de mauvaise hygiène informatique (« *lousy cyber hygiene* ») [24]. Parmi les leviers qui permettent d'avoir plus de ressources pour la protection des données, l'étude de HP souligne le rôle important du régulateur. En effet, une étude conduite auprès des responsables de sécurité informatique montre que 61 % des personnes interrogées pensent que la régulation pourrait avoir un impact pour renforcer la protection des données détenues par l'organisation, soit une augmentation de 5 % par rapport à l'étude conduite l'année précédente.

5. Risque croissant de perte de contrôle sur les données

Les rapports identifient un risque croissant de perte de contrôle sur les données [25] en lien avec :

— le *cloud computing*,

— la montée en puissance d'intermédiaires privés de gestion des données,

— les croisements permis par le *big data* et les nouveaux algorithmes qui permettent de reconstituer des données par croisement,

— l'augmentation de l'Internet mobile très vulnérable (*smartphones* et tablettes),

— l'augmentation du paiement sans contact,

— la longueur des circuits de fabrication où certains composants d'espionnage peuvent être inclus avant la vente lors de la production ou la distribution.

---

20. HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.*

21. WEST Darell M., *op. cit.*

22. DEIBERT Ron, *op. cit.*

23. VERIZON RISK TEAM, *2013 Data Breach Investigations Report*, 2013. URL : http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf. Consulté le 5 juillet 2013.

24. WEST Darell M., *op. cit.*

25. DUPONT Benoît, *op. cit.* ; DEIBERT Ron, *op. cit.*

Parmi les solutions pour contrecarrer la tendance, les rapports mentionnent :

— réintroduire de la souveraineté (par exemple des *cloud* souverains) ;

— renforcer la « *privacy by design* », conception visant à intégrer la protection des données dès la conception des applications ;

— réinvestir dans le cryptage.

6. Risque croissant d'usurpation d'identité

En usurpant l'identité d'un cadre ou d'un directeur, certains accèdent à des données privées illégalement. En usurpant l'identité d'individus, des transactions non souhaitées par les propriétaires de compte peuvent avoir lieu. Selon A. Bendiek, qui s'appuie sur des rapports de police allemands, ce genre d'attaques a triplé au cours des deux dernières années [26].

7. Complexification des recours en justice

Nos sociétés sont de plus en plus dépendantes, pour leur bon fonctionnement, d'opérateurs, de systèmes ou de données qui ne sont pas toujours localisés sur leur sol, ou qui ne sont pas toujours sous le contrôle d'entreprises ou d'acteurs de leur territoire [27]. Cela peut rendre complexe la poursuite des responsables en cas de problème. Par ailleurs, le *cloud computing* et les difficultés de traçabilité qui sont liées aux réseaux [28] rendent complexes les recours en justice, même si les services en charge de la protection du secret dans les différents États montent en compétence sur le sujet en tentant de développer des outils pour réussir à savoir qui est l'attaquant [29]. L'Union européenne tente de développer des coopérations entre États pour permettre une meilleure cybersécurité par la justice [30]. Toutefois, une tendance lourde reste la complexification des modes d'attaque, brouillant les pistes d'identification des agresseurs à l'œuvre. Comme le souligne J.L. Granatstein, la plupart des attaques ciblées probablement perpétrées par des États ne sont pas attribuables à ce jour à un ennemi ou une source particulière. Par rapport à d'autres formes d'attaques traditionnelles, cela change la nature des modes de réponses possibles, qu'elles soient juridiques, diplomatiques ou militaires [31].

8. Déplacement démographique du cyberespace

Certains rapports mentionnent le déplacement démographique du cyberespace en lien avec l'accroissement du nombre d'utilisateurs dans les pays en voie de développement [32]. Ils soulignent la montée en puissance de l'Asie, et plus particulièrement de la Chine. Ces nouveaux utilisateurs n'ont pas les mêmes valeurs, les mêmes normes politiques. Il y aurait en conséquence un risque de « balkanisation » du Net et un risque croissant d'une

26. BENDIEK Annegret, *op. cit.*

27. CLEMENTE Dave, *Cyber Security and Global Interdependence: What Is Critical?*, Londres : Chatham House (The Royal Institute of International Affairs), février 2013, p. VIII.

28. DUPONT Benoît, *op. cit.*

29. WEST Darell M., *op. cit.*

30. BENDIEK Annegret, *op. cit.*

31. GRANATSTEIN J.L. (sous la dir. de), *The Canadian Forces in 2025: Prospects and Problems,* Victoria : Friesen Press, février 2013.

32. DEIBERT Ron, *op. cit.*

société du contrôle, par la censure pratiquée par certains pays non démocratiques et l'usage d'algorithmes prédictifs facilitant le traçage de comportements déviants.

Toutes ces tendances lourdes ne sont pas indépendantes les unes des autres, mais interagissent entre elles, voire se renforcent mutuellement. Il semble toutefois important de faire la différence entre d'une part une augmentation des attaques et de la vulnérabilité à tout-va, à petite échelle, par des virus, des *malwares* (par augmentation du nombre d'objets et de personnes connectés, etc.), et d'autre part le développement d'attaques précises de plus en plus ciblées ayant pour objet des intérêts vitaux, comme par exemple l'usage de Stuxnet en Iran pour stopper des centrifugeuses nucléaires. Ainsi, il ne faudrait pas déduire automatiquement de l'augmentation des connexions et du nombre d'objets connectés, une augmentation d'attaques de grande ampleur menaçant les intérêts vitaux de la nation.

Par ailleurs, il faut aussi distinguer ce qui est de l'ordre de l'attaque volontairement visible, pour nuire à l'image d'une organisation, par exemple en bloquant ou trafiquant ses pages Internet, et ce qui relève de l'attaque masquée à des fins d'espionnage, parfois non répertoriée dans l'inventaire des cyberattaques. Cette fois-ci, il existe un risque de minimiser des attaques importantes sur des intérêts économiques nationaux, par non-communication des entreprises affectées.

Il faut donc être prudent avec ces données qui mélangent parfois de petits et de grands risques, qui ne sont pas toujours transparentes sur le mode d'agrégation des données statistiques, entre autres.

Les ruptures identifiées

Les rapports identifient différentes ruptures à venir, d'ordre technologique, sociétal, politique, économique ou militaire.

1. Les ruptures technologiques

Les ruptures identifiées viennent avant tout des technologies. Cet argument est défendu d'autant plus que les évolutions technologiques numériques sont peu conditionnées par des contraintes financières, contrairement aux autres domaines plus intensifs en capitaux.

Des ruptures à court terme pourraient par exemple survenir en lien avec le développement du *cloud computing*. Comme le *cloud computing* est à ce jour considéré comme une forte vulnérabilité [33], de nouvelles technologies pourraient se développer pour détecter mais aussi répondre aux attaques sur le *cloud* [34]. Des projets seraient en cours d'expérimentation pour permettre le développement de détecteurs d'empreintes digitales pour tenter de cerner plus précisément qui commet l'attaque [35] . Cette possibilité est à relier à la forte augmentation des investissements dans la protection des réseaux. Selon IDC, 440 millions de dollars US étaient consacrés à financer la sécurité des réseaux au niveau mondial en 2011. En 2015, on devrait passer à 695 millions de dollars US [36].

33. GEORGIA TECH, *Emerging Cyber Threats Report 2013,* Atlanta : Georgia Institute of Technology, 2013.

34. KUNDRA Vivek, *Federal Cloud Computing Strategy,* Washington, D.C. : Maison Blanche, 2011.

35. SAALBACH Klaus-Peter, *Cyber War: Methods and Practice, version 6.0,* Osnabrück : université d'Osnabrück, 2 janvier 2013 ; et BLAKELY Benjamin A., *Cyberprints: Identifying Cyber Attackers by Feature Analysis,* Ames : Iowa State University, 2012.

36. KOLODGY Charles, « Server Security for Today's Datacenters », *IDC Analyst Connection*, février 2012.

Les exemples de ruptures à moyen et long termes mentionnés dans les rapports sont : les capacités de mesure de l'activité cérébrale pour retracer ce que pense un cerveau, les capacités à développer des interfaces neuronales entre humains et non-humains (« *human cybernetic interfaces* ») [37]. Cela pourrait donner lieu à des technologies visant à détecter la vérité, accéder à des souvenirs, voire à pirater des cerveaux humains. Un autre exemple presque toujours cité est celui de l'informatique quantique, qui pourrait changer le monde de la cryptologie notamment [38].

Les rapports soulignent en outre que des ruptures technologiques sont susceptibles d'émerger à l'interface entre des nouveaux développements informatiques et des nouveaux développements dans d'autres domaines jusqu'alors évoluant en parallèle, comme par exemple celui des nanotechnologies [39].

2. Les ruptures dans les usages sociaux

Les ruptures identifiées concernent aussi les usages sociaux des technologies de l'information et de la communication. Les usagers peuvent trouver des applications non anticipées à des avancées numériques. Les exemples de ruptures par les usages sont nombreux dans l'espace cyber. Les rapports mentionnent l'exemple du printemps arabe, largement basé sur l'usage des réseaux sociaux. Un autre exemple donné est celui de l'*open data*, qui remet en cause les modèles actuels payants d'accès à des bases de données. Enfin, le développement de réseaux de pirates informatiques donnant lieu à des fuites de documents (« *leaks* ») est aussi cité. Quelles ruptures dans les usages pourraient donc survenir ? Peu de rapports s'attaquent à la question. Selon *The Future,* d'Al Gore [40], on pourrait voir émerger des segmentations dans la population en fonction des usages numériques :

— entre ceux qui valorisent en priorité la liberté et ceux qui valorisent en priorité le contrôle sur leur vie et leurs réseaux à des fins de sécurité ;

— entre les individus qui partagent librement de l'information sur les réseaux sociaux et ceux qui évitent de le faire par peur d'agrégation de leurs données ;

— entre les acteurs sociaux qui ne suivent pas le rythme des évolutions cyber et ceux qui se positionnent en *leaders* sur les outils émergents ;

— entre des acteurs qui tireront leur revenu du secret et ceux qui tireront le leur de l'accès massif à des données.

Ce sont avant tout les possibilités d'auto-organisation permises par le développement de l'*open data*, des logiciels libres, etc., qui rendent les ruptures dans les usages sociaux nombreuses.

3. Les ruptures politiques

Des ruptures politiques majeures pourraient émerger si les tensions s'exacerbaient entre les nouveaux pays à forte démographie cyber, où les régimes cherchent à contrôler l'Internet (exemple : la Chine), et les anciens pays à l'origine du *Web* (exemple : les États-Unis), qui veulent garantir l'accès au réseau sans pour autant censurer les contenus du

37. GRANATSTEIN J.L. (sous la dir. de), *op. cit.*

38. GORE Albert A., *op. cit.*

39. DUTTA Soumitra et BILBAO-OSORIO Beñat (sous la dir. de), *op. cit.*

40. GORE Albert A., *op. cit.*

Web [41]. Les rapports donnent l'exemple de l'Organisation de coopération de Shanghai [42] et de l'opposition vive qui existe entre d'un côté la Chine et la Russie, et de l'autre les États-Unis et l'Europe [43]. Des tentatives existent de nouvelles structures diplomatiques informelles entre la Chine et les États-Unis pour aider au déblocage de la situation, mais les avancées sont à ce jour suffisamment difficiles pour que des risques de rupture politique soient mentionnés dans les rapports [44].

Des ruptures politiques pourraient aussi avoir lieu si des personnes révèlent par des attaques cyber d'espionnage que certains pays ont développé des capacités offensives dans le cyberespace et s'il peut être avéré par fuites qu'ils s'en sont servi ou planifiaient de le faire. Ron Deibert évoque l'exemple de la chute du président Moubarak qui a permis à des opposants de révéler que l'Égypte avait un contrat avec une entreprise britannique pour des services de cyberoffensives [45].

On peut aussi citer ici la récente polémique autour du programme *Prism* des États-Unis, permettant l'espionnage des données échangées par Internet.

4. Les ruptures économiques

Parmi les éléments de rupture, les rapports mentionnent la mise au point d'un marché mondial de la cyberoffensive ou du cyberespionnage, avec la mise en place d'entreprises qui vendraient des services de défense et d'attaque cyber au plus offrant. Cela pourrait, pas à pas, éroder la neutralité de l'Internet et faire basculer l'intelligence économique à la limite de la légalité [46]. En conséquence, les agents économiques doivent être de plus en plus résilients, adaptables, flexibles, pour faire face [47].

5. Les ruptures militaires

Des ruptures pourraient voir le jour sur les champs de bataille physiques, avec des changements dans l'interface cybernétique, une plus grande robotisation et des liens homme-machine renforcés [48]. Comme l'indique J.L. Granatstein : « On peut imaginer qu'à moyen terme, on puisse envisager des avions sans pilote, avec un centre de commande et de contrôle totalement externe [49]. » Une autre rupture pourrait venir de la plus grande synchronisation des moyens et des hommes par l'interface cybernétique, grâce à des progrès dans les outils de géolocalisation, de *geotagging* et des systèmes d'information géographique [50].

---

41. BENDIEK Annegret, *op. cit.*

42. DEIBERT Ron, *op. cit.*

43. AHRENS Nathaniel, *National Security and China's Information Security Standards: Of Shoes, Buttons, and Routers. A Report of the CSIS Hills Program on Gouvernance*, Washington, D.C. : Center for Strategic and International Studies (CSIS), novembre 2012.

44. LIEBERTHAL Kenneth et SINGER Peter W., *Cybersecurity and U.S.-China Relations*, Washington, D.C. : The Brookings Institution (China Center), février 2012.

45. DEIBERT Ron, *op. cit.*, p. 14.

46. *Ibidem*.

47. CLEMENTE Dave, *op. cit.*, p. VIII.

48. GRANATSTEIN J.L. (sous la dir. de), *op. cit.*

49. GRANATSTEIN J.L. (sous la dir. de), *op. cit.*, emplacement 812 sur *Kindle* : « *One can imagine that mid-life modernisation of existing platforms might include the removal of the pilote from the cockpit to the safety of a command and control centre.* »

50. *Ibidem*, emplacement 970 sur *Kindle*.

Un nouveau champ de bataille cyber pourrait voir le jour, et avec lui un nouveau corps d'armée dédié à la cybersécurité. J.L. Granatstein estime que cette rupture organisationnelle, avec la création d'une structure dédiée au cyber, est probable à l'horizon 2025 [51]. En effet, certains pays comme l'Iran ou la Corée du Nord pourraient voir, dans le développement d'armes cyber, une façon de pouvoir conduire la guerre ou dissuader à moindre coût [52]. J.L. Granatstein souligne que lors d'attaques ciblées perpétrées par des États, il est difficile de pouvoir répondre par des voies classiques (antivirus, *firewall*, etc.). Il devient donc nécessaire d'avoir une entité dédiée au cyber. Ron Deibert va jusqu'à parler d'un risque croissant de cyberguerre [53].

L'identification de cette rupture donne lieu à une importante littérature en cyberstratégie, pour envisager comment adapter les stratégies militaires à un nouveau domaine, celui du cyberespace, et mieux comprendre les éléments offensifs et défensifs qui pourraient être mis en œuvre (tableau 2).

Cela donne aussi lieu à de la littérature sur les adaptations organisationnelles à prévoir. J.L. Granatstein propose, pour les forces canadiennes, trois adaptations au cyber d'ici 2025 : la mise en place d'une force régulière, dédiée au cyberespace. La constitution d'un groupe de forces spéciales du cyber qui pourraient anticiper les attaques à venir en s'appuyant sur une approche basée sur la menace, par analogie avec ce qui existe pour les attaques radiologiques, biologiques ou chimiques. Cette force spéciale pourrait aussi être utilisée pour répondre aux attaques. Enfin, un dernier groupe est identifié comme crucial à l'avenir : celui des ingénieurs de soutien. Ils travailleraient dès la conception des systèmes à leur protection et leur sécurité.

Les recommandations effectuées

Il n'existe pas de consensus pour savoir qui doit garantir quelle sécurité, où doivent être les garde-fous : au niveau international, national, au niveau des entreprises ? La question du degré de privatisation de la cybersécurité reste ouverte. Certains points ressortent toutefois en termes de recommandations :

- **Avoir une philosophie, une éthique de base** qui serve de cadrage à la stratégie cyber [54].

- **Développer des outils de veille**, car l'environnement stratégique cyber évolue très vite. Il s'agit de pouvoir anticiper et de ne pas être surpris. Une combinaison de veille en temps réel et d'approches systémiques est nécessaire pour ne pas passer à côté de signaux faibles. Or, la veille est rendue difficile car des cas d'attaques sur des entreprises privées peuvent rester inconnus des services, les entreprises ne souhaitant pas toujours révéler des failles [55].

- **Harmoniser le droit** pour pouvoir rétorquer sans être piégé par des décalages transnationaux. Un des défis d'avenir est de savoir comment sortir des juridictions nationales

51. *Ibidem*, emplacement 859 sur *Kindle*.

52. BENNY Lim, *Future Stake*, Singapour : RAHS (Risk Assessment and Horizon Scanning) Think Centre, 2012.

53. DEIBERT Ron, *op. cit.*, p. 13.

54. DEIBERT Ron, *op. cit.*

55. *Ibidem* ; DUPONT Benoît, *op. cit.*

Tableau 2 — Cybercapacités offensives et défensives selon RAHS		
	Offensive	**Defensive**
Scanning **Identifying vulnerabilities**	Deep web scanning Open source scanning Port and address scanning Social media scanning Vulnerability scanning	Clean metadata Encryption Port relocation Proxies Reduce information
Penetration/Escalation **Compromising and accessing systems**	Brute force cracking Malware/backdoors Phishing/pharming Physical tempering Public exploits Social engineering Zero day exploits	Antivirus/anti-malware Intrusion detection systems Intrusion prevention systems Least privilege policy Penetration testing Regular software patching Strong password policies System hardening Vulnerability assessment
Surveillance **Monitoring data and communications**	Key logging/Screen grabbing Packet sniffing/interception System fingerprinting Wiretapping/eavesdropping	Encryption Hardware shielding Traffic monitoring
Exfiltration **Extracting and sending information**	Analogue exfiltration Network exfiltration Physical exfiltration	Employee screening Restricting physical access System hardening Traffic monitoring
Obfuscation **Disguising and hiding an attack**	File manipulation IP address spoofing Log manipulation Proxy routing Virtual private networks (VPN)	Backup logging File monitoring
Access **Opening a system to attack**	Custom malware Zero day exploits	Defence in depth Intrusion detection systems Intrusion prevention systems
Disrupt **Degrading and disrupting systems**	Denial of service (DOS) Network disconnection Physical sabotage System degradation	Disaster recovery planning Electronic countermeasures Firewall/router/server rules Redundancy/over-provisioning
Damage **Physical or logical damage to systems**	Control system failure Control system manipulation Physical sabotage System/database damage	Air-grapping critical systems Electronic countermeasures Redundancy/over-provisioning System hardening
Source : BENNY Lim, *op. cit.,* p. 20-21.		

quand cela est nécessaire. Pour cela, l'Union européenne offre un exemple, avec la mise en place de *standards* communs qui doivent permettre d'améliorer la prévention, la résilience, la coopération entre États [56].

56. BENDIEK Annegret, *op. cit.* ; DUPONT Benoît, *op. cit.*

◗ **Créer des instances de coordination gouvernementale** afin d'éviter des concurrences entre services pour les ressources, et d'avoir une approche globale et cohérente des risques [57].

◗ **Développer des capacités au niveau local** pour avoir des modes de réponse rapides, flexibles au plus près du terrain [58].

◗ **Renforcer les partenariats public / privé**, surtout dans le domaine de la cyberdéfense. La question de la confiance entre acteurs publics et privés sur les questions de sécurité est présentée, dans les travaux analysés, comme un élément clef de succès pour lutter contre les cybermenaces. Le *Common Assurance Maturity Model* (CAMM) et la *Cloud Security Alliance (*CSA) sont cités comme des exemples de bonnes pratiques dans ce domaine [59].

◗ **Intensifier les recherches** pour se garantir une avance technologique [60].

◗ **Redéfinir le rôle des services secrets et de l'espionnage :** « La cybersécurité touche à un domaine qui est traditionnellement très sensible : celui de la surveillance électronique autrement appelé le renseignement [...] Les agences de renseignement jouent aujourd'hui un rôle de plus en plus important avec la prise en compte des questions de cybersécurité comme enjeux de sécurité nationale [61]. » Quelle place donner alors au secret et à ces services ?

◗ **Faire attention lors de l'achat de matériel** (*procurement policy and supply chain*) [62]. Certains rapports vont jusqu'à proposer la mise en place d'un système de management global dans la chaîne d'approvisionnement (*global supply chain management*) [63].

◗ **Investir en ressources humaines** pour avoir les meilleurs « cerveaux » et éviter une fuite (*brain drain*) des talents numériques [64].

◗ **Savoir dans quels cas de cyberattaque rétorquer** militairement, et comment l'armée peut aider les civils en cas d'attaques massives : avoir une doctrine prête en amont [65].

◗ Ne pas avoir l'objectif de tout sécuriser mais **bien hiérarchiser les priorités** selon la sensibilité des données et des fonctions [66].

◗ **Renforcer les relations entre alliés** sur les questions cyber, notamment à travers l'OTAN ou l'Union européenne [67].

◗ **Éduquer les populations** [68]. Une première cible de population à éduquer en priorité est celle des cadres du privé et du public qui manient des données stratégiques. Ils doivent

---

57. CLEMENTE Dave, *op. cit.*, p. IX.
58. DUPONT Benoît, *op. cit.*
59. GRAUMAN Brigid, *op. cit.*
60. DUPONT Benoît, *op. cit.*
61. DEIBERT Ron, *op. cit.* : « *Cyber security touches upon what is traditionally one of the most sensitive areas of national security: electronic surveillance, otherwise known as signal intelligence. [...] These agencies are now taking on a more expansive role as cyber security becomes a more vital issue to national security.* »
62. HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.*
63. GEORGIA TECH, *op. cit.*
64. HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.*
65. GRANATSTEIN J.L. (sous la dir. de), *op. cit.*
66. GRAUMAN Brigid, *op. cit.*
67. HOUSE OF COMMONS DEFENCE COMMITTEE, *op. cit.*
68. GRAUMAN Brigid, *op. cit.* ; KAY David J., PUDAS Terry J. et YOUNG Brett. « Preparing the Pipeline: The US Cyber Workforce for the Future », *Defense Horizons*, n° 72, août 2012 ; GEORGIA TECH, *op. cit.*

avoir bénéficié d'une formation initiale ainsi que d'une formation continue pour être au courant de l'évolution des risques en temps réel. Un deuxième cercle plus large est celui des populations en général, qui doivent elles aussi être sensibilisées dans leur quotidien aux risques du cyberespace.

- **Développer un code de conduite international** (« *a global code of conduct* ») [69] qui servirait de base à la régulation de l'espace cyber et à des actions diplomatiques.

Conclusion

Points clefs des rapports étudiés

Les rapports étudiés posent une série de questions clefs : que faut-il protéger ? Qu'est-ce qui relève du domaine de la sécurité ? Qu'est-ce qui doit être rendu public ou rester de l'ordre du secret ? Que peut-on considérer comme une vraie menace ou comme relevant simplement de la petite attaque de tous les jours ?

Il est possible de tout faire entrer dans le domaine de la cybersécurité, de la protection et du secret, dans un scénario où tous les objets connectés pourraient devenir des armes, tous les acteurs potentiels devenir des cibles ou des attaquants, toutes les données personnelles permettre, une fois combinées, de manipuler des individus à leurs dépens. Il est tout aussi possible d'opter pour un scénario d'ouverture, en limitant le plus possible le fort degré de sécurité à des données ultrasensibles, en évitant le phénomène de tabou qui entoure les cyberattaques que subissent les entreprises, pour former des citoyens responsables ayant conscience des menaces tout en maîtrisant les outils et leur hygiène informatiques. Derrière ce questionnement et ces scénarios, il y a des enjeux juridiques, des choix de société, des modèles économiques, des valeurs et une éthique, des politiques étrangères et des stratégies militaires très différentes. La prospective exploratoire proposée dans ces rapports doit donc permettre la mise en place de prospectives plus normatives, où chaque État pourrait préciser sa vision du futur souhaitable en matière de cybersécurité. L'enjeu est alors de trouver le bon équilibre entre liberté démocratique et contrôle de sécurité, entre ouverture et fermeture / secret, comme le soulignent R. Deibert et A. Bendiek dans leurs travaux respectifs.

Éléments sous-estimés dans les rapports étudiés

Face aux documents analysés, plusieurs éléments semblent sous-estimés, par rapport aux sujets considérés dans les publications françaises récentes. Par exemple, aucune voie alternative au clivage États-Unis / Chine ne semble prise en considération dans les analyses proposées. Or, il est possible de citer le rapport de la sénatrice française Catherine Morin-Desailly, intitulé *L'Union européenne, colonie du monde numérique ?* [70], qui lui a le mérite d'envisager une « troisième voie pour la gouvernance Internet », afin « d'éviter que ne se creuse le clivage entre les États-Unis et la Chine en rendant plus transparent le fonctionnement de l'ICANN [Internet Corporation for Assigned Names and Numbers] et en reva-

69. BENDIEK Annegret, *op. cit.*

70. MORIN-DESAILLY Catherine, *Rapport d'information fait au nom de la Commission des affaires européennes sur l'Union européenne, colonie du monde numérique ?*, Paris : Sénat, 20 mars 2013. URL : http://www.senat.fr/rap/r12-443/r12-4431.pdf. Consulté le 5 juillet 2013.

lorisant en même temps le rôle des gouvernements pour la défense d'une forme d'ordre public sur Internet [71] ».

Par ailleurs, les réflexions autour du marché de la cybersécurité sont également peu présentes, alors que les acteurs privés sont déterminants sur le sujet. Il est désormais consensuel que « la construction d'un marché européen de la cybersécurité est en marche » et « pourrait bien être l'une des premières étapes pour combattre les pirates informatiques » [72]. Le rapport *L'Union européenne, colonie du monde numérique ?* identifie par exemple la question économique et industrielle comme étant un défi majeur. Ainsi « le numérique ne doit pas être considéré comme un simple secteur industriel mais comme un "facteur de renversement des modèles d'affaires existants" et un levier de croissance qui imprègne progressivement l'ensemble des secteurs [73] ». Ce rapport a l'originalité de poser des questions du point de vue de la « fiscalité numérique » [74]. Notion également rappelée dans la feuille de route numérique du gouvernement français qui envisageait de « renforcer la compétitivité de[s] entreprises [françaises] grâce au numérique », notamment grâce à la sécurité des systèmes informatiques [75]. Un autre rapport [76], plus récent, issu d'une étude confiée à des enseignants chercheurs de Télécom ParisTech et à des membres de la Fondation Internet nouvelle génération (FING), par le Commissariat général à la stratégie et à la prospective, analyse l'évolution d'Internet à l'horizon 2030. La première des recommandations est de « soutenir la réindustrialisation de l'Europe dans le numérique, en identifiant les plates-formes émergentes liées à l'Internet des objets et à la robotique, et en accompagnant leur développement industriel à l'échelle européenne ». Cette vision est confirmée par les récentes annonces de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) [77] quant aux futures initiatives visant à stimuler le marché de la cybersécurité, notamment par l'obligation faite aux opérateurs d'infrastructures vitales d'installer des sondes de détection d'intrusion informatique ; outils opérés par des Européens sur le territoire européen.

Enfin, la problématique de l'identité numérique qui est au cœur des discussions actuellement, reste peu mentionnée dans les rapports étudiés. Or, le Secrétariat général pour la modernisation de l'action publique (SGMAP) a récemment lancé une consultation sur l'identité numérique [78]. Cette initiative aborde un sujet qui mérite que l'on s'y attarde dans les prochaines années, alors même que les rapports étudiés ici ne le mentionnent que très peu.

---

71. Voir TISSIER Guillaume, « L'Europe, colonie du monde numérique ? », Lille : 5e Forum international de la cybersécurité, 28-29 janvier 2013. URL : http://fic2013.com/leurope-colonie-du-monde-numerique-par-guillaume-tissier-ceis/. Consulté le 5 juillet 2013.

72. Voir le numéro spécial « Cybersécurité », *Global Security Mag*, n° 23, avril-juin 2013.

73. Voir TISSIER Guillaume, *op. cit.*

74. MORIN-DESAILLY Catherine, *op. cit.*

75. Voir TISSIER Guillaume, *op. cit.*

76. GILLE Laurent et MARCHANDISE Jacques-François, *La Dynamique d'Internet. Prospective 2030*, Paris : Commissariat général à la stratégie et à la prospective, mai 2013.

77. Voir « Livre blanc et cybersécurité des OIV : point sur les chantiers législatifs en cours », *Secu(Insight).fr*, 18 juin 2013. URL : http://www.secuinsight.fr/2013/06/18/livre-blanc-et-cybersecurite-des-oiv-point-sur-les-chantiers-legislatifs-en-cours/. Consulté le 5 juillet 2013.

78. Voir *Identité(s) numérique(s). Quelle stratégie pour l'État ? Point de vue initial soumis à la consultation*, Paris : SGMAP, mai 2013. URL : http://www.modernisation.gouv.fr/fileadmin/Mes_fichiers/pdf/300413_IdentiteNumerique.pdf. Consulté le 5 juillet 2013.

Éléments non considérés dans les rapports étudiés

Parmi les manques identifiés dans les rapports prospectifs étudiés figure l'absence de prise en compte de la cybercrise en tant que telle. En cas d'attaques coordonnées et massives, coupant les centres de crise existants de leurs outils informatiques habituels, quels sont les scénarios pour permettre de maintenir la sécurité, la conduite d'activité, l'État, etc. ? Cela n'est pas évoqué. Un autre manque identifié est celui de la communication de crise en cas d'attaques cyber massives. Comment inclure les populations, que communiquer ou taire ? Enfin, on ne trouve pas non plus la question de l'évaluation de la gradation de la cybermenace avec différents échelons de réponses proportionnelles et appropriées. Or, on aurait pu penser que la prospective exploratoire permettrait de mieux cerner ces enjeux de gradation et d'intensité dans les attaques, sans tout mettre nécessairement sur le même plan.

Une des limites vient enfin du fait que tous les rapports étudiés émanent de pays de l'Ouest, pays partageant une certaine vision commune de l'Internet et de la cybersécurité. Il serait intéressant de pouvoir accéder à des rapports similaires mais produits par la Chine, par exemple, pour voir en quoi les visions des menaces et de l'avenir peuvent différer en la matière.

Au-delà de cette note

Il serait enfin intéressant de croiser les éléments analysés dans ce rapport basé sur sources ouvertes uniquement, avec ceux que peuvent compiler les services travaillant sur sources fermées, confidentielles ou classifiées, pour voir si les mêmes analyses prospectives des risques et des vulnérabilités se dégagent ou bien si, au contraire, leurs visions des enjeux stratégiques diffèrent. ■

Bibliographie

AHRENS Nathaniel, *National Security and China's Information Security Standards: Of Shoes, Buttons, and Routers. A Report of the CSIS Hills Program on Gouvernance*, Washington, D.C. : Center for Strategic and International Studies (CSIS), novembre 2012, 28 p. URL : http://csis.org/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf. Consulté le 5 juillet 2013.

ARMSTRONG Illena, « Guarding Against a Data Breach », *SC Magazine*, janvier 2012, p. 27-33, Hewlett-Packard (HP). URL : http://www.hpenterprisesecurity.com/collateral/report/SC%20Magazine%202012%20Guarding%20Against%20A%20Data%20Breach%20Survey.pdf. Consulté le 5 juillet 2013.

BENDIEK Annegret, *European Cyber Security Policy*, Berlin : Stiftung Wissenschaft und Politik (SWP, German Institute for International and Security Affairs), *SWP Research Paper,* octobre 2012, 27 p. URL : http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf. Consulté le 5 juillet 2013.

BENNY Lim, *Future Stake*, Singapour : RAHS (Risk Assessment and Horizon Scanning) Think Centre, 2012. URL : http://app.rahs.gov.sg/public/www/content.aspx?sid=2950. Consulté le 5 juillet 2013.

BLAKELY Benjamin A., *Cyberprints: Identifying Cyber Attackers by Feature Analysis,* Ames : Iowa State University, 2012, 144 p. URL : http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3287&context=etd. Consulté le 5 juillet 2013.

CLEMENTE Dave, *Cyber Security and Global Interdependence: What Is Critical?*, Londres : Chatham House (The Royal Institute of International Affairs), février 2013, 46 p. URL : http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf. Consulté le 5 juillet 2013.

DEIBERT Ron, *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace,* Calgary : Canadian Defence & Foreign Affairs Institute (CDFAI), août 2012, 28 p. URL : http://www.cdfai.org/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf. Consulté le 5 juillet 2013.

DUPONT Benoît, *L'Environnement de la cybersécurité à l'horizon 2022. Tendances, moteurs et implications*, Montréal : Chaire de recherche du Canada en sécurité et technologie, université de Montréal, Note de recherche n° 14, septembre 2012, 47 p. URL : http://www.cerium.ca/IMG/pdf/Dupont_2012_Cybersecurite_2022_note_14.pdf. Consulté le 5 juillet 2013.

DUTTA Soumitra et BILBAO-OSORIO Beñat (sous la dir. de), *The Global InformationTechnology Report 2012: Living in a Hyperconnected World,* Genève : World Economic Forum, 2012, 441 p. URL : http://www3.weforum.org/docs/Global_IT_Report_2012.pdf. Consulté le 5 juillet 2013.

GEORGIA TECH, *Emerging Cyber Threats Report 2013*, Atlanta : Georgia Institute of Technology, 2013, 9 p. URL : http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf. Consulté le 5 juillet 2013.

GILLE Laurent et MARCHANDISE Jacques-François, *La Dynamique d'Internet. Prospective 2030*, Paris : Commissariat général à la stratégie et à la prospective, mai 2013, 208 p. URL : http://www.strategie.gouv.fr/system/files/etude_internet_2030-web.pdf. Consulté le 5 juillet 2013.

GORE Albert A., *The Future: Six Drivers of Global Change*, New York : Random House, janvier 2013, 192 p.

GRANATSTEIN J.L. (sous la dir. de), *The Canadian Forces in 2025: Prospects and Problems*, Victoria : Friesen Press, février 2013, 97 p. URL : http://www.friesenpress.com/bookstore/title/119734000010394648. Consulté le 5 juillet 2013.

GRAUMAN Brigid, *Cyber-security: The Vexed Question of Global Rules. An Independent Report on Cyber-preparedness around the World,* Bruxelles : Security & Defence Agenda's (SDA), 2012, 108 p.

URL : http://fr.scribd.com/doc/80154379/SDA-Cyber-Security-The-Vexed-Question-of-Global-Rules. Consulté le 5 juillet 2013.

HP (Hewlett-Packard), *HP2012 Cyber Risk Report,* 2012, 23 p. URL : http://www.hpenterprisesecurity.com/collateral/whitepaper/HP2012CyberRiskReport_0313.pdf. Consulté le 4 juillet 2013.

HOUSE OF COMMONS DEFENCE COMMITTEE, *Defence and Cyber-Security: Sixth Report of Session 2012-13,* vol. 1 « Report, together with formal minutes, oral and written evidence », Londres : The Stationery Office, janvier 2013, 99 p. URL : http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf. Consulté le 5 juillet 2013.

KAY David J., PUDAS Terry J. et YOUNG Brett. « Preparing the Pipeline: The US Cyber Workforce for the Future », *Defense Horizons*, n° 72, août 2012, 16 p. URL : http://www.ndu.edu/CTNSP/docUploaded/DH 72 for web.pdf. Consulté le 5 juillet 2013.

KOLODGY Charles, « Server Security for Today's Datacenters », *IDC Analyst Connection,* février 2012, 4 p. URL : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_idc-server-sec_120203us.pdf. Consulté le 5 juillet 2013.

LIEBERTHAL Kenneth et SINGER Peter W., *Cybersecurity and U.S.-China Relations*, Washington, D.C. : The Brookings Institution (China Center), février 2012, 52 p. URL : http://www.brookings.edu/~/media/research/files/papers/2012/2/23-cybersecurity-china-us-singer-lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english. Consulté le 5 juillet 2013.

MORIN-DESAILLY Catherine, *Rapport d'information fait au nom de la Commission des affaires européennes sur l'Union européenne, colonie du monde numérique ?,* Paris : Sénat, 20 mars 2013, 158 p. URL : http://www.senat.fr/rap/r12-443/r12-4431.pdf. Consulté le 5 juillet 2013.

SAALBACH Klaus-Peter, *Cyber War: Methods and Practice, version 6.0,* Osnabrück : université d'Osnabrück, 2 janvier 2013, 54 p. URL : http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf. Consulté le 5 juillet 2013.

SGMAP (Secrétariat général pour la modernisation de l'action publique), *Identité(s) numérique(s). Quelle stratégie pour l'État ? Point de vue initial soumis à la consultation*, Paris : SGMAP, mai 2013. URL : http://www.modernisation.gouv.fr/fileadmin/Mes_fichiers/pdf/300413_IdentiteNumerique.pdf. Consulté le 5 juillet 2013.

TISSIER Guillaume, « L'Europe, colonie du monde numérique ? », Lille : 5e Forum international de la cybersécurité, 28-29 janvier 2013. URL : http://fic2013.com/leurope-colonie-du-monde-numerique-par-guillaume-tissier-ceis/. Consulté le 5 juillet 2013.

UIT (Union internationale des télécommunications), *Trends in Telecommunication Reform 2013: Transnational Aspects of Regulation in a Networked Society,* Genève : UIT, avril 2013, 28 p. URL : http://www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.14-2013-SUM-PDF-E.pdf. Consulté le 5 juillet 2013.

VERIZON RISK TEAM, *2013 Data Breach Investigations Report,* 2013, 63 p. URL : http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf. Consulté le 5 juillet 2013.

WEST Darell M., *A Vision for Homeland Security in the Year 2025,* Washington, D.C. : Brookings Institution, *Governance Studies*, juin 2012, 16 p. URL : http://www.brookings.edu/~/media/Research/Files/Papers/2012/6/26 security homeland west/26_homeland_security_west.pdf. Consulté le 5 juillet 2013.

WEF (World Economic Forum), *Global Risks 2013: Eighth Edition. An Initiative of The Risk Response Network,* Genève : WEF, 2013, 80 p. URL : http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf. Consulté le 5 juillet 2013.

Conformément au cadre fixé dans l'Observatoire de la prospective internationale de défense, les publications antérieures à 2012 ne sont pas incluses dans cette bibliographie.

Pourquoi un Observatoire de la prospective internationale de défense ?

À l'image des rapports de prospective géostratégique et géopolitique réalisés par la Délégation aux affaires stratégiques (DAS) au cours des dernières années, nombre de ministères de la Défense étrangers élaborent et publient des analyses de référence à caractère prospectif et géostratégique. Concentrées jusqu'à présent dans les pays anglo-saxons, ces approches ont connu un relatif essor au cours des dernières années au sein d'autres pays occidentaux et émergents.

Au-delà de cette approche institutionnelle, les acteurs privés (instituts de recherche) et publics (universités, etc.) produisent régulièrement, par eux-mêmes, un corpus de travaux prospectifs intéressant directement ou indirectement la défense. Ils représentent une source ouverte d'information dense et de qualité, dont les points de convergence avec les travaux institutionnels peuvent être par ailleurs importants.

Pour identifier ces travaux, la DAS a créé un observatoire en charge du suivi des études internationales de nature prospective intéressant la défense à un horizon de 10 à 30 ans. Cet observatoire donne lieu à une veille sur les travaux de prospective issus de neuf pays (Afrique du Sud, Allemagne, Australie, Brésil, Canada, Chine, États-Unis, Inde, Royaume-Uni). Des rapports trimestriels rendent compte des principaux documents identifiés ; certains d'entre eux font l'objet d'une analyse plus approfondie. Six notes d'analyse thématiques annuelles complètent les travaux de l'observatoire.

La création et les activités de cet observatoire ont été confiées à un consortium réunissant la Compagnie européenne d'intelligence stratégique (CEIS), l'Institut de relations internationales et stratégiques (IRIS) et Futuribles.

Qu'est-ce que la prospective ?

Démarche d'anticipation, la prospective n'a pas pour autant comme ambition de prédire l'avenir. Elle se fixe en revanche comme objectif d'étudier avec rigueur les futurs possibles en germe dans la situation actuelle. Cette prospective dite exploratoire est le plus souvent développée comme instrument d'aide à la décision.

Le terme « prospective » peut recouvrir différentes pratiques qui vont de l'exploration se voulant la plus objective possible des futurs envisageables, à l'expression de visions plus ou moins structurées et argumentées. Quelle que soit leur méthodologie, les démarches prospectives dont il est rendu compte dans le cadre de cet observatoire ont pour ambition de servir ou d'orienter les politiques publiques des États, ou les stratégies des acteurs non étatiques.

Les notes d'analyse de l'Observatoire de de la prospective internationale de défense sont publiées par la Délégation aux affaires stratégiques (DAS).

Comité de rédaction : Matthieu Anquez (CEIS), Robert Chaouad (IRIS), François de Jouvenel (Futuribles) et Jean-Pierre Maulny (IRIS)

Conception graphique et secrétariat de rédaction : Stéphanie Debruyne (Futuribles)

Informations - contact : Nicolas Bronard, DAS, ministère français de la Défense
E-mail nicolas.bronard@defense.gouv.fr