2012

L'environnement de la cybersécurité à l'horizon 2022
Tendances, moteurs et implications

Note de recherche no. 14

Benoit Dupont

La Chaire de recherche du Canada en sécurité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers. Elle collabore pour cela avec des organismes gouvernementaux et des entreprises.

Prof. Benoit Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada

benoit.dupont@umontreal.ca
www.benoitdupont.net

Préparé pour

La Direction Générale de la Cybersécurité Nationale
Sécurité Publique Canada

Sommaire exécutif

En octobre 2010, le Gouvernement du Canada publiait sa stratégie de cybersécurité, prenant acte de l'omniprésence des infrastructures numériques, ainsi que des nouvelles vulnérabilités qui accompagnent cette évolution technologique. En raison des innovations constantes qui caractérisent le secteur numérique, et afin d'y répondre de manière appropriée, toute stratégie de cybersécurité doit s'accompagner d'un exercice de prospective visant à anticiper les tendances technologiques, culturelles et criminelles émergentes.

Ce rapport identifie neuf tendances technologiques émergentes à partir de 21 documents de prospective technologique publiés par des entreprises spécialisées et des organismes publics. Ces tendances regroupent des technologies ayant le potentiel de transformer durablement l'écosystème numérique, que nous définissons comme l'ensemble des infrastructures, des applications logicielles, des contenus et des pratiques sociales qui en déterminent les modes d'utilisation. La notion d'écosystème nous permet d'examiner de manière intégrée les interactions entre les dimensions technique, économique, sociale, politique et juridique de cet assemblage complexe.

Ces neuf tendances sont:

1. L'informatique dans les nuages
2. La massification des données
3. L'internet des objets
4. L'internet mobile
5. Les interfaces neuronales directes
6. Les paiements sans contact
7. La robotique mobile
8. L'informatique quantique
9. La militarisation de l'internet

L'analyse des caractéristiques et des moteurs de développement de chacune des neuf tendances a été effectuée à l'aide d'une recension de la littérature scientifique et du contenu de sites internet spécialisés dans les nouvelles technologies. Le degré de maturité et de diffusion parmi les utilisateurs professionnels et le grand public varient fortement d'une tendance à l'autre. Si l'informatique dans les nuages ou l'internet mobile font déjà partie de notre quotidien de consommateurs, l'informatique quantique reste encore à un stade de développement théorique embryonnaire et la mise sur le marché d'applications pratiques ne se fera pas avant au moins une dizaine d'années. En ce qui concerne les moteurs de développement, plusieurs catégories distinctes ont été identifiées, notamment les moteurs scientifiques, industriels, économiques, sociaux, juridiques et stratégiques. Finalement, chaque tendance a fait l'objet d'une analyse de ses implications pour la cybersécurité. Parmi les implications qui apparaissent le plus fréquemment, figurent la multiplication des opportunités d'attaques malveillantes, l'absence de prise en compte des besoins de sécurité lors du développement des technologies concernées, même lorsque ces dernières sont utilisées pour effectuer des

transactions financières, la dilution des mécanismes de contrôle de l'intégrité des systèmes, due à l'interconnexion toujours plus poussée des machines, ou encore l'érosion de la vie privée des utilisateurs, dont les informations personnelles représentent pour les organisations une source irrésistible de valeur ajoutée.

Quelques thématiques transversales aux neuf tendances sont également abordées en conclusion. Il s'agit de l'interdépendance des technologies examinées, qui exigera la mise en œuvre de politiques de sécurité intégrées afin d'éviter une fragmentation contreproductive des ressources, de l'expansion et de la diversification de l'écosystème numérique, qui va également nécessiter des politiques de coordination élaborées, de la transformation de la notion de vie privée, de la convergence des problèmes de cybersécurité et de sécurité humaine, de l'indispensable équilibre entre des mesures de cybersécurité adéquates et le maintien d'une compétitivité économique et technologique qui repose sur une certaine liberté réglementaire, des risques de voir des groupes d'individus adopter des pratiques d'autodéfense en cas de défaillance étatique, ou enfin des contributions positives de certaines des neuf tendances à la cybersécurité.

Les cinq recommandations suivantes viennent dans cette dernière section traduire en gestes concrets les constats dressés dans ce rapport.

1. Concevoir et déployer une méthodologie et des outils de veille permanents dont l'objectif sera de suivre l'évolution de l'écosystème numérique, d'en cartographier les divers acteurs, les interactions, et d'évaluer les implications de ces transformations sur la cybersécurité.

2. Aligner les régimes réglementaires applicables aux diverses infrastructures, applications et contenus avec les ressources et les stratégies mises en œuvre par un nombre croissant d'acteurs gouvernementaux, ainsi que leurs partenaires privés, afin de déceler rapidement les risques numériques émergents et limiter leur impact sur un écosystème en constante évolution.

3. Engager un exercice de consultation et de réflexion approfondi destiné à formuler des propositions sur la restructuration des institutions gouvernementales existantes ou la création de nouvelles institutions, afin d'adapter les capacités d'intervention et de coordination du gouvernement canadien aux nouveaux besoins.

4. Intensifier les recherches empiriques sur les transformations des risques, des normes et des pratiques reliées à la protection de la vie privée dans l'écosystème numérique.

5. accentuer les initiatives de coordination et de transferts de connaissances des autorités nationales et provinciales afin d'accélérer et de standardiser le développement des capacités locales.

Table des matières

Introduction et contexte

En octobre 2010, le Gouvernement du Canada rendait publique sa stratégie de cybersécurité, prenant acte de l'omniprésence des infrastructures numériques dans la vie quotidienne des usagers, des entreprises et des institutions publiques, ainsi que des nouvelles vulnérabilités qui accompagnent cette évolution technologique.

En raison des innovations constantes qui caractérisent le secteur numérique, et afin d'y répondre de manière appropriée, toute stratégie de cybersécurité doit s'accompagner d'un exercice de prospective visant à anticiper les tendances technologiques, culturelles et criminelles émergentes. La vélocité de l'innovation dans le secteur numérique est pour une large part attribuable à la fréquence d'apparition de technologies de rupture (disruptive technologies), qui redéfinissent constamment les propriétés de ce marché et exploitent de nouvelles opportunités dans des marchés moins dynamiques, ou créent tout simplement de nouveaux marchés. Le terme « technologie de rupture » a été employé pour la première fois par Clayton Christensen (1997) afin d'analyser des innovations qui ne se contentent pas d'améliorer la performance des technologies existantes (ce sont alors des technologies de continuité), mais qui définissent plutôt des produits ou services entièrement nouveaux afin de répondre à des besoins inassouvis, et transforment par conséquent durablement le paysage technologique dans lequel ils s'inscrivent. Mais cette notion de technologie de rupture peut s'appliquer à n'importe quel secteur d'activité, et elle ne permet pas à elle seule d'expliquer pourquoi le secteur numérique est si fertile en ce domaine.

Ce sont plutôt les travaux de Yochai Benkler (2006) sur la richesse des réseaux qui nous permettent de comprendre pourquoi ce secteur semble plongé dans une révolution permanente. Ce dernier postule en effet que les technologies numériques sont à l'origine d'un nouvel écosystème informationnel, dont la principale propriété est qu'il serait beaucoup moins exposé aux contraintes financières que ses prédécesseurs. En effet, alors qu'une concentration de capitaux était requise à l'ère industrielle pour produire et diffuser de l'information, la décentralisation radicale que permettent les réseaux techniques et sociaux contemporains permettrait d'abaisser les coûts d'entrée –et donc d'innovation– pour les nouveaux acteurs de l'ère numérique (Benkler, 2006 : 32), ce qui favoriseraient donc l'émergence selon des intervalles de plus en plus courts de technologies de rupture.

La combinaison de ces deux axes de réflexion nous semble particulièrement stimulante, car elle nous permet d'envisager des formes d'innovation spontanées provenant des usagers eux-mêmes ou d'acteurs considérés comme marginaux, à l'image des fraudeurs, des pirates informatiques ou des hacktivistes. La prolifération des technologies de rupture multiplierait donc le nombre de brèches (Killias, 2006), qui seraient alors exploitées par les délinquants sans être détectées des autorités pendant un certain temps, avant de donner lieu à des réponses policières et pénales plus systématiques une fois un seuil de gravité franchi.

Nous tenterons donc dans ce rapport d'identifier, à partir des technologies de rupture qui devraient atteindre leur maturité au cours des dix prochaines années, quelles brèches sont susceptibles d'affecter la cybersécurité des citoyens, des entreprises et des institutions canadiennes. Cette approche se concentre donc sur l'évolution à moyen terme de l'écosystème numérique, et sur les adaptations qu'elle provoquera de la part des délinquants, plutôt que sur des prédictions hasardeuses basées sur l'état actuel de la cybercriminalité.

Méthodologie

Neuf tendances sociotechniques et socioéconomiques ont été identifiées à partir d'une recension de 21 rapports de prospective technologique publiés par des entreprises comme Gartner Research, IBM ou PricewaterhouseCoopers, et des organismes publics comme le Ministère français de l'industrie ou le Foresight Horizon Scanning Centre du Royaume Uni, qui ont développé une expertise internationale dans ce domaine. La liste de ces documents ou sites de prospective figure dans l'annexe 1.

Ces tendances regroupent des technologies émergentes ayant le potentiel de transformer durablement l'écosystème numérique, que nous définissons comme l'ensemble des infrastructures, des applications logicielles, des contenus et des pratiques sociales qui en déterminent les modes d'utilisation (et par extension d'encadrement). La notion d'écosystème nous permet d'examiner de manière intégrée les interactions entre les dimensions technique, économique, sociale, politique et juridique de cet assemblage caractérisé par la complexité. Chaque tendance réunit des technologies de rupture convergentes qui sont rendues possibles par des percées scientifiques ou de nouvelles manières de combiner ou d'utiliser des technologies existantes. Il ne s'agit pas à ce titre de tendances générales purement fonctionnelles, comme le sont la « convergence des infrastructures » ou « l'identification et l'authentification personnelles » (Cave et al., 2009 : 5), mais plutôt de développements socio-techniques suffisamment bien définis pour correspondre à des acteurs industriels et commerciaux et à des usages légaux ou illicites parfaitement identifiables.

Les neuf grandes tendances ont été classées par ordre de fréquence d'apparition dans les rapports de prospective. Ceux qui font l'objet d'un large consensus ou qui semblent plus près d'atteindre leur maturité figurent en haut de la liste :

1. L'informatique dans les nuages (cloud computing) – 15 mentions
2. La massification des données (big data) – 12 mentions
3. L'internet des objets (internet of things) – 9 mentions
4. L'internet mobile (mobile internet) – 7 mentions
5. Les interfaces neuronales directes (brain-computer interface) – 7 mentions
6. Les paiements sans contact (near field communication (NFC) payment) – 5 mentions
7. La robotique mobile (mobile robots) – 3 mentions
8. L'informatique quantique (quantum computing) – 3 mentions

9. La militarisation de l'internet (internet weaponization)[1]

Une fois ces neuf tendances identifiées, une recherche plus systématique fut lancée pour chacune d'entre elles dans les principales bases de données scientifiques relevant des quatre disciplines suivantes : informatique, criminologie, sociologie, et gestion. Les bases de données consultées incluent : ProQuest (1.560 revues), Factiva (31.000 sources d'information), Web of Science (ISI) (8.500 revues), Business Source Premier (EBSCO) (1.125 revues), ScienceDirect (1.700 périodiques), SpringerLink (1.250 périodiques), NCJRS (210.000 publications indexées sur les questions de justice criminelle) and SSRN (665.000 articles scientifiques en prépublication). Ces bases de données ont été consultées à l'aide du méta-moteur de recherche Maestro développé par l'Université de Montréal. Des sites internet spécialisés dans les technologies émergentes et l'analyse de leurs implications sociales ont également été consultés, parmi lesquels Wired, ArsTechnica, O'Reilly Radar ou le MIT Technology Review, pour n'en citer que quelques uns.

Ce rapport présentera pour chacune des neuf tendances les éléments qui nous ont semblé comme les plus significatifs dans les textes consultés. Chaque tendance fait d'abord l'objet d'une rapide présentation technique et historique qui en retrace l'origine (si celle-ci fait l'objet d'un consensus) et les principales étapes de développement. L'évolution récente de cette tendance est ensuite décrite, qu'il s'agisse de percées technologiques accélérant son développement et ses applications commerciales, d'investissements majeurs réalisés par des intérêts publics ou privés, ou encore de comportements sociaux nouveaux qui soutiennent une très large diffusion de la technologie parmi les utilisateurs. La présence ou l'absence des principaux moteurs (drivers)[2] qui semblent influencer les tendances identifiées sont ensuite examinées, afin de comprendre comment les besoins sociaux, les conditions économiques, les décisions gouvernementales ou encore le développement de nouvelles connaissances scientifiques pourraient accélérer ou ralentir l'émergence de ces technologies. Enfin, une analyse des implications en matière de cybersécurité vient conclure l'étude de chaque tendance, qu'il s'agisse de l'apparition de vulnérabilités particulières aisément exploitables par les délinquants ou d'enjeux plus généraux en matière de régulation des acteurs directement ou indirectement responsables de la sécurité des infrastructures numériques.

[1] Cette dernière tendance n'est mentionnée dans aucun des 21 rapports, qui se concentrent sur les innovations technologiques, mais elle découle de nos observations et de la divulgation des initiatives de plus en plus nombreuses prises par les États dans ce domaine. Elle nous semble donc mériter sa place dans cette étude de prospective.

[2] Silberglitt et al. (2006 : 41-54) recensent ainsi les dix moteurs majeurs qui influencent la plupart des technologies. Il s'agit des coûts financiers, du cadre juridique et politique, des valeurs sociales de l'opinion publique, des infrastructures, des préoccupations pour le respect de la vie privée, des facteurs environnementaux, des investissements en recherche et développement, du niveau d'éducation et d'alphabétisme (literacy), des facteurs démographiques, et de la gouvernance et de la stabilité politique.

Cette méthodologie a été optimisée pour répondre à de fortes contraintes de temps et de ressources, ce qui explique notamment pourquoi elle repose exclusivement sur des données documentaires. La méthodologie élaborée par la Rand Corporation afin d'anticiper l'impact des nouvelles technologies sur les affaires internationales à l'horizon 2020 est une alternative beaucoup plus coûteuse, qui permet toutefois d'approfondir de manière plus systématique l'impact de ces tendances technologiques. Un indicateur chiffré unique mesure pour chaque tendance la faisabilité technique (probabilité que la technologie soit commercialisable), la facilité d'implantation (différence nette entre les moteurs et les freins non techniques à l'implantation, comme la demande, les coûts d'acquisition, les politiques publiques, les besoins en infrastructures, et le cadre règlementaire), et le degré de diffusion (global ou modéré). Le score de chaque tendance est ensuite pondéré en fonction des pays, afin de refléter les capacités différentielles de chaque nation à s'approprier des technologies émergentes afin de résoudre des problèmes économiques, politiques et sociaux (comme le développement durable, l'indépendance énergétique, la santé publique, le maintien de capacités de défense crédibles, etc.) (Silberglitt et al., 2006). Une méthodologie semblable, adaptée aux questions de cybersécurité et mise à jour à intervalles réguliers de cinq années, produirait certainement des prédictions mieux étayées et un classement plus fiable des tendances susceptibles de générer de profondes transformations.

Nous mettons enfin le lecteur en garde sur la nature hypothétique des transformations présentées dans les pages qui suivent, puisque le propre des technologies de rupture est d'être difficile à anticiper. Dans la mesure où l'objectif est de cartographier les tendances qui seront déterminantes au cours des dix prochaines années, on ne sera pas surpris de retrouver dans cette étude des arguments qui relèvent de la spéculation, même si elles sont inspirés par les travaux de chercheurs réputés qui publient dans des revues à comités de pairs ou d'experts unanimement reconnus.

Informatique dans les nuages

L'apparition de ce terme[3] dans le langage scientifique ne fait pas consensus (Choo, 2010). Certains estiment qu'il aurait été employé pour la première fois par Eric Schmidt, un haut responsable de Google, en 2006, alors que d'autres suggèrent que cette terminologie était utilisée dès les années 1990 par le secteur des télécommunications, lorsque les réseaux privés virtuels (VPN) furent créés afin de rendre les transferts de données plus efficaces. Le concept de logiciel en tant que service (Software as a Service ou SaaS en anglais) s'est également rapidement répandu dès la fin des années 1990, sans que le terme d'informatique dans les nuages y soit pour autant rattaché.

La définition de référence de l'informatique dans les nuages nous est fournie par le National Institute of Standards and Technology (NIST):

> A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Mell et Grance, 2011: 2)

Ce modèle se caractérise donc par l'accès à des ressources matérielles potentiellement illimitées qui ne nécessitent aucun investissement en amont de la part des usagers, puisque ceux-ci sont assumés par des tierces parties, et qui s'avèrent d'une très grande élasticité pour répondre aux besoins informationnels fluctuants des organisations (Chen et al., 2010 : 4). Le paiement se fait en effet à la minute ou à l'heure, en fonction de la consommation, sur le même modèle que l'électricité, l'eau ou le téléphone, ce qui permet une « variabilisation » des coûts (MEFI, 2011 : 67). Par ailleurs, les responsabilités et contraintes reliées à la maintenance du service sont entièrement laissées à la charge du fournisseur, l'usager n'ayant besoin que d'un accès à internet (Foresight Horizon Scanning Centre, 2010: 144).

Quatre configurations d'informatique dans les nuages sont habituellement recensées, selon le degré d'exclusivité dans l'accès aux infrastructures matérielles : les ressources peuvent être publiques, partagées par un groupe réduit d'organisations, privées, ou bien hybrides, lorsque les entreprises ont recours à un mélange de solutions publiques et propriétaires (Mell et Grance, 2011 : 2; Fenn et LeHong, 2011 : 39).

Évolution de la technologie

Les diverses évaluations de la taille du marché de l'informatique dans les nuages laissent entrevoir des niveaux de croissance à deux chiffres au cours des prochaines années. Les revenus mondiaux reliés aux services d'informatique dans les nuages s'élevaient à 68,3 milliards de dollars en 2011 et devraient doubler pour atteindre 148 milliards en 2014

[3] Le Commissariat à la protection de la vie privée du Canada (2011) a choisi d'utiliser plutôt le néologisme d'infonuagique.

(Foresight Horizon Scanning Centre, 2010: 146). Quelques acteurs dominants dans ce secteur, comme Amazon et Google, réaliseront en 2012 un chiffre d'affaires avoisinant un milliard de dollars US (Gens, 2011 : 4), ce qui en fera des fournisseurs majeurs de services aux entreprises. Cisco et IDC estiment de manière plus optimiste qu'en 2020, le tiers des données informatiques seront stockées ou transiteront par des systèmes administrés dans les nuages, et que l'explosion de ce marché pourrait générer des revenus supérieurs à un trillion[4] de dollars d'ici 2014 (Gantz et Reinsel, 2010; Nash, 2011).

Le secteur public sera aussi affecté par cette tendance, puisque le gouvernement américain estime que d'ici 2015, ses dépenses budgétaires annuelles reliées à l'achat de services d'informatique dans les nuages atteindront sept milliards de dollars (Kaufman, 2009 : 62). Le Ministère français de l'économie, qui évalue la part de l'informatique dans les nuages à 20%-25% de l'ensemble du marché informatique en 2020, estime quant à lui que les gouvernements qui désireront rester compétitifs dans ce domaine devront consentir des investissements aussi importants de ceux accordés aux industries traditionnelles comme l'automobile, et il prévoit d'injecter 780 millions d'euros dans cette technologie au titre des investissements d'avenir (MEFI, 2011 : 67).

Ce marché n'est d'ailleurs pas uniquement réservé aux entreprises ou aux gouvernements, puisque des services grand public comme DropBox proposent des outils abordables (parfois même gratuits) de partage de documents ou de synchronisation simultanée des données sur plusieurs appareils numériques (Webbmedia Group, 2011 : 14), et que Netflix ne pourrait pas commercialiser de films par diffusion vidéo en temps réel (streaming) sans s'appuyer sur les capacités techniques de l'informatique dans les nuages (Webb, 2011).

Moteurs de développement

Le premier moteur est d'ordre technique. L'informatique dans les nuages répond à une demande très forte de la part des sites de socialisation en ligne, qui s'en servent comme levier de croissance face à une explosion du nombre d'utilisateurs (plus de 800 millions dans le cas de Facebook). La prolifération des sites offrant des contenus vidéos et mobiles contribue aussi à l'essor de l'informatique dans les nuages, car elle leur permet de gérer avec agilité l'augmentation exponentielle des volumes de données devant être accessibles en tous lieux et en tout temps.

Le second moteur de développement est d'ordre financier. La flexibilité inégalée que l'informatique dans les nuages promet aux entreprises utilisatrices, ainsi que les économies réalisées, aussi bien sur les dépenses de fonctionnements qu'au chapitre des investissements, en font une proposition alléchante, particulièrement en cette période de turbulences financières (IBM, 2011 : 8).

[4] Mille milliards dans l'échelle courte en vigueur aux États-Unis et au Canada.

Implications pour la cybersécurité

L'informatique dans les nuages procure de nombreux avantages aux entreprises, mais le succès commercial espéré a quelque peu occulté le débat sur les questions de cybersécurité.

Il sera notamment nécessaire de clarifier l'encadrement règlementaire de la propriété des données, puisque celles-ci seront hébergées sur les machines des fournisseurs et non plus sur les machines ou les réseaux de leurs propriétaires. Les responsabilités de chacune des parties en matière de protection de la vie privée et de conformité aux obligations réglementaires devront faire l'objet d'une attention particulière (Kaufman, 2009 : 62), notamment en ce qui concerne la circulation et le stockage transfrontaliers des données, qui ne pourra s'affranchir des régimes réglementaires nationaux (Commissariat à la protection de la vie privée du Canada, 2011; Helmbrecht et al., 2011 : 8). Dans le même ordre d'idée, la possibilité que des fournisseurs malhonnêtes de ces services volent les informations confidentielles de leurs clients afin de les revendre à des compétiteurs n'est pas à exclure (Chen et al., 2010).

Les adeptes de l'informatique dans les nuages seront confrontés à une perte de contrôle sur la nature et l'efficacité des solutions de sécurité déployées, dans la mesure où ces décisions reposent entre les mains des fournisseurs de service qui ne disposent pas tous des mêmes capacités de protection que les leaders du marché comme Google ou Amazon. Il sera concrètement difficile, voire impossible, pour les utilisateurs de s'assurer de la mise en œuvre effective des mesures de sécurité promises (Cattedu et Hogben, 2009). La confidentialité des données risque ainsi de devenir plus difficile à assurer dans cette configuration.

Cela est d'autant plus vrai que l'architecture particulière de l'informatique dans les nuages crée une vulnérabilité accrue aux actes de malveillance ou aux défaillances internes des administrateurs ou des utilisateurs privilégiés, qui vont concentrer entre leurs mains un pouvoir inégalé sur de grandes quantités de données. Il sera toutefois plus difficile pour les utilisateurs externes d'évaluer la compétence et la fiabilité de ces administrateurs (Rocha et al., 2011 : 45), qui pourront également causer des dommages dont la gravité sera plus élevée, en raison de la quantité de données sous leur responsabilité.

Face à des risques criminels, naturels ou accidentels, l'informatique dans les nuages crée une interdépendance accrue des victimes hébergées sur une même plateforme. En effet, si un pirate s'infiltre dans les systèmes d'une entreprise offrant des services d'informatique dans les nuages, ce sont potentiellement tous les clients de cette organisation qui deviennent exposés à cette menace (Choo, 2010 : 2; Cloud Security Alliance, 2010 : 11). D'autre part, si le fournisseur de services est obligé pour une raison ou une autre (catastrophe naturelle, piratage, défaillance technique, perquisition ou saisie…) d'interrompre le fonctionnement de ses serveurs, et à moins qu'il ne dispose d'une infrastructure de redondance immédiatement disponible, ses clients perdront l'accès à leurs données jusqu'à ce que la situation soit rétablie, et verront leur performance dégradée ou leur survie menacée.

Certains chercheurs évoquent également l'utilisation criminelle qui pourrait être faite de ces capacités techniques par les pirates et les fraudeurs, afin de mobiliser leur puissance de calcul considérable pour mener des attaques et échapper à la surveillance des organisations de sécurité. D'après l'agence de presse Bloomberg, le réseau dans les nuages d'Amazon (connu sous le nom d'EC2 pour Elastic Compute Cloud) aurait ainsi été utilisé par des pirates au début de l'année 2011 pour attaquer les ordinateurs de l'entreprise Sony et s'emparer des données personnelles de plusieurs dizaines de millions de ses clients (Alpeyev, Galante et Yasu, 2011). Au début de la même année, un chercheur en sécurité allemand a dévoilé un logiciel permettant de casser les mots de passe des réseaux sans fil protégés en utilisant le service EC2 d'Amazon pour tester plus de 400.000 possibilités par seconde (Thomas, 2011). Des producteurs et de consommateurs de pornographie juvénile pourraient finalement être amenés à utiliser ces capacités afin de mieux protéger leurs transactions (Biggs et Vidalis, 2009 : 4; Choo, 2010 : 4);

En cas de litige juridique ou d'enquête criminelle, le recours à des services d'informatique dans les nuages introduit un degré de complexité additionnel lors des investigations, notamment en ce qui concerne la préservation et l'analyse de la preuve (Butler Curtis et al., 2010 : 2). En effet, l'informatique judiciaire (digital forensic investigations) répond à un cadre procédural rigoureux devant permettre l'admissibilité des preuves recueillies devant un tribunal, et parfois un jury. Les principes relatifs à la chaîne de possession (chain of custody), qui doivent garantir la provenance de la preuve, sont par exemple quasiment impossibles à respecter pour l'informatique dans les nuages, où les données sont souvent stockées hors du contrôle des enquêteurs. Les métadonnées et les informations contenues dans les journaux informatiques sont également très difficiles à obtenir dans les nuages, alors qu'elles fournissent aux enquêteurs des informations essentielles sur les activités des suspects (Reilly et al., 2010 : 6). Des protocoles adaptés à cette nouvelle réalité technologique devront donc être développés par les organismes d'application de la loi, en collaboration avec les acteurs privés qui fournissent ces services.

Conscients de l'impact des questions de sécurité sur la viabilité commerciale de leur offre de services, les principaux fournisseurs se sont d'ailleurs regroupés au sein de la Cloud Security Alliance[5] afin de concevoir des normes et standards de sécurité uniformes à toute l'industrie. Cependant, cette démarche est menée de manière autonome, sans consultation des autorités gouvernementales des principaux pays concernés, ce qui ne favorise pas réellement l'émergence de partenariats ou de réseaux de sécurité robustes.

[5] https://cloudsecurityalliance.org/.

Massification des données

Le terme « données massives » (big data) reflète l'apparition ces dernières années de fichiers de données (datasets) contenant des volumes gigantesques d'informations non structurées ou disparates. Les unités de mesure utilisées pour quantifier ces volumes de données ne sont plus le gigabit ou le terabit, mais le peta-, l'exa-, voire le zettabit (10^{21} bits). L'entreprise IDC estime ainsi qu'en 2011, la quantité mondiale d'informations créées et échangées sur des supports numériques (l'univers numérique) équivalait à 1,8 zettabits, et qu'elle serait multipliée par vingt d'ici 2020 pour atteindre 38 zettabits (Gantz et Reinsel, 2011).

Évolution de la technologie

Pour les entreprises, ces flux massifs et à très haute vélocité prennent la forme de données relationnelles internes émanant des interactions avec les clients ou les fournisseurs via les sites internet ou les centres d'appel, de résultats de sondages et d'enquêtes démographiques, de coordonnées de géolocalisation mises à jour en temps réel, de toute information produite par un équipement numérique (voir la section sur l'internet des objets), mais aussi de contenus externes provenant des sites de socialisation en ligne (social media). La volumétrie et la diversité des données traitées empêchent que les techniques traditionnelles d'analyse soient utilisées, et on doit donc faire appel à des solutions spécialisées qui s'appuient sur des outils informatiques et statistiques de pointe (technique de programmation Hadoop MapReduce, langage R pour les analyses statistiques et la visualisation), à des infrastructures conçues expressément pour de tels usages (bases de données NoSQL, bases de données massivement parallèles ou massively parallel processing, réseaux à très haut débit) et à des analystes disposant de compétences transversales en informatique et en statistique (Asthana, 2011).

Plutôt que d'analyser les données de manière sélective, les techniques de massification des données adoptent une approche globale en traitant simultanément l'ensemble des données à la disposition d'une organisation en temps quasi-réel (Fenn et LeHon, 2011 : 6), afin d'en extraire des connaissances nouvelles. Cette valeur cachée découle de l'identification de détails infimes dans un océan de données (la proverbiale aiguille dans la botte de foin) qui annoncent des tendances émergentes ou des sources de profits inexploitées (Manyika et al., 2011). Le principal attrait de la massification des donnés est en effet d'articuler à une échelle inédite des informations qui étaient auparavant appréhendées séparément, comme des données disparates sur un même individu, sur des réseaux d'individus, sur des communautés, sur des comportements collectifs ou encore sur des phénomènes naturels (Boyd et Crawford, 2011). Gartner estime que les entreprises qui maîtriseront cette panoplie de techniques réaliseront en 2015 des bénéfices surpassant de 20% ceux de leurs concurrents moins bien préparés (Fenn et LeHon, 2011 : 20). Parmi les utilisateurs les plus intensifs de ces techniques à l'heure actuelle, figurent IBM, Facebook, Google, ou encore Walmart. Les agences de renseignement, les institutions financières, les compagnies d'assurance, les entreprises

de marketing ou les opérateurs de télécommunication sont également à la pointe de cette tendance technologique de gestion « extrême » de l'information (Gruman, 2010 : 12; Banerjee et al., 2011).

Moteurs de développement

Le premier moteur de développement est social, puisque les volumes de données générés par de nouvelles pratiques de sociabilité vont connaître une croissance exponentielle au cours des prochaines années. Tout d'abord, les médias sociaux, qui sont en train de devenir le moyen de communication dominant (ayant récemment supplanté le courrier électronique), et un outil privilégié d'organisation et de mise en valeur de la mémoire personnelle des individus, génèrent d'immenses quantités de données, qu'il s'agisse de messages personnels ou collectifs, de mises à jour des différents statuts (localisation, émotions, état matrimonial, occupations professionnelles, loisirs, etc.) ou de photos partagées avec des « amis ». Ces montagnes de données devront être analysées de manière sophistiquée par les entreprises qui mettent ces plateformes à la disposition des utilisateurs afin de les valoriser auprès des annonceurs publicitaires. Par ailleurs, la pratique de plus en plus répandue de la quantification de soi (quantified self), qui préconise l'enregistrement systématique des données personnelles dans un objectif d'amélioration des performances physiques ou intellectuelles, contribue également à augmenter la quantité de données numériques pouvant faire l'objet d'analyses à très grande échelle (Webbmedia Group, 2011). Finalement, le mouvement mondial qui prône le libre accès aux données des administrations publiques (open government data), et qui connaît un succès grandissant dans certains pays, au premier rang desquels figure les États-Unis, le Royaume Uni et dans une moindre mesure le Canada, va probablement alimenter les outils de traitement massif des données. À titre d'exemple, le site américain data.gov met à la disposition des internautes plus de 390.000 fichiers de données librement exploitables, alors que le site canadien datadotgc.ca (maintenu par de simples citoyens) propose plus modestement 523 fichiers de données.

Dans le monde des affaires, on assiste depuis quelques mois à la création de marchés des données (data marketplaces) permettant aux entreprises d'accéder aux données d'autres organisations publiques ou privées afin de renforcer la puissance analytique de leurs outils. Microsoft vient ainsi de lancer ce type initiative pour sa plateforme Azure[6], et offre ou loue l'accès à 118 bases de données contenant plusieurs trillions d'entités. Des outils de visualisation de plus en plus performants vont également permettre aux organisations d'explorer et d'expliquer les données massives en leur possession de manière plus intuitive, ce qui va décloisonner l'utilisation de ce type d'analyses qui étaient jusque là réservées à un petit groupe d'experts et en accélérer l'adoption au sein des organisations (Dumbill, 2011). Enfin, l'interpénétration croissante entre le monde des entreprises et celui de la recherche, en informatique mais aussi en sciences sociales,

[6] https://datamarket.azure.com/.

va favoriser les collaborations autour de l'utilisation des données massives et permettre de nouvelles innovations dans ce domaine (Boyd et Walker, 2011).

Sur le plan technique, la croissance de l'internet des objets, que nous analyserons dans la section suivante, va également directement contribuer à l'explosion de la quantité de données recueillies par les organisations et des possibilités d'analyses novatrices qui en découleront.

Implications pour la cybersécurité

Un nombre croissant d'entreprises et d'organisations voient le potentiel commercial que la revente de telles quantités de données peut générer, et elles cherchent à en tirer une source additionnelle de revenus. De grandes institutions financières ont ainsi commencé à commercialiser les données reliées aux transactions par carte de paiement de leurs clients (magasins fréquentés et produits achetés) (Banerjee et al., 2011). En Hollande, un fournisseur de solutions de localisation par GPS a également vendu les données géocodées des déplacements de ses usagers à des agences gouvernementales, dont un service de police, qui s'en est servi pour planifier l'installation optimale de radars automatisés de vitesse (Lasar, 2011). Ce marché secondaire des données massives expose néanmoins la vie privée des clients et des usagers à des intrusions indésirables et soulève des problèmes éthiques importants. Par exemple, le croisement de fichiers de données massives permet de désanonymiser avec un degré suffisamment élevé de confiance des fragments d'information en apparence anodins (Acquisti et al., 2011). Ce déluge ininterrompu de données rend aussi particulièrement difficile l'exercice des mécanismes traditionnels de contrôle de la vie privée auxquels les organisations, les individus et les autorités régulatrices ont présentement recours. En effet, dans un tel environnement, comment arriver à déterminer avec certitude quels types de données sont collectées et détenues, avec quel degré de précision et de fiabilité, ou encore quelles sont les politiques de rétention, d'échange, de commercialisation et de destruction mises en œuvre (Newton et Pfleeger, 2006 : 180)?

Dans un tel contexte, des mécanismes automatisés de protection de la vie privée (privacy by design) et de gestion des accès devront certainement être conçus afin que les usagers et les entreprises puissent reprendre le contrôle et gérer de manière responsable les quantités massives de données qu'ils génèrent (parfois sans le savoir) et qui deviennent dorénavant exploitables (Hourcade et al., 2009 : 31; Jonas, 2011). Certaines initiatives destinées aux individus comme les applications MyPermissions[7], ThinkUp[8], ou le Locker Project[9], et les applications Accumulo, développée en source ouverte (open source) par la National Security Agency (Jackson, 2011), et Infosphere Sensemaking, développée par IBM (Jonas, 2011 : 15), illustrent la forme que pourraient prendre ces outils.

[7] http://mypermissions.org/.
[8] http://thinkupapp.com/.
[9] http://lockerproject.org/.

Si l'analyse des données massives soulève un certain nombre de problèmes techniques, assurer leur sécurité présente également de nombreux défis. Le cryptage de l'ensemble des données n'est pas une solution envisageable à une telle échelle, en raison des contraintes techniques que cela représente, et seules les informations les plus sensibles peuvent faire l'objet d'un tel traitement. Ces données doivent cependant être décryptées lors de chaque analyse, afin de permettre les croisements, ce qui expose ces informations de manière plus fréquente et plus massive à des menaces criminelles. On devra donc accélérer le développement de techniques de chiffrement qui permettent de manipuler et d'analyser les donnés sans avoir à les décrypter. Ces techniques novatrices de cryptographie protègent l'intégrité des données tout en conservant leur format initial (format-preserving encryption) (Spies, 2008).

Les plateformes techniques utilisées pour analyser les données massives sont encore relativement peu matures et n'ont pas été conçues à l'origine pour offrir des niveaux de sécurité élevés, puisqu'il s'agissait principalement d'étudier des données ouvertes (open data). Les organisations qui décident d'exploiter cette technologie devront donc acquérir ou développer des solutions de sécurité additionnelles qui resteront toujours moins robustes qu'une approche plus intégrée (security by design) (Lane, 2011).

Le processus d'amalgamation et de réutilisation des données pour des analyses répétées engendre également un phénomène de prolifération qui fait en sorte que la traçabilité des données, et particulièrement celles qualifiées de sensibles, devient de plus en plus difficile à établir. Cela multiplie donc les vulnérabilités et les opportunités pour les délinquants de s'emparer de grandes quantités de données personnelles potentiellement très profitables.

Internet des objets

L'internet des objets (internet of things) ou IdO fait référence à l'interpénétration croissante entre le monde physique et le monde numérique, par le biais de capteurs et de senseurs intégrés aux objets qui nous entourent (des véhicules automobiles aux pacemakers en passant par les réfrigérateurs et les compteurs électriques), ces derniers devenant dotés de la capacité de communiquer sans fil avec des réseaux informatiques grâce au protocole internet. Les flux de données massives produits par ces objets facilitent alors la surveillance de leur fonctionnement ainsi que des environnements dans lesquels ils opèrent (Chui et al., 2010). Ils peuvent ainsi renseigner leur propriétaire ou l'entreprise qui les exploite sur leur état général de fonctionnement, leurs besoins éventuels de maintenance, leur productivité, les heures prévues d'arrivée à une destination prédéterminée, mais aussi sur le rythme cardiaque ou le taux de glycémie de la personne qui est équipée d'un tel appareil, etc. (Gens, 2011 : 18). On va donc assister à une expansion de l'internet, qui va non seulement englober des réseaux numériques traditionnels mais aussi des réseaux locaux d'objets capables de communiquer entre eux et avec leurs contrôleurs (Hourcade et al., 2009 : 2).

Évolution de la technologie

Gartner estime que cette tendance atteindra son apogée d'ici une décennie, même s'il y a déjà plus d'objets que d'ordinateurs connectés à internet (Fenn et LeHong, 2011 : 23). Cisco prédit qu'il y aura plus de 50 milliards d'objets connectés à internet en 2020 (Evans, 2011 : 3), alors que l'association internationale des opérateurs de télécommunication mobile est plus circonspecte avec un estimé de 24 milliards, ce qui s'explique par une définition plus restrictive de ce qu'est un objet connecté (GSMA, 2011 : 3).

Moteurs de développement

Le premier moteur de développement est d'ordre technique. Bien que le concept d'IdO ne soit pas nouveau en soi, la miniaturisation des composants électroniques, leurs bas coûts et l'augmentation de la puissance de calcul et de la bande passante des réseaux informatiques ont entraîné une diversification et une accélération du nombre d'objets qui peuvent être connectés à l'internet (Fenn et LeHong, 2011 : 6). L'adoption de la version 6 du protocole internet (IPv6), qui fait passer le nombre d'adresses disponibles de 4,2 milliards à 340 sextillions (10^{36}), facilitera aussi l'expansion de l'internet des objets et ouvrira la voie à un nombre incalculable de nouvelles possibilités, pour peu que ces dernières procurent une valeur ajoutée aux services existants.

Sur le plan fonctionnel, l'IdO devrait en effet permettre aux entreprises et aux institutions publiques d'offrir des services qui n'étaient pas disponibles auparavant et qui amélioreront la qualité de vie des usagers, comme de localiser en temps réel les places de stationnement disponibles dans un quartier, ou d'améliorer la qualité des soins en faisant converger plus rapidement des patients en détresse et l'expertise médicale la plus proche (Fenn et LeHong, 2011 : 23). Les nombreuses applications pratiques de l'IdO qui permettront aux individus et aux organisations d'optimiser leur

utilisation de l'espace et du temps devraient alimenter la croissance rapide de cette tendance au cours des prochaines années.

Enfin, sur le plan économique, l'association GSMA évalue les opportunités de profits reliées à l'IdO à 445 milliards de dollars pour l'industrie de l'électronique grand public, 202 milliards pour l'industrie automobile, 69 milliards pour le secteur de la santé et 36 milliards pour les distributeurs d'électricité, d'eau, ou de gaz (utilities) (GSMA, 2011).

Implications pour la cybersécurité

L'IdO va ouvrir de nouvelles possibilités en matière de surveillance, qui risquent cependant de soulever de nombreux débats concernant l'éthique et le respect de la vie privée. Contrairement aux systèmes de vidéosurveillance qui sont limités par le type de données qu'ils peuvent recueillir et traiter, l'IdO sera en mesure d'offrir aux services de sécurité l'accès à des données très riches, qu'il s'agisse d'images prises par des téléphones intelligents, mais aussi de sons, d'odeurs, de composés chimiques, d'informations biométriques, etc (Silberglitt et al., 2006 : 28). Quelques services de police canadiens ont déjà eu recours aux capacités d'enregistrement d'appareils électroniques utilisés par de simples citoyens pour identifier les auteurs d'actes de vandalisme lors d'émeutes urbaines à Montréal, Toronto ou Vancouver. D'autres villes nord-américaines comme Washington, Los Angeles ou Boston ont installé dans leurs quartiers les plus violents des grappes de capteurs acoustiques qui peuvent détecter l'origine de coups de feu ou de cris de détresse (Klein, 2006; Ntalampiras et al., 2009). L'IdO va accélérer cette tendance à l'emploi de capteurs technologiques pour des fonctions de sécurité. Cependant, l'utilisation qui sera faite de telles capacités soulèvera certainement de nombreuses objections de la part des organismes de protection de la vie privée.

L'augmentation du nombre d'entités connectées à internet va mathématiquement augmenter le nombre de cibles disponibles pour les pirates informatiques, qu'il s'agisse de voitures, d'instruments médicaux, ou d'appareils domotiques (home automation). Un employé mécontent d'une concession automobile du Texas a ainsi déjà réussi à pirater en 2010 une centaine de voitures en accédant à distance au système d'immobilisation des véhicules, prévu pour être utilisé en cas de non paiement des mensualités (Poulsen, 2010). Des chercheurs ont également mis en évidence comment des pompes à insuline, des pacemakers et des défibrillateurs cardiaques implantés dans le corps de patients pouvaient être piratés et reprogrammés à distance en exploitant la sécurité déficiente des connexions de ces objets (The Future Laboratory, 2011 : 11).

Du fait de leur nombre et de la nécessité de maintenir des coûts de production et de fonctionnement aussi bas que possible, les concepteurs et fabricants de ces objets connectés ne souhaiteront (ou ne pourront) probablement pas les équiper de dispositifs de sécurité trop contraignants, sauf pour ceux qui sont intégrés à des biens de consommation onéreux (comme les voitures de luxe) ou à des services essentiels relevant de la santé humaine ou des infrastructures essentielles (les compteurs intelligents ou smart meters). Cette réticence risque de créer de nouvelles vulnérabilités pour l'internet dans son ensemble, puisque ces objets pourront être utilisés par les

pirates comme points d'accès à des systèmes plus attractifs vers lesquels ils redirigeront leurs attaques (Roman et al., 2011);

Les implications ne sont pas uniquement d'ordre numérique, puisque la multiplication dans les espaces publics des objets connectés à internet (feux de circulation, caméra de vidéosurveillance, véhicules, compteurs divers, etc.) va aussi poser le problème de leur sécurité physique. À moins que des mécanismes de protection et de durcissement (hardening) soient imaginés, ils échapperont en effet à la vigilance de gardiens capables (capable guardians), en dépit du fait qu'ils constitueront des cibles intéressantes pour des délinquants motivés (Cohen et Felson, 1979) qui disposeront à travers eux d'un accès matériel à des réseaux informatiques sensibles.

Internet mobile

Le concept d'internet mobile (mobile internet ou mobile computing) désigne l'ensemble des technologies qui permettent l'accès complet ou allégé à internet à l'aide d'appareils mobiles tels que des téléphones intelligents ou des tablettes informatiques (de type iPad). L'internet mobile englobe trois composantes : 1) les appareils mobiles qui rendent cela possible; 2) les applications qui permettent à ces appareils de se connecter à des réseaux informatiques (comme les systèmes d'exploitation iOS d'Apple, Android de Google, Windows 8 de Microsoft ou Blackberry OS), ainsi que les nombreuses applications disponibles pour chacun d'entre eux; 3) et les technologies qui permettent aux sites internet de reconnaître leurs usagers connectés via des technologies mobiles et de leur offrir ainsi un contenu adapté à leur position géographique ou à leurs intérêts personnels.

Évolution de la technologie

L'internet mobile est né vers la fin des années 1990 (Kaikonnen, 2009), mais il est resté jusqu'à récemment un phénomène marginal. C'est la croissance actuelle du marché des téléphones intelligents –qui intègrent en un même appareil des fonctions de téléphonie, de gestion des données, de photographie, de vidéo, de musique ou de géolocalisation– qui alimente cette tendance et permet aux usagers d'être connectés à internet en tous lieux et en tout temps.

Pour l'année 2012, IDC prévoit qu'il se vendra deux fois plus d'appareils mobiles (895 millions d'unités) que d'ordinateurs classiques (400 millions d'unités) (Gens, 2011 : 7), et que les dépenses reliées à la consommation de données via des réseaux mobiles vont pour la première fois dépasser les dépenses associées à la consommation de données distribuées par des réseaux fixes (technologie ADSL ou fibre optique par exemple). Le téléchargement anticipé de 85 milliards d'applications mobiles (mobile apps) devrait permettre à l'internet mobile de soutenir une croissance très dynamique pendant encore quelques années (Gens, 2011).

D'ici 2015, un quart des cartes SIM[10] activées dans le monde seront associées à des téléphones intelligents ou à des modems mobiles (identiques aux clés 3G), ce qui représentera un marché de 1,5 milliards de consommateurs (GSMA, 2011 : 2).

Moteurs de développement

Le premier moteur de développement est d'ordre économique. Les entreprises de télécommunication mobile investissent en effet massivement dans le déploiement de technologies de dernière génération (3G, LTE), qui offriront des accès à internet aussi rapides que ceux dont disposent les clients résidentiels branchés sur des connexions à haut débit. Au cours des cinq prochaines années, les investissements mondiaux dans ce

[10] La carte SIM est une puce qui permet d'identifier un utilisateur sur un réseau mobile.

domaine devraient s'élever à plus de 100 milliards de dollars, et 300 millions d'usagers devraient être connectés aux réseaux de dernière génération LTE en 2015 (GSMA, 2011 : 2). Les profits que ces entreprises espèrent tirer de la vente de services de données sont directement proportionnels aux investissements consentis et expliquent donc cet engouement.

Les implications techniques de ces investissements financiers vont très rapidement se faire sentir, dans la mesure où l'association professionnelle GSMA (2011 : 4) prévoit que cette infrastructure technique multipliera par dix le volume de données numériques qui transiteront par les réseaux mobiles d'ici 2020, pour atteindre 42 exabits. Cette croissance des données échangées bénéficiera particulièrement aux pays en voie de développement, pour qui l'internet mobile sera un moyen d'accéder directement à des connexions à haut débit, en l'absence d'infrastructures terrestres (ITU, 2010 : 2).

Les moteurs économique et technique vont également entraîner un troisième moteur, d'ordre commercial. Les entreprises de services voient en effet dans l'internet mobile des opportunités à exploiter, étant donné que les applications leurs permettront d'améliorer la rentabilité de leurs modèles d'affaires et d'interagir de manière beaucoup plus personnalisée avec leurs clients, en profitant notamment des capacités de géolocalisation de l'internet mobile (Yuan et Barker, 2011 : 6; Webbmedia, 2011 : 12). En réponse à ce moteur commercial, on estime que d'ici 2013, près de 80% des entreprises devraient équiper une partie de leurs employés de tablettes informatiques (Yuan et Barker, 2011 : 6). Une barrière potentielle à ce moteur lié à une meilleure productivité concerne la multiplication des plateformes en concurrence (Android, iOS, Windows 8, Blackberry OS, webOS, etc.). Elle risque d'entraîner des coûts de développement plus élevés pour les nouvelles applications, surtout si ces dernières doivent être disponibles sur l'ensemble plateformes existantes (IBM, 2011 : 7).

Implications pour la cybersécurité

Les consommateurs profiteront des capacités techniques des téléphones intelligents et des appareils mobiles, combinées aux services offerts par les entreprises, pour effectuer des transactions financières ou bancaires en ligne où qu'ils se trouvent et en tout temps. D'ailleurs, des services de portefeuille mobiles (mobile wallets), destinés à se substituer aux paiements en espèce sont en développement. Les fraudeurs vont donc trouver là une nouvelle source de revenus, et l'infection des téléphones à l'aide d'applications malveillantes (malware) devrait connaître une croissance reflétant le fort taux d'adoption de l'internet mobile. L'entreprise de sécurité Norton a ainsi mesuré à l'aide d'un sondage que 10% de la population adulte aurait déjà été victime de crimes reliés à l'utilisation de téléphones intelligents, et Symantec évaluait en 2010 que les menaces spécifiques à l'internet mobile avaient connu une croissance de 42% par rapport à l'année précédente (Albanesius, 2011).

Comme dans toute période d'émergence de nouveaux risques, les délinquants bénéficient d'une fenêtre d'opportunité durant laquelle le public reste mal informé des vulnérabilités auxquelles il est exposé et des moyens de protection à mettre en œuvre. Ainsi un sondage récent conduit en France montrait que seulement 4% des utilisateurs

de téléphones intelligents étaient préoccupés par les risques liés aux virus informatiques, alors que ce chiffre était de 22% pour les utilisateurs d'internet (The Future Laboratory, 2011 : 14). De même, près du tiers des répondants d'un sondage mené par Damballa en 2011 était préoccupé par la cybercriminalité liée à l'utilisation des ordinateurs personnels, alors que ce chiffre n'était que de 13% pour la cybercriminalité liée aux téléphones intelligents (Damballa, 2011). Cela se traduit par des taux moins élevés d'adoption de solutions de sécurité parmi les utilisateurs de l'internet mobile, puisque seulement 16% avaient installé les plus récentes applications de sécurité, et 13% des personnes interrogées avaient installé un logiciel capable d'effacer les données personnelles en cas de perte ou de vol (Damballa, 2011). Dans ce contexte, la sécurité des applications téléchargées par les utilisateurs et les politiques de contrôle (prospective ou rétrospective) mises en œuvre par les grandes plateformes telles qu'Android Market ou iTunes App Store vont s'avérer déterminantes (Giles, 2010).

Les problèmes de sécurité reliés à l'internet mobile ne concernent pas uniquement les logiciels. Les équipements mis sur le marché et la chaîne d'approvisionnement en composants et de distribution devront également faire l'objet d'une vigilance particulière. Ainsi, en 2010, la filiale espagnole du géant anglais des télécommunications Vodafone a été confrontée à un incident lors duquel 3.000 téléphones intelligents infectés par le logiciel malveillant Mariposa ont été commercialisés par ses propres revendeurs agréés (Leyden, 2010).

Bien évidemment, l'internet mobile ne sera pas uniquement une source additionnelle de risques, et de nombreuses institutions financières ont déjà intégré à leur dispositif de lutte anti-fraude des alertes par email et SMS qui facilitent l'identification précoce de transactions suspectes (de Villiers, 2010). L'internet mobile dispose donc d'un potentiel attrayant de contribution à la sécurité de l'écosystème numérique.

Interfaces neuronales directes

Les interfaces neuronales directes (brain-computer interface) sont des technologies qui permettent de connecter directement des dispositifs informatiques externes au cerveau ou au système nerveux humain. Cela permet ainsi aux individus d'interagir avec des ordinateurs par la pensée. Ces technologies sont actuellement utilisées en médecine afin de compenser, d'assister ou d'augmenter les fonctions cognitives et motrices de personnes souffrant de déficiences physiques (paralysie, syndrome d'enfermement ou locked-in syndrome) ou psychologiques (stress, déficit de l'attention) (Foresight Horizon Scanning Centre, 2010). Ces technologies impliquent généralement l'utilisation d'électrodes plus ou moins invasives, c'est-à-dire fonctionnant par simple contact avec le cuir chevelu ou au contraire implantées directement dans le cerveau lors d'une opération chirurgicale, pour capter les ondes émises par le cerveau (Demetriades et al., 2010 : 267).

Évolution de la technologie

Cette technologie est en développement depuis le début des années 1970, mais peu d'avancées ont été initialement réalisées en raison des limites techniques de l'électro-encéphalographie (EEG), c'est-à-dire la méthode par laquelle on mesure l'activité électrique du cerveau. En effet, les taux élevés d'erreur entre les signaux émis et leurs interprétations sont longtemps restés trop importants pour envisager des applications en dehors des laboratoires de recherche (Wang et Jung, 2011 : 2).

Ces interfaces se situent dans le prolongement des interfaces intuitives d'interaction avec les technologies numériques, comme les systèmes de reconnaissance vocale, les écrans tactiles ou les systèmes de détection des mouvements, que l'on retrouve sur les technologies Wii de Nintendo, Kinect de Microsoft ou SIRI d'Apple. Ces technologies auparavant coûteuses et réservées au monde de la recherche ou de l'entreprise sont en train de faire leur apparition dans l'électronique grand public, et seront amenées à remplacer progressivement le clavier et la souris comme modes privilégiés d'interaction entre les humains et les machines (Yuan et Barker, 2011).

Moteurs de développement

Sur le plan technique, le développement de méthodes non invasives de mesure des activités cérébrales et d'équipements de plus en plus légers devrait accélérer le développement et l'adoption de cette technologie. En effet, jusqu'à récemment, on estimait que les interfaces neuronales directes devraient avoir recours à des implants électroniques dans le cerveau humain pour pouvoir fonctionner efficacement, ce qui constituait une barrière technique majeure au développement de cette technologie pour des applications commerciales (Silberglitt et al., 2006 : xix). Des avancées importantes ont été réalisées dans ce domaine, et la société Emotiv[11] commercialise

[11] http://www.emotiv.com/index.php.

depuis quelques mois, et au prix de 300$, un casque neuronal sans fil (wireless neuroheadset) permettant l'acquisition et le traitement de signaux cérébraux. Des recherches sont par ailleurs engagées afin de mesurer les signaux neuronaux sans contact physique, en combinant plusieurs catégories de capteurs différents (Fenn et LeHong, 2011). La miniaturisation et la baisse des coûts de cette technologie, ainsi que le développement d'applications grand public et le raffinement des techniques d'interprétation des signaux émis par le cerveau devraient favoriser son adoption d'ici les cinq prochaines années, selon IBM Research (Brown, 2011).

Implications pour la cybersécurité

Cette technologie manifeste un potentiel élevé pour la détection de la vérité et la lecture directe des souvenirs, qui ne concernent pas la cybersécurité en tant que telle mais illustre la convergence entre les avancées des technologies numériques et leurs applications à des problèmes de sécurité plus classiques. Cependant, de telles utilisations vont soulever des problèmes inédits en matière de protection de la vie privée s'il devient possible de lire dans les pensées ou de mesurer les émotions des individus à leur insu de manière routinière et avec un taux satisfaisant de fiabilité.

Les interfaces neuronales directes ouvrent également la voie à de nouveaux risques de piratage du cerveau (brain hacking), d'autant plus que les effets à long terme de ces interfaces sur les sujets humains et les changements de personnalité qu'elles provoquent restent très mal connus (Clausen, 2009). Si l'on poursuite ce raisonnement, on pourrait alors envisager des attaques lancées depuis l'écosystème numérique, à partir d'ordinateurs, vers des cibles humaines, et qui auraient pour conséquences directes des lésions psychologiques ou physiques durables. Cela constituerait un facteur additionnel et inédit de convergence entre risques numériques et risques physiques. Dans le même ordre d'idées, il est aussi possible que ces technologies soient utilisées comme substituts aux produits stupéfiants actuellement disponibles, et que de nouveaux marchés criminels similaires à ceux de la drogue offrent des expériences inédites d'addiction à travers ces technologies interactives en réseau (Cave et al., 2009 : 15).

La généralisation de cette technologie devra également nous amener à reconsidérer les règles existantes permettant d'établir la responsabilité pénale des individus. En effet, si un acte criminel découle de l'interprétation erronée qu'une interface neuronale pourrait faire des pensées d'un utilisateur, comment attribuer avec certitude la responsabilité aux diverses composantes de ce système hybride (Nishida et Nishida, 2007)? On peut donc supposer que la régulation de ces technologies devra combiner des approches légales, techniques et médicales, ce qui risque de poser un problème significatif aux autorités de régulation, peu habituées à opérer à l'intersection de plusieurs domaines d'activités (Cave et al., 2009; Demetriades et al., 2010).

Paiements sans contact

La technologie des paiements sans contact (near field communication (NFC) payment) exploite diverses technologies de communication sans fil apparentées aux puces RFID afin de faciliter les transactions financières aux points de vente. Cette technologie est principalement installée sur des cartes de paiement et des téléphones mobiles, qu'il suffit d'approcher à quelques centimètres d'un appareil récepteur équipé pour effectuer la transaction, ce qui accélère considérablement le passage aux points de vente (Tata, 2011 : 9). Cette technologie vise à faciliter les interactions de proximité entre divers appareils et vient directement concurrencer des moyens de paiement traditionnels comme les espèces ou les cartes de débit et de crédit (Ondrus et Pigneur, 2009).

Évolution de la technologie

Dès 2003, la société américaine Applied Digital Solution (ADS) créait le système VeriPay, une puce RFID sous-cutanée permettant de payer ses achats sans avoir à sortir son portefeuille. Ce système n'a toutefois jamais obtenu le succès escompté et sa production a été interrompue en 2010.

Des acteurs industriels majeurs tels que Google (Google Wallet), Apple, Nokia (système Obopay), AT&T, T-Mobile et Verizon (consortium Isis) ou encore BMW (technologie de clé Connected Drive) ont réalisé au cours des derniers mois des investissements importants dans cette technologie et devraient en faire la promotion auprès des consommateurs. Des entreprises de la Silicon Valley comme Naratte (système Zoosh) développent également des alternatives technologiques qui possèderont toutefois les mêmes fonctions que les systèmes de paiement sans contact décrites plus haut (Webbmedia Group, 2011 : 12).

Moteurs de développement

À l'heure actuelle, on observe des degrés d'adoption très variables à l'échelle internationale : alors que cette technologie s'avère populaire en Asie (particulièrement au Japon), elle a encore du mal à percer en Europe et en Amérique du Nord. On doit donc chercher dans des moteurs commerciaux et économiques les raisons de ces rythmes différents de développement.

Sur le plan commercial, La généralisation de cette technologie sera principalement déterminée par son adoption dans les domaines du service rapide et des secteurs économiques où les transactions sont très fréquentes, comme celui du transport en commun (Ondrus et Pigneur, 2009). Aux États-Unis, les cafés Starbucks figurent ainsi parmi les premières entreprises à investir dans cette technologie (Kunur, 2011), et au Canada, plusieurs sociétés de transport commercialisent leurs abonnements mensuels sur des cartes de paiement sans contact (carte Opus dans la région de Montréal). L'arrivée de Google et d'Apple sur ce marché devrait également accélérer le rythme d'adoption.

Mais les efforts commerciaux ne seront pas les seuls déterminants du développement de cette technologie, qui fonctionne selon une structure économique particulière. La technologie du paiement sans contact correspond en effet à ce que les économistes appellent un marché biface (two-sided market), dans lequel les usagers et les entreprises devront adopter la technologie simultanément pour qu'elle se généralise (Rochet et Tirole, 2003). Les entreprises du secteur financier, qui ont appris à maîtriser ce type de marché par le biais des cartes de paiement, joueront donc un rôle important. Leur capacité à conclure des ententes stratégiques avec les entreprises de télécommunication sera déterminante. Dans le prolongement des considérations sur les technologies de rupture, il se pourrait cependant que des entreprises extérieures au secteur bancaire (par exemple internet et télécommunications) choisissent de concurrencer frontalement ce dernier en ne s'associant pas à lui dans le déploiement de cette technologie. À titre d'exemple, l'entreprise China Mobile, spécialisée comme son nom l'indique dans la téléphonie cellulaire, a investi en mars 2010 près de six milliards de dollars dans la Shangai PuDong Development Bank afin d'accélérer la commercialisation de ses services de paiement en ligne (Bloomberg, 2010).

D'un point de vue technique, l'interopérabilité entre les divers systèmes en développement reste une question non résolue, et tant que des normes internationales n'auront pas été acceptées par l'ensemble des acteurs de ce marché émergent, ou qu'un consortium d'acteurs dominants n'aura pas affirmé sa suprématie, cette technologie aura du mal à se développer à l'échelle mondiale.

Implications pour la cybersécurité

Les implications pour la cybersécurité sont très similaires à celles déjà soulevées pour l'internet mobile, mais un problème de sécurité additionnel relève de la transmission non sécurisée de données bancaires qui entraîne un risque d'interception et de manipulation des données par des tiers malveillants (Balaba, 2009). La technologie n'est en effet pas conçue pour des applications liées à la transmission de données sensibles et les opérateurs de télécommunication, les fabricants de téléphones, de terminaux de paiement ainsi que les concepteurs d'applications devront superposer leurs propres solutions de sécurité à l'architecture technologique existante.

Robotique mobile

La robotique mobile (mobile robots) fait référence à des systèmes mécaniques poly-articulés capables de se déplacer de manière autonome ou semi-autonome et ayant la capacité d'influencer leur environnement immédiat (Fenn et LeHong, 2011). Ces machines remplissent trois fonctions principales : la perception, le raisonnement et l'action. Certains de ces robots disposent aussi de fonctions de communication sans fil, ce qui permet de parler de robotique collaborative (MEFI, 2011 : 74).

Évolution de la technologie

On retrouve la robotique mobile dans un nombre croissant de secteurs d'activités, comme les industries manufacturières, mais aussi les entreprises de services, le secteur de la santé, ainsi qu'en remplacement des humains afin de remplir des tâches dangereuses.

Le Japon et l'Allemagne sont les pays les plus avancés dans le développement de technologies civiles de robotique mobile, alors que les États-Unis et Israël dominent le marché de la robotique militaire. Le Ministère français de l'économie estime que le marché des robots pourrait représenter 30 milliards de dollars d'ici 2015 (MEFI, 2011).

Moteurs de développement

Sur le plan scientifique, les récents progrès en ingénierie biomédicale ont permis de concevoir des robots dont la mobilité se rapproche maintenant de celle des êtres vivants (Newton et Pfleeger, 2006 : 187), comme en attestent les modèles développés par Sony et Honda (voir ci-dessous), mais aussi Boston Dynamics pour le robot BigDog destiné au transport de matériel en terrain accidenté pour les troupes américaines (Raibert et al., 2008). Des avancées importantes restent cependant encore à accomplir en matière de communication « naturelle » entre machines et humains afin que le partage de l'espace et la coopération puisse se faire de manière harmonieuse (Luo et Perng, 2011). L'intelligence artificielle et la vision, qui déterminent la compréhension par les robots de la réalité tridimensionnelle qui les entoure, devra aussi faire l'objet de recherches additionnelles (Costa et al., 2011). Enfin, le traitement de l'information, comme la capacité à oublier afin de se débarrasser des informations inutiles afin de ne pas surcharger les capteurs, devra être amélioré afin de rendre la performance de ces machines compatible avec leur évolution dans des environnements complexes (Freedman et Adams, 2011).

Pour ce qui concerne les moteurs industriels, on relèvera que Sony et Honda ont créé des robots de compagnie ayant une apparence humaine ou animale, ce qui laisse penser que ce marché devrait s'élargir au cours des prochaines années pour ne plus concerner exclusivement les applications professionnelles. Les algorithmes et les applications logicielles font également l'objet d'initiatives industrielles favorisant le développement de nouveaux produits : Microsoft ou iRobot mettent ainsi désormais à la disposition des

ingénieurs en robotique les codes sources de leurs produits (Kinect et Roomba), afin que ceux-ci puissent les intégrer librement à leurs projets.

Les moteurs sociaux vont également jouer un rôle important dans le développement de la robotique mobile. Le vieillissement de la population dans les pays occidentaux et les moyens budgétaires limités pour la prise en charge institutionnelle de personnes à mobilité réduite va conduire au développement de technologies facilitant le maintien à domicile des personnes âgées. Les robots mobiles pourraient donc constituer une alternative attractive combinant des fonctions d'aide à l'exécution des tâches ménagères et de surveillance des signes vitaux de leurs propriétaires, donnant l'alerte en cas de problème de santé. Les robots pourraient également être utilisés dans les milieux de travail où évoluent des employés aux compétences extrêmement rares (on pense notamment ici aux chirurgiens), afin de leur permettre de se « projeter » à plusieurs endroits simultanément. Ces robots incarneraient alors des individus existants dans des lieux où ils ne peuvent se rendre mais où leur expertise est requise (Newton et Pfleeger, 2006 : 187). Une barrière à surmonter sera toutefois celle de l'acceptabilité sociale. En effet, la peur d'interagir avec des machines trop (ou pas assez) anthropomorphes, ou encore la crainte de voir ces dernières supplanter les emplois d'êtres humains pourraient freiner le déploiement de cette technologie (Salvini et al., 2010a).

Implications pour la cybersécurité

La multiplication de robots autonomes dans l'espace public va faire apparaître de nouveaux risques pour la sécurité des individus, notamment si des robots adoptent des comportements indésirables ou commettent des erreurs à l'origine d'accidents. Des règles et des normes de comportement respectueuses de l'intégrité physique des humains devront donc être élaborées et insérées dans les applications de contrôle de ces robots afin de réduire les menaces (Bicchi et al., 2010) et d'assigner les responsabilités en cas d'incident.

Dans la mesure où les communications avec les robots mobiles reposeront sur des technologies sans fil (voir section sur l'internet des objets et l'internet mobile), la multiplication de ces machines dans l'espace public va générer des opportunités pour leur prise de contrôle malveillante par des pirates informatiques. Les protocoles de communication qui seront utilisés et les mécanismes d'authentification permettant d'envoyer des instructions aux robots mobiles devront donc faire l'objet de précautions particulières, même si cela contribuera à augmenter les coûts de fonctionnement. À titre d'exemple, des drones militaires américains utilisés en Irak ont déjà été piratés par des insurgés qui ont pu intercepter les signaux émis et en déduire les lieux ou les personnes ciblées par leurs opérateurs. L'interception de ce type de signaux risque de se multiplier avec l'utilisation croissante de robots pour des activités de surveillance, dans les environnements aérien, mais aussi maritime et terrestre (extérieurs et intérieurs) (Räty, 2010). Les pirates pourraient utiliser ces données de surveillance afin de planifier des attaques physiques (comme des cambriolages) ou accéder à des informations

personnelles susceptibles de les aider dans leurs attaques numériques (comme le recueil d'identifiants et de mots de passe).

Le statut juridique de robots qui seront dotés dans un avenir proche d'autonomie et de ce qui pourrait s'apparenter à de l'intentionnalité devra aussi faire l'objet de réflexions approfondies (Salvini et al., 2010b). Le Japon a ainsi établi depuis 2003 des zones géographiques dans lesquelles les robots peuvent évoluer dans l'espace public sans permis spécial (les *Tokku* ou zones dérèglementées), mais ce statut juridique particulier est limité aux tests et aux expérimentations de prototypes.

Informatique quantique

L'informatique quantique (quantum computing) est une branche de l'informatique encore à un stade très embryonnaire de développement qui laisse néanmoins entrevoir des applications révolutionnaires en matière de puissance de calcul, et par conséquent de sécurité. L'informatique quantique s'appuie sur les lois de la mécanique quantique afin de traiter de grands volumes d'information de manière beaucoup plus efficace que l'informatique traditionnelle. Pour rappel, cette dernière utilise comme unité de mesure les bits, qui servent à coder l'information de manière binaire à partir de uns et de zéros. Par contraste, l'informatique quantique repose plutôt sur des qubits (abbréviation de quantum bits) qui possèdent deux caractéristiques uniques à la mécanique quantique, que sont la superposition et l'intrication (entanglement). La superposition est un phénomène par lequel le même système peut être simultanément dans plusieurs états différents, ce qui augmente considérablement la complexité des opérations qui peuvent être effectuées. L'intrication décrit quant à elle la très forte corrélation entre des particules quantiques qui se comportent de manière identique, même si elles sont séparées par de grandes distances[12]. Cette seconde propriété s'avère particulièrement utile en matière de sécurité, car toute tentative d'interception d'un message crypté échangé entre deux parties modifiera l'état des particules reçues par le destinataire et dévoilera de manière incontestable la tentative de compromission.

Évolution de la technologie

Pour l'instant, l'informatique quantique reste essentiellement au stade théorique, même si des solutions très spécifiques de cryptographie quantique sont déjà disponibles sur le marché. Les rares ordinateurs qui ont été fabriqués restent confinés aux laboratoires des grandes universités et des entreprises qui mènent des recherches dans ce domaine. L'Université de Waterloo a développé en collaboration avec le Massachusetts Institute of Technology l'ordinateur quantique le plus puissant à l'heure actuelle, qui est capable de traiter douze qubits[13]. Cela reste toutefois encore insuffisant pour égaler la performance des ordinateurs classiques, de l'aveu de ses propres concepteurs. En raison de l'instabilité des systèmes quantiques et des nombreux obstacles techniques à surmonter, plusieurs années seront nécessaires avant que l'informatique quantique ne tienne pleinement ses promesses (QISTEP, 2004). Il y a quelques années de cela, la Rand Corporation qualifiait sa faisabilité technique de hautement improbable (Silberglitt et al., 2006 : xix).

Moteurs de développement

Parmi les moteurs industriels, signalons que de grandes entreprises comme IBM, HP, Microsoft et Google, ainsi que des entreprises en démarrage (start-ups) comme D-Wave

[12] http://www.physique.usherbrooke.ca/~ablais/intro_info_quantique.htm;
[13] http://iqc.uwaterloo.ca/welcome/quantum-computing-101.

Systems en Colombie Britannique, ou MagiQ Technologies aux États-Unis, investissent des sommes importantes dans l'informatique quantique afin d'accélérer le développement de machines et d'applications pratiques.

Ces efforts industriels sont menés conjointement avec le monde de la recherche, qui bénéficie de soutiens financiers importants. Au Canada par exemple, Mike Lazaridis, le co-fondateur de Research in Motion (RIM), a fait un don de 100 millions de dollars à l'Université de Waterloo en 2002 afin de financer la création d'un Institut d'Informatique Quantique (Institute for Quantum Computing) (Gillmor, 2012), auquel le gouvernement canadien a accordé une subvention additionnelle de 50 millions en 2009[14]. D'autres pays, comme les États-Unis, la Chine, mais aussi l'Union Européenne investissent des ressources significatives dans la recherche fondamentale et appliquée sur cette technologie (Palmer, 2009; Weinberger, 2009; Shay, 2010).

Implications pour la cybersécurité

L'informatique quantique est particulièrement adaptée à plusieurs catégories de problèmes centraux à la cybersécurité comme la cryptographie ou la cryptanalyse.

En matière de cryptographie, l'informatique quantique serait en mesure de produire et de transmettre des clés de cryptage inviolables puisque toute interception serait détectée instantanément. Cette propriété en ferait un outil indispensable pour les agences de renseignement, les autres services gouvernementaux exigeant de hauts niveaux de confidentialité, ainsi que des institutions financières (Silberglitt et al., 2006 : 31).

Dans le domaine de la cryptanalyse (le déchiffrement de messages cryptés sans clé), la puissance de calcul offerte par l'informatique quantique permettrait, à priori, de casser sans grande difficulté les clés de chiffrement les plus puissantes et rendrait toute communication fondamentalement vulnérable (Sanders, 2012).

Ainsi, une percée décisive dans la mise en application des théories de l'informatique quantique aurait le potentiel de menacer la cybersécurité, et plus largement la sécurité nationale, des adversaires (ou même des alliés) de l'État ayant fait cette découverte le premier.

[14] http://www.ic.gc.ca/eic/site/ic1.nsf/eng/04558.html.

Militarisation de l'internet

La militarisation de l'internet (internet weaponization ou internet militarization) ne découle pas d'innovations techniques particulières, mais plutôt de l'évolution des doctrines stratégiques et tactiques. Même si l'histoire de l'internet est intimement liée aux investissements militaires réalisés par diverses agences de recherche du Ministère américain de la défense dès le début des années 1960, l'environnement numérique n'avait pas été considéré jusqu'à présent comme un champ de bataille à part entière, comme le sont les environnements terrestre, maritime, aérien ou même spatial. Les signaux électromagnétiques font bien l'objet d'applications militaires depuis la deuxième Guerre mondiale, mais toujours dans un but instrumental, afin de garantir la supériorité opérationnelle lors des conflits armés classiques impliquant la maîtrise des quatre espaces mentionnés précédemment.

Évolution de la tendance

On assiste cependant depuis quelques années à une évolution de la doctrine militaire qui fait du contrôle de l'internet, non seulement un enjeu de sécurité intérieure, mais aussi de sécurité nationale, avec une multiplication des ressources consacrées au développement de capacités défensives et offensives (Deibert, 2010).

Le Pentagone s'est doté en 2011 d'une stratégie visant à traiter les environnements numériques (ou le cyberespace) comme un domaine opérationnel à part entière, en mettant officiellement l'accent sur la protection des réseaux et des infrastructures vitales (DoD, 2011). Cependant, un volet offensif moins médiatisé de cette stratégie semble également connaître une montée en puissance opérationnelle. Le virus informatique Stuxnet, principalement dirigé contre l'effort iranien d'enrichissement militaire de l'uranium, est ainsi attribué par de nombreux experts à une initiative clandestine du gouvernement américain visant à se doter d'un cyber-arsenal, principalement en raison de son degré de sophistication et des ressources nécessaires à la création d'un tel virus.

Mais les États-Unis ne sont pas seuls à développer des capacités militaires dans ce domaine. Au moins 32 autres États (dont le Canada) ont explicitement reconnu développer des capacités opérationnelles offensives et défensives dans le cyberespace (Lewis et Timlin, 2011). Certains pays y consacrent des budgets très significatifs, comme le Royaume Uni, qui prévoit de dépenser un milliard de dollars canadiens sur quatre ans dans le cadre de sa politique militaire de cybersécurité, rendue publique en 2010, alors que le Pentagone dépensera en 2012 un peu plus de 3,2 milliards de dollars US pour ses efforts défensifs et offensifs dans le domaine « cyber » (Sternstein, 2011).

Moteurs de développement

Parmi les moteurs légaux, on mentionnera le droit de la guerre et les conventions internationales, ainsi que les dispositions législatives nationales. Ces divers cadres juridiques vont déterminer (pour les démocraties libérales tout du moins) dans quelle mesure les outils offensifs et défensifs vont pouvoir être officiellement intégrés à l'arsenal militaire, ou au contraire restreints à un usage clandestin. Le Congrès américain

a ainsi donné le 12 décembre 2011 l'autorisation au Pentagone de mener des actions offensives dans le cyberespace dans le cadre des contraintes légales existantes sur l'engagement des troupes américaines dans des conflits armés[15]. Cependant, les instruments juridiques classiques devront probablement être modifiés afin de prendre en compte les spécificités techniques de ces nouvelles capacités offensives, comme la difficulté d'attribution des attaques par exemple. Cette réforme du droit de la guerre ne semble pas avoir encore été engagée.

Les moteurs techniques et économiques s'appuient essentiellement sur des coûts de recherche et de développement d'armes numériques offensives, qui s'avèrent beaucoup plus abordables que ceux des armes conventionnelles. Cette caractéristique les met donc à la portée de puissances militaires intermédiaires, voire marginalisées sur la scène internationale, comme la Corée du Nord ou l'Iran. Ces armes vont s'avérer d'autant plus attractives que la dépendance croissante des infrastructures essentielles envers les réseaux numériques va leur conférer une puissance de nuisance et de destruction indéniable. Cependant, les prédictions qui assimilent ce type d'attaques à un « Pearl Harbor » numérique semblent excessives et sous-estiment ou feignent d'ignorer la résilience de l'écosystème numérique.

Des moteurs stratégiques expliquent également l'attrait que représentent pour certains États la militarisation de l'internet. En effet, l'architecture des infrastructures numériques fait en sorte que le recours à des armes numériques offensives peut toujours faire l'objet de démentis plausibles (plausible deniability), et que l'attribution de responsabilité pour une telle attaque reste impossible à établir avec une certitude absolue (NCIX, 2011). Il s'agit donc là d'une arme opérationnellement très avantageuse, car elle réduit significativement les risques de riposte.

Implications pour la cybersécurité

Tout d'abord, la militarisation de l'internet, si elle n'est pas encadrée à l'échelle internationale par de grands traités modelés sur ceux ayant été utilisés pendant la Guerre froide pour plafonner la production d'armes nucléaires (SALT, START et ABM), risque d'aboutir à une situation analogue de course aux armements. La principale différence verrait se substituer à l'affrontement bilatéral d'alors (USA-URSS) une configuration multilatérale beaucoup plus ouverte et instable, articulée autour des trois acteurs dominants dans ce domaine que sont les États-Unis, la Russie et la Chine (Yannakogeorgos, 2009). Une telle course aux armements ferait peser sur l'écosystème numérique une incertitude et des menaces de destruction dont l'ampleur et les répercussions sont difficilement envisageables.

La multiplication des capacités offensives décrites précédemment va également contribuer à augmenter l'insécurité de l'internet en favorisant la prolifération incontrôlable d'armes numériques toujours plus sophistiquées. Outre l'incertitude et les nouvelles menaces que cette militarisation va faire peser sur les opérateurs civils et

[15] National defense authorization act for fiscal year 2012 (HR 1540), section 954.

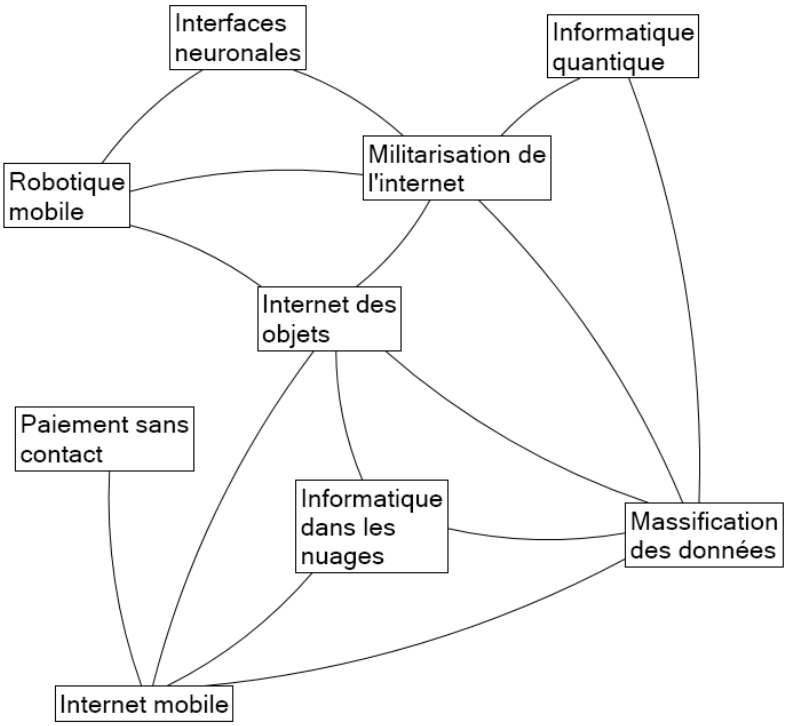
commerciaux, l'architecture ouverte et distribuée d'internet fait en sorte qu'une fois utilisées, ces armes numériques pourront être analysées et recyclées par tous ceux qui disposeront de capacités techniques suffisantes de rétro-ingénierie (reverse engineering). Dans l'écosystème particulier de l'internet, des applications malveillantes élaborées à des fins de sécurité nationale pourront ainsi se retrouver rapidement entre les mains d'intérêts criminels, ce qui a déjà été observé dans le cas du virus Stuxnet. En décembre 2010, des failles encore inconnues (zero day exploits) utilisées par ce virus sont apparues dans l'application malveillante TDL-4, un des plus importants botnets en fonctionnement à l'heure actuelle (Golovanov, 2010);

De manière plus générale, la militarisation de l'internet introduit une confusion dangereuse entre les sphères de la sécurité intérieure et de la sécurité nationale, en considérant que les principaux risques pesant sur l'écosystème numérique relèvent en priorité de la responsabilité des forces armées, et que ces dernières doivent donc déployer des ressources considérables et mobiliser les acteurs privés dans des partenariats caractérisés par le secret pour y faire face. Si cette approche fait le bonheur des sous-traitants du secteur de la défense, qui y voient là une source très lucrative de revenus pour les prochaines années, elle a pour principal défaut d'apporter une réponse unique et disproportionnée à des risques aussi diversifiés que les risques criminels (cyber fraude, harcèlement en ligne, production et consommation de pédopornographie), les risques économiques (téléchargement illégal de contenus protégés par les divers régimes de propriété intellectuelle), les risques liés au cyber espionnage (acquisition par des entités gouvernementales ou privées de secrets détenus par des adversaires ou des compétiteurs) ou les risques militaires, qui impliquent la destruction d'actifs physiques ou informationnels. Sans nier le besoin pour les forces armées d'adapter leurs capacités d'attaque et de riposte aux réalités des environnements numériques actuels et futurs, une réflexion devrait être initiée dans les meilleurs délais afin de délimiter le rôle qu'elles devront jouer dans l'écosystème de la cybersécurité, aux côtés d'autres acteurs tout aussi importants comme les organisations policières, la sécurité privée, les entreprises du secteur des hautes technologies, les ONG, les autorités réglementaires et judiciaires, et bien entendu, les utilisateurs. Si ce débat n'est pas mené, cette militarisation risque de fragiliser encore un peu plus l'écosystème numérique et de le déstabiliser plutôt que de le rendre plus résilient face aux diverses menaces énumérées précédemment.

Conclusion et recommandations

Dans cette dernière section, on traitera de plusieurs thèmes transversaux qui se dégagent des neuf tendances identifiées dans le rapport et de leurs implications pour la cybersécurité, en formulant également quelques recommandations générales qui doivent néanmoins être considérées avec prudence, compte tenu de la nature prospective des problèmes abordés.

Il faut tout d'abord signaler que ces tendances ne doivent pas être considérées séparément les unes des autres, même si nous avons pris le parti de les étudier de cette manière afin d'en faciliter la description et l'analyse en termes de moteurs de développement et d'impacts sur la sécurité de l'écosystème numérique. Ces neuf tendances sont techniquement et socialement interdépendantes, certaines entretenant même entre elles des relations symbiotiques (comme l'internet mobile et les paiements sans contact). D'autres vont converger afin d'offrir de nouveaux services aux individus et aux entreprises, tel l'internet des objets qui va bénéficier des avancées scientifiques de la massification des données pour améliorer la productivité des entreprises. Cette convergence est déjà en marche, puisque selon IDC, les deux tiers des applications de l'internet mobiles développées en 2012 intègreront des capacités analytiques offertes par des entreprises en pointe dans la massification des données, et la moitié des applications seront connectées ou intégrées à des plateformes d'informatique dans les nuages (Gens, 2011 : 9).



Le diagramme ci-dessus représente les interdépendances identifiées dans la littérature consultée, sans prétendre à l'exhaustivité, dans la mesure où de nouveaux liens apparaîtront certainement au gré des innovations perturbatrices qu'il est encore difficile d'anticiper. La principale conséquence de cette interdépendance, outre la mise en lumière de la complexité structurelle inhérente à l'écosystème numérique, est de nous sensibiliser au fait que toute politique ou stratégie de cybersécurité ne peut s'avérer réellement efficace qu'en adoptant une vue d'ensemble des diverses tendances et en surveillant constamment l'évolution de leurs interactions réciproques, puisque leur processus de maturation respectif connaît de fortes variations.

Recommandation no. 1 : concevoir et déployer une méthodologie et des outils de veille permanents dont l'objectif sera de suivre l'évolution de l'écosystème numérique, d'en cartographier les divers acteurs, les interactions, et d'évaluer les implications de ces transformations sur la cybersécurité.

Le risque réglementaire à éviter dans ce type de configuration est alors qu'une prise en compte séparée de chacune des tendances identifiées conduise à une fragmentation des régimes réglementaires (regulatory regimes) et des stratégies de gestion des risques et nuise à la cybersécurité, là où une intégration s'avère indispensable, comme on vient de le souligner.

Recommandation no. 2 : aligner les régimes réglementaires applicables aux diverses infrastructures, applications et contenus avec les ressources et les stratégies mises en œuvre par un nombre croissant d'acteurs gouvernementaux, ainsi que leurs partenaires privés, afin de déceler rapidement les risques numériques émergents et limiter leur impact sur un écosystème en constante évolution.

Trois caractéristiques semblent partagées par les diverses tendances analysées dans les pages précédentes. Il s'agit de l'augmentation exponentielle du nombre d'entités connectées, de la quantité des données traitées par ces entités dans l'écosystème numérique, et de la circulation accrue de ces mêmes données. Ces trois propriétés auront pour conséquence de multiplier les points et les opportunités de compromission permettant d'attaquer les systèmes et des données les plus sensibles, ce qui fragilisera l'équilibre de l'écosystème numérique sans la mise en œuvre de stratégies adaptées. Cette expansion et cette diversification de l'écosystème numérique devront donc s'accompagner d'innovations institutionnelles et réglementaires qui viendront dans certains cas bousculer les pratiques et les juridictions établies, et seront confrontées à des manifestations de résistance plus ou moins intransigeantes.

Recommandation no. 3 : engager un exercice de consultation et de réflexion approfondi destiné à formuler des propositions sur la restructuration des institutions gouvernementales existantes ou la création de nouvelles institutions, afin d'adapter les capacités d'intervention et de coordination du gouvernement canadien à des besoins nouveaux.

En effet, il faut rappeler que les concepteurs de l'internet n'ont jamais envisagé que celui-ci serait un jour amené à transmettre une telle quantité de données (Hourcade et

al., 2009 : iv), ni que ces données occuperaient une place aussi importante dans le fonctionnement des organisations et la vie quotidienne des individus. Il en résulte que chaque nouvelle tendance identifiée dans ce rapport vient complexifier un écosystème numérique global déjà confronté à des défis énormes en matière de capacités techniques, de résilience et de sécurité. Toute technologie perturbatrice entraîne en effet l'apparition dans l'écosystème numérique de nouveaux acteurs et la disparition des entreprises ou des technologies n'ayant pas réussi à s'adapter à cette évolution. Dans une perspective de cybersécurité, cette instabilité rend les efforts de coordination plus ardus, en introduisant constamment de nouveaux acteurs organisationnels, dont les capacités et la volonté de contribuer à la sécurité de tout l'écosystème sont difficiles à évaluer (et à mobiliser) pour leurs partenaires et les autorités régulatrices.

La transformation de la notion de vie privée risque en particulier de générer un certain nombre de tensions entre les défenseurs du régime protecteur existant (du moins au Canada et en Europe), les organisations manifestant un appétit insatiable pour les données personnelles de leurs clients, usagers ou employés, et les autorités chargées de sécuriser l'écosystème numérique. Si l'on peut s'attendre à ce que les usagers continuent à valoriser la protection de la vie privée et à exiger que les organisations publiques et privées utilisent leurs informations personnelles avec discernement, il semble difficilement justifiable de s'appuyer sur des outils réglementaires imaginés durant les années 1970 et 1980 pour répondre aux besoins des années 2020. L'évolution de la technologie doit s'accompagner d'une réflexion moins dogmatique et plus empirique sur les normes sociales émergentes en matière de vie privée et sur les pratiques socialement acceptables et éthiquement responsables qui en découlent. Il n'est pas concevable que de grands groupes comme Facebook ou Google déterminent unilatéralement (et en fonction de leurs seuls intérêts commerciaux) quelles seront les limites de la vie privée en 2020, mais faire reposer la préservation de cette notion, centrale dans une société de l'information, sur une architecture juridique héritée de l'ère industrielle est tout aussi insatisfaisant. Cela nous semble d'autant plus vrai que la convergence de l'informatique traditionnelle et de la bioinformatique, déjà mise en lumière avec les interfaces neuronales, va élargir les réflexions sur la vie privée et la cybersécurité aux domaines de la biologie et de la santé et poser des questions délicates en matière d'éthique et de droits individuels.

Recommandation no. 4 : intensifier les recherches empiriques sur les transformations des risques, des normes et des pratiques reliées à la protection de la vie privée dans l'écosystème numérique.

Les implications soulevées dans ce rapport concernent principalement la cybersécurité, mais l'omniprésence dans notre vie quotidienne des outils numériques constamment connectés, via l'internet mobile, l'internet des objets ou encore les paiements sans contact, ainsi que leur accès quasiment illimité à nos données personnelles, vont accélérer la convergence des problèmes de cybersécurité avec les problèmes de sécurité humaine ou physique 'classiques'. Une meilleure coordination des acteurs chargés de la prévention et de l'application de la loi dans des sphères de sécurité très différentes va

donc s'imposer. La distinction actuelle entre sécurité humaine et cybersécurité perdant de son sens, les institutions de sécurité locales (principalement les services de police) qui ne seront pas capable d'évoluer et de redéfinir leur mandat afin d'y intégrer ces deux dimensions verront certainement leur légitimité remise en question par leurs administrés.

Recommandation no. 5 : accentuer les initiatives de coordination et de transferts de connaissances des autorités nationales et provinciales afin d'accélérer et de standardiser le développement des capacités locales.

Par ailleurs, même si nous avons analysé ces neuf tendances selon une perspective de cybersécurité, il faut rappeler que l'écosystème numérique n'est pas seulement devenu indispensable au bon fonctionnement de l'économie (via l'intégrité des transactions financières par exemple), mais qu'il joue également un rôle déterminant en ce qui concerne les efforts de recherche menés dans d'autres secteurs technologiques stratégiques comme les biotechnologies, les nano-technologies, ou encore les matériaux intelligents (Newton et Pfleeger, 2006 : 188). À ce titre, la sécurité et la stabilité de l'écosystème numérique constituent ljes conditions indispensables au maintien de la compétitivité technologique et des capacités d'innovation du Canada.

Cela explique pourquoi il sera impératif de trouver le point d'équilibre entre, d'une part, le renforcement de la cybersécurité, et d'autre part, le maintien des capacités d'innovation technique et de la compétitivité économique canadienne. Comme nous l'avons déjà mentionné, la tendance à la militarisation de l'internet constitue selon nous un facteur de rupture de ce délicat équilibre. La théorie de la régulation progressive (responsive regulation) d'Ayres et Braithwaite (1992), qui imagine une gradation du niveau coercitif des mesures de contrôle en fonction de la sévérité des risques et du degré de coopération des acteurs impliqués, nous semble ici bien mieux adaptée à la recherche de cet équilibre.

Nous n'avons abordé cette question pour aucune des neuf tendances, en raison de la nature prospective de ce rapport, mais on peut logiquement imaginer qu'en cas d'incapacité des gouvernements démocratiques à proposer et à mettre en œuvre des mécanismes de gouvernance et de contrôle satisfaisants de la cybersécurité, à l'échelle locale, nationale ou internationale, la nature ouverte et distribuée des technologies décrites dans ce rapport, ainsi que leurs coûts d'accès relativement abordables, pourraient inciter des individus ou des collectifs d'hacktivistes à promouvoir des initiatives d'autodéfense et de justice privée (vigilantism), ce qui augmenterait d'autant plus l'insécurité et l'anarchie régnant aux marges de l'écosystème numérique.

Enfin, il serait contreproductif de ne prendre en considération que les risques dérivés des tendances examinées dans ce rapport. Comme nous l'avons illustré dans le cas des interfaces neuronales directes ou de l'informatique quantique, certaines de ces technologies recèlent également un fort potentiel en matière d'amélioration de la sécurité des canadiens, et ces caractéristiques duales doivent être pleinement intégrées à toute planification en matière de cybersécurité.

Références

Acquisti, A., Gross, R. et F. Stutzman (2011), "Faces of Facebook : Privacy in the age of augmented reality", *Black Hat 2011*, 3-4 août, Las Vegas, accessible en ligne à http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf, consulté le 26 décembre 2011.

Albanesius, C. (2011), "Cyber crime costs $114B per year, mobile attacks on the rise", *PCmag.com*, 7 septembre, accessible en ligne à http://www.pcmag.com/article2/0,2817,2392570,00.asp, consulté le 28 décembre 2011.

Alpeyev, P., Galante, J. et M. Yasu (2011), "Amazon.com server said to have been used in Sony Attack", *Bloomberg*, 14 mai, accessible en ligne à http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html , consulté le 20 décembre 2011.

Asthana, P. (2011), "Big Data and Little Data", *Forbes.com*, accessible en ligne à http://www.forbes.com/sites/dell/2011/10/31/big-data-and-little-data/print/, consulté le 26 décembre 2011.

Ayres, I. et J. Braithwaite (1992), *Responsive regulation: Transcending the regulation debate*, Oxford University Press: Oxford.

Balaba, D. (2009), "NFC mobile payment: A new front in the security battle?", *Cards & Payments*, vol. 22, no. 7, 14-17.

Banerjee S., Bolze J., McNamara, J. et K. O'Reilly (2011), "How big data can fuel bigger growth", *Outlook*: *The online journal of high-performance business*, no. 3, accessible en ligne à http://www.accenture.com/us-en/outlook/Pages/outlook-journal-2011-how-big-data-fuels-bigger-growth.aspx, consulté le 26 décembre 2011.

Benkler, Y. (2006), *The wealth of networks: How social production transforms markets and freedoms*, Yale University Press: New Haven.

Bicchi, A., Fagiolini, A. Et L. Pallottino (2010), "Toward a society of robots: Behaviors, misbehaviors and security", *IEEE Robotics and Automation Magazine*, décembre, pp. 26-36.

Biggs, S. et S. Vidalis (2009), "Cloud computing : The impact on digital forensic investigations", *International Conference for Internet Technologies and Secured Transactions*, 9-12 novembre, Londres.

Bloomberg (2010), "In China, investment to expand E-payments", *New York Times*, 10 mars, B6.

Butler Curtis, W., Heckman, C. et A. Thorp (2010), *Cloud computing : eDiscovery issues and other risk*, Orrick: Washington DC.

Boyd, D. et K. Crawford (2011), "Six provocations for big data", *A decade in internet time: Symposium on the dynamics of the internet and society*, 21 septembre, Oxford Internet Institute: Oxford.

Brown, K. (2011), "IBM 5 in 5: Mind reading is no longer science fiction", *IBM Research Blog*, 19 décembre, accessible en ligne à

http://ibmresearchnews.blogspot.com/2011/12/mind-reading-is-no-longer-science.html, consulté le 28 décembre 2011.
Catteddu, D. et G. Hogben (2009), *Cloud computing : Benefits, risks and recommendation for information security*, ENISA: Heraklion.
Cave, J., Van Oranje, C., Schindler, R., Shehabi, A., Brutscher, Ph-B. et N. Robinson (2009), *Trends in connectivity technologies and their socio-economic impacts*, RAND Europe: Cambridge.
Chen, Y., Paxson, V. et R. Katz (2010). *What's new about cloud computing security?*, Technical report no. UCB/EECS-2010-5, Electrical Engineering and Computer Sciences Department - University of California at Berkeley: Berkeley.
Choo, K.R. (2010), "Cloud computing: Challenges and future directions", *Trends & Issues in Crime and Criminal Justice*, no. 400, Australian Institute of Criminology: Canberra.
Christensen, C. (1997), *The innovator's dilemma: When new technologies cause great firms to fail*, Harvard Business School Press: Boston.
Chui, M., Löffler, M. et R. Roberts (2010), « The internet of things", *McKinsey Quaterly*, no. 2, accessible en ligne à https://www.mckinseyquarterly.com/High_Tech/Strategy_Analysis/The_Internet_of_Things_2538, consulté le 27 décembre 2011.
Clausen, J. (2009), "Man, machine and in between", *Nature*, vol. 457, 1080-1081.
Cloud Security Alliance (2010), *Top threats to cloud computing V1.0*, CSA.
Cohen, L. et M. Felson (1979), "Social change and crime rate trends: A routine activity approach", *American Sociological Review*, vol. 44, no. 4, 588-608.
Commissariat à la Protection de la Vie Privée du Canada (2011), *Rapport sur la consultation de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*, CPVPC : Ottawa.
Costa, D., Cavalcanti, J. et D. Costa (2011), "A Cambrian explosion of robotic life", *Management Science and Engineering*, vol. 5, no. 1, 98-105.
Damballa (2011), *Damballa Threat Report: First half 2011*, Damballa: Atlanta.
Deibert, R. (2010), "Militarizing cyberspace", *Technology Review*, Juillet/Août, accessible en ligne à http://www.technologyreview.in/printer_friendly_article.aspx?id=25570, consulté le 20 janvier 2012.
Demetriades, A., Demetriades Ch., Watts, C. et K. Ashkan (2010), "Brain-machine interface: The challenge of neuroethics", *The surgeon*, vol. 8, 267-269.
De Villiers, C. (2010), *A case study to examine the use of SMS-based transactional alerts in the banking sector in South Africa*, MBA research report, University of Stellenbosch: Stellenbosch.
DoD (2011), *Department of defense strategy for operating in cyberspace*, Department of Defense: Washington DC.
Dumbill, E. (2011), "Five big data predictions for 2012", *O'Reilly Radar*, 14 décembre, accessible en ligne à http://radar.oreilly.com/2011/12/5-big-data-predictions-2012.html, consulté le 26 décembre 2011.
Evans, D. (2011), *The internet of things: How the next evolution of the internet is changing everything*, Cisco Internet Business Solutions Group: San Jose.

Fenn, J. et H. LeHong (2011), *Hype cycle for emerging technologies, 2011*, Gartner: Stamford.

Foresight Horizon Scanning Centre (2010), *Technology and innovation futures: Technology annex,* Department for Business Innovation & Skills: Londres.

Freedman, S. et J. A. Adams (2011), "Filtering data based on human-inspired forgetting", IEEE Transactions on Systems, Man, and Cybernetics—Part B, vol. 41, no. 6, 1544-1555.

Gantz, J. et D. Reinsel (2010), *The digital universe decade – Are you ready?*, IDC: Framingham, accessible en ligne à http://www.emc.com/collateral/analyst-reports/idc-digital-universe-are-you-ready.pdf, consulté le 20 décembre 2011.

Gantz, J. et D. Reinsel (2011), *Extracting value from chaos*, IDC: Framingham, accessible en ligne à http://idcdocserv.com/1142, consulté le 25 décembre 2012.

Gens, F. (2011), *Top 10 predictions – IDC predictions 2012: Competing for 2020*, IDC: Framingham.

Giles, J. (2010), "Sneaky app shows potential for smartphone botnets", *New Scientist*, 5 mars, accessible en ligne à http://www.newscientist.com/blogs/shortsharpscience/2010/03/mobile-botnets-threaten-smartp.html?DCMP=OTC-rss&nsref=online-news, consulté le 27 décembre 2011.

Gillmor, D. (2012), "The invention of Waterloo", *The Walrus*, janvier, accessible en ligne à http://www.walrusmagazine.com/articles/2012.01-cities-the-invention-of-waterloo/, consulté le 9 janvier 2012.

Golovanov, S. (2010), "TDL4 starts using 0-day vulnerability", *Securelist Blog*, 7 décembre, accessible en ligne à http://www.securelist.com/en/blog/337/TDL4_Starts_Using_0_Day_Vulnerability , consulté le 2 janvier 2012.

Gruman, G. (2010), "Tapping into the power of big data", *Technology Forecast*, no. 3, 4-13.

GSMA (2011), *Connected life*, GSMA: Londres.

Helmbrecht, U., Purser, S. et Klejnstrup, R. (2011), *Cyber security : Future challenges and opportunities*, ENISA : Heraklion.

Hourcade, J.-C., Neuvo, Y., Posch, R., Saracco, R., Sharpe, M. et W. Wahlster (2009), *Future internet 2020 : Visions of an industry expert group*, Commission Européenne: Bruxelles.

IBM (2011), *The 2011 IBM tech trends report*, IBM: Armonk.

ITU (2010), *Measuring the information society*, International Telecommunication Union: Genève.

Jackson, J. (2011), "NSA extends label-based security to big data stores", *Computerworld*, 6 septembre, accessible en ligne à http://www.computerworld.com/s/article/9219743/NSA_extends_label_based_security_to_big_data_stores, consulté le 27 décembre 2011.

Jonas, J. (2011), "Privacy by design (PbD): Confessions of an architect", *Privacy by design: Time to take control*, 28 janvier, Toronto, accessible en ligne à

http://privacybydesign.ca/content/uploads/2010/04/Jonas-PbD-Confessions-of-an-Architect-2011.pdf, consulté le 28 janvier 2012.
Kaikkonen, A. (2009), "Mobile Internet: past, present, and the future", *International Journal of Mobile Human Computer Interaction*, vol. 1, no. 3, 29-45.
Kaufman, L. (2009), "Data security in the world of cloud computing", *IEEE Security and Privacy Archive*, vol. 7, no. 4, 61-64.
Killias, M. (2006), "The opening and closing of breaches: A theory on crime waves, law creation and crime prevention", *European Journal of Criminology*, vol. 3, no. 11, 11-31.
Klein, A. (2006), "Gunshot sensors are giving DC police jump on suspects", *The Washington Post*, 22 octobre, accessible en ligne à http://www.washingtonpost.com/wp-dyn/content/article/2006/10/21/AR2006102100826.html, consulté le 20 janvier 2012.
Kunur, P. (2011), "What are mobile payments?", *Advertising Age*, vol. 82, no. 9, 42.
Lane, A. (2011), "Big data and bad security", *Darkreading.com*, 16 novembre, accessible en ligne à http://www.darkreading.com/database-security/167901020/security/news/231903153/big-data-and-bad-security.html, consulté le 27 décembre 2011.
Lasar, M. (2011), "Dutch traffic cops use Tom Tom GPS data to nail speeders", *Ars Technica*, 28 avril, accessible en ligne à http://arstechnica.com/tech-policy/news/2011/04/dutch-traffic-cops-use-tomtom-gps-data-to-nail-speeders.ars, consulté le 26 décembre 2011.
Lewis, J. et K. Timlin (2011), *Cybersecurity and cyberwarfare : Preliminary assessment of national doctrine and organization*, Centre for Strategic and International Studies: Washington DC.
Leyden, J. (2010), "Vodafone Spain admits 3,000 smartphones shipped with Mariposa", *The Register*, 19 mars, accessible en ligne à http://www.theregister.co.uk/2010/03/19/voda_spain_mariposa_latest/, consulté le 27 décembre 2011.
Luo, R. et Y. W. Perng (2011), "Advances of mechatronics and robotics: Challenges and perspectives", *IEEE Industrial Electronics Magazine*, septembre, p. 27-34.
Manyika, J., Chui, M., Brown B., Bughin, J., Dobbs, R., Roxburgh C. et A. Byers (2011), *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute: Washington DC, accessible en ligne à http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation, consulté le 26 décembre 2011.
Mell, P. et T. Grance (2011), The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology, US Department of Commerce: Washington DC.
Ministère de l'Économie, des Finances et de l'Industrie (MEFI) (2011), *Technologies Clés 2015*, MEFI : Paris.

Nash, K. (2011), “Ten tech trends reshaping your world”, *CIO.IN*, 27 septembre, accessible en ligne à http://www.cio.in/article/ten-tech-trends-reshaping-your-world, consulté le 15 décembre 2011.

NCIX (2011), *Foreign spies stealing US economic secrets in cyberspace*, National Counterintelligence Executive: Washington DC.

Newton, E. et S. L. Pfleeger (2006), “Appendix D: Information technology trends to 2020”, in Silberglitt, R., Anton, P., Howell, D. et A. Wong (eds), *The global technology revolution 2020, in-depth analyses: Bio/Nano/Material/Information trends, drivers, barriers and social implications*, Rand National Security Research Division: Santa Monica, 179-189.

Nishida, T. et R. Nishida (2007), « Socializing artifacts as a half Mirror of the mind”, *AI & Society*, vol. 21, 548-566.

Ntalampiras, S., Potamitis, I. et N. Fakotakis (2009), “A portable system for robust acoustic detection of atypical situations”, *17th European Signal Processing Conference*, 24-28 août, Glasgow.

Ondrus, J. et Y. Pigneur (2009), “Near field communication: an assessment for future payment systems”, *Information Systems and E-Business Management*, vol. 7, no. 3, 347-361.

Palmer, J. (2009), “EU funding push in blue-sky tech”, *BBC News*, 21 avril, accessible en ligne à http://news.bbc.co.uk/2/hi/technology/8010075.stm, consulté le 28 janvier 2012.

Poulsen, K. (2010), “Hacker disables more than 100 cars remotely”, *Wired Threat Level Blog*, 17 mars, accessible en ligne à http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/, consulté le 27 décembre 2011.

QISTEP (Quantum Information Science and Technology Experts Panel) (2004), *A quantum information science and technology roadmap – Part 1: Quantum computation*, Advanced Research and Development Activity: Fort Meade.

Raibert, M., Blankespoor, K., Nelson, G., Playter, R. et The BigDog Team (2008), *BigDog, the rough terrain quadruped robot*, Boston Dynamics: Waltham.

Räty, T. (2010), “Survey on contemporary remote surveillance systems for public safety”, *IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews*, vol. 40, no. 5, 493-515.

Rocha, F., Abreu, S. et M. Correia (2011), “The final frontier: Confidentiality and privacy in the cloud”, *IEEE Computer*, vol. 44, n. 9, 44-50.

Rochet, J.-C. et J. Tirole (2003), “Platform competition in two-sided markets”, *Journal of the European Economic Association*, vol. 1, no. 4, 990-1029.

Roman, R., Najera, P. et J. Lopez (2011), “Securing the internet of things”, *IEEE Computer*, vol. 44, no. 9, 51-58.

Reilly, D., Wren, C. et T. Berry (2010), “Controlling data in the cloud: outsourcing computation without outsourcing control”, *International Conference for Internet technology and Secured Transactions*, 8-11 novembre, Londres.

Salvini, P., Laschi, C. et P. Dario (2010a), “Design for acceptability: Improving robots’ coexistence in human society”, *International Journal of Social Robotics*, vol. 2, no. 4, 451-460.

Salvini, P., Teti, G., Spadoni, E., Frediani, E., Boccalatte, S., Nocco, L., Mazzolai, B., Laschi, C., Comandée, G., Rossic, E., Carrozzac, P. et P. Dario (2010b), “An investigation on legal regulations for robot deployment in urban areas: A focus on Italian law”, A*dvanced Robotics*, vol. 24, 1901–1917.

Sanders, B. (2012), “Quantum cryptography for information-theoretic security”, in A. Vaseashta et al. (eds.), *Technological innovations in sensing and detection of chemical, biological, radiological, nuclear threats and ecological terrorism*, Springer: Dordrecht, 335-343.

Shay, C. (2010), “China’s great (quantum) leap forward”, *Time Magazine*, 9 septembre, accessible en ligne à http://www.time.com/time/world/article/0,8599,2016687,00.html, consulté le 28 janvier 2012.

Silberglitt, R., Anton, P., Howell, D. et A. Wong (2006), *The global technology revolution 2020, in-depth analyses: Bio/Nano/Material/Information trends, drivers, barriers and social implications*, Rand National Security Research Division: Santa Monica.

Spies, T. (2008), *Format preserving encryption - white paper*, Voltage Security: Cupertino, accessible en ligne à http://157.238.212.45/pdf/Voltage-Security-WhitePaper-Format-Preserving-Encryption.pdf, consulté le 27 décembre 2011.

Sternstein, A. (2011), “Defense spending for cybersecurity is hard to pin down”, *Nextgov*, 29 mars, accessible en ligne à http://www.nextgov.com/nextgov/ng_20110329_4961.php?oref=mostread, consulté le 20 janvier 2012.

Tata (2011), *The TCS COIN emerging technology trends report 2011*, Tata Consultancy Services: Mumbai.

The Future Laboratory (2011), *Cybercrime futures: an independent report for AVG technologies*, The Future Laboratory: Londres.

Thomas, K. (2011), “Cloud computing used to hack wireless passwords”, *PC World Business Centre*, 10 janvier, accessible en ligne à http://www.pcworld.com/businesscenter/article/216434/cloud_computing_used_to_hack_wireless_passwords.html , consulté le 16 décembre 2011.

Wang, Y. et T.-P. Jung (2011), *A collaborative brain-computer interface for improving human performance*, *PloS ONE*, vol. 6, no. 5, 1-11.

Webb, J. (2011), “How the cloud helps Netflix”, *O’Reilly Radar*, 11 mai, accessible en ligne à http://radar.oreilly.com/2011/05/netflix-cloud.html, consulté le 15 janvier 2012.

Webbmedia Group (2011), *2012 tech trends - Looking ahead: 30 trends that will impact your business in 2012*, Webbmedia Group: Baltimore.

Weinberger, S. (2009), “Spooky research cuts”, *Nature*, vol. 459, juin, 625.

Yannakogeorgos, P. A. (2009), *Technogeopolitics of militarization and security in cyberspace*, Thèse de doctorat, Rutgers University: Newark.

Yuan, L. et P. Barker (2011), *Literature scan: Technology forecasts*, JISC Observatory: Londres.

Annexe 1. Les 21 rapports et sites de prospective consultés

1) Gartner's 2011 Hype Cycle Special Report
2) Institute for the Future's Technology Horizons
3) GSM Association's Connected Life Report
4) UK Technology and Innovation Futures: Growth Opportunities for the 2020s
5) IBM's 2011 Tech Trends Report
6) RAND's report on Trends in Connectivity Technologies
7) Tata consultancy services' Co-innovation Network
8) Ministère français de l'industrie (MFI) – Technologies clés 2015
9) PWC Technology Forecast (http://www.pwc.com/us/en/technology-forecast)
10) Battelle Memorial Institute (http://www.battelle.org/SPOTLIGHT/tech_forecast/technology2020.aspx)
11) JISC Observatory Forecasting Literature Review 2011 (http://blog.observatory.jisc.ac.uk/2011/05/16/technology-forecasting-literature-review/)
12) TechCast (http://www.techcast.org/Forecasts.aspx?ID=22)
13) Accenture's Technology Vision 2010
14) European Future Internet Portal (http://www.future-internet.eu/activities/fp7-projects.html)
15) Deloitte's Technology Trends
16) Ovum (http://about.datamonitor.com/media/archives/5153)
17) Technology Review Emerging Technologies (http://www.technologyreview.com/tr10/
18) Rand Global Technology Revolution 2020
19) Webbmedia Group 2012 Tech Trends
20) IDC Predictions 2012: Competing for 2020
21) European Commission Future Internet 2020