EN QUÊTE DE LA CYBERCONFIANCE

Union internationale des télécommunications

EN QUÊTE DE LA CYBERCONFIANCE

Par le Dr Hamadoun I. Touré

Secrétaire général

de l'Union internationale des télécommunications

et le

Groupe permanent de surveillance sur la sécurité de l'information

World Federation of Scientists

NOVEMBRE 2014

Mention légale

Les différent auteurs conservent leurs droits d'auteur pour leur travail. Les sources tierces sont citées, s'il y a lieu. L'Union internationale des télécommunications (UIT) n'est pas responsable du contenu des sources externes, y compris des sites web externes auxquels il est fait référence dans la présente publication.

L'UIT, de même que toute personne agissant en son nom, dégage toute responsabilité pour l'utilisation qui pourrait être faite des informations contenues dans la présente publication.

Avertissement

Les chapitres de la présente publication représentent les opinions de chacun de leurs auteurs, qui ne sont pas nécessairement approuvées par l'organisation qui les emploie ou à laquelle ils sont affiliés et qui n'ont pas vocation à représenter ses opinions. Le renvoi à des pays, des sociétés, des produits, des initiatives ou des directives spécifiques ou leur mention n'implique aucunement que l'UIT, les auteurs, ou toute autre organisation à laquelle les auteurs sont affiliés, les avalisent ou les recommandent à titre préférentiel par rapport à tout autre pays, société, produit, initiative ou directive similaire non mentionnée.

Remerciements

Le Secrétaire général de l'UIT et la World Federation of Scientists tiennent à remercier Henning Wegener et tous les auteurs qui ont contribué à faire connaître leurs vues sur ce sujet, d'une importance croissante pour le monde entier. Le Secrétaire général exprime aussi sa reconnaissance au Professeur Antonino Zichichi, Président de la WFS, et adresse ses sincères remerciements à Marco Obiso, qui a dirigé et coordonné la présente publication et à l'équipe de l'UIT travaillant sur la cybersécurité, en particulier Alex Gamero Garrido, Aliya Abdul Razack, Despoina Sareidaki, Anthony Drummond, Preetam Maloor et Rosheen Awotar-Mauree, ainsi qu'à tous les collaborateurs de l'UIT et de la WFS sans l'aide desquels la présente publication n'aurait pu paraître.

Les lecteurs qui auraient des commentaires à faire voudront bien s'adresser à l'équipe cybersécurité de l'Union internationale des télécommunications cybersecurity@itu.int.

TABLE DES MATIÈRES

Page

A propos de l'Union internationale des télécommunications

L'Union internationale des télécommunications (UIT) est la principale institution des Nations Unies chargée des questions relatives aux technologies de l'information et de la communication (TIC) et l'instance mondiale où pouvoirs publics et secteur privé se rencontrent pour développer les réseaux et les services.

Dans le prolongement du Sommet mondial sur la société de l'information (SMSI) et de la Conférence de plénipotentiaires de 2006 de l'UIT, l'Union a, entre autres, pour tâche fondamentale de renforcer la confiance et la sécurité dans l'utilisation des TIC. Les chefs d'Etat et de gouvernement, ainsi que d'autres dirigeants internationaux participant au SMSI, de même que les Etats Membres de l'UIT, ont chargé l'Union d'agir concrètement en vue de réduire les risques et vulnérabilités liés à la société de l'information. Pour s'acquitter de ce mandat, le Dr Hamadoun I. Touré, Secrétaire général de l'UIT, a lancé en 2007 le Programme mondial cybersécurité (GCA) – cadre de la coopération internationale multi-parties prenantes visant à bâtir des synergies avec des partenaires actuels et futurs et à collaborer avec des initiatives en vigueur ou en projet. Ce programme est axé sur les cinq grands thèmes de travail suivants: mesures juridiques, mesures techniques et de procédure, structures organisationnelles, renforcement des capacités et coopération internationale.

Citons aussi certaines initiatives fondamentales visant à aider les Etats Membres à renforcer leurs capacités en matière de cybersécurité, sous l'égide du GCA et avec l'appui de partenaires internationaux:

- Le programme relatif aux équipes nationales CIRT (équipes d'intervention en cas d'incident informatique), aux termes duquel les activités de ces équipes et leur mise en oeuvre sont évaluées et des exercices régionaux de cybersécurité sont menés à bien en réponse à la demande d'Etats Membres.
- La création de centres régionaux de cybersécurité ayant pour objet d'accélérer et de renforcer la coopération, la coordination et la collaboration régionales face à la progression des cybermenaces.
- Le projet UIT "Renforcer la cybersécurité dans les pays les moins avancés", qui vise à aider les PMA à renforcer leurs capacités, leur préparation, leurs compétences et leurs connaissances en matière de cybersécurité.
- L'Indice de cybersécurité dans le monde (GCI), qui mesure le niveau de cybersécurité dans chaque pays. Son objet est d'inciter les pays à intensifier leurs efforts dans le domaine de la cybersécurité. A terme, le but est d'encourager une culture mondiale de la cybersécurité et de l'intégrer au coeur des technologies de l'information et de la communication.

A propos de la World Federation of Scientists

La World Federation of Scientists (WFS) a été fondée à Erice (Sicile), en 1973, par un groupe d'éminents scientifiques dirigé par Isidor Isaac Rabi et Antonino Zichichi. Depuis lors, de nombreux autres scientifiques sont devenus membres de la Fédération, notamment T. D. Lee, Laura Fermi, Eugene Wigner, Paul Dirac et Piotr Kapitza.

La WFS est une association ouverte à tous, qui compte aujourd'hui plus de 10 000 membres scientifiques de 110 pays. Tous partagent les mêmes objectifs et idéaux et adhèrent volontairement aux principes de la Fédération. Celle-ci encourage la collaboration internationale en matière scientifique et technologique entre les scientifiques et les chercheurs de toutes les régions du monde – Nord, Sud, Est et Ouest. La Fédération et ses membres ont pour ambition de favoriser le libre-échange de l'information et de faire en sorte que les découvertes et progrès scientifiques ne soient plus le privilège de quelques-uns. L'objectif est de mettre ces connaissances à la portée de tous les habitants de la planète, de sorte que chacun puisse bénéficier des avantages du progrès scientifique.

La création de la World Federation of Scientists a été rendue possible par l'existence, à Erice, d'un centre de culture scientifique portant le nom du physicien Ettore Majorana***, la Fondation et centre de culture scientifique Ettore Majorana***. Ce centre, que l'on appelle "l'Université du troisième millénaire", est devenu un pôle d'enseignement mondial. Depuis sa création en 1963, ce Centre a organisé 123 ateliers et 1 497 stages pour 103 484 participants (dont 125 lauréats du Prix Nobel), venant de 932 universités et laboratoires de 140 pays.

Il a été le précurseur de la World Federation of Scientists et de son action face aux situations d'urgence planétaires. La World Federation of Scientists a identifié 15 catégories de **situations d'urgence planétaires** et entrepris d'organiser la riposte. L'un de ses principaux résultats a été l'élaboration de la **Déclaration d'Erice**, rédigée en 1982 par Paul Dirac, Piotr Kapitza et Antonino Zichichi. Cette déclaration énonçait clairement les idéaux de la Fédération et présentait un ensemble de propositions visant à les mettre en pratique. Un autre tournant a été la tenue d'une série de séminaires internationaux sur la guerre nucléaire, qui ont contribué pour beaucoup à éloigner le danger d'une catastrophe nucléaire planétaire et par la même, à accélérer la fin de la guerre froide. En 1986, grâce à l'action d'un groupe d'éminents scientifiques (dont la plupart étaient membres de la WFS), le **Laboratoire mondial du Centre international de culture scientifique** a été créé à Genève pour aider à atteindre les objectifs définis dans la déclaration d'Erice.

La WFS a établi en 2001 son Groupe permanent de surveillance sur la société de l'information (PMP). Le rapport de ce groupe ("*Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*") est l'un des principaux documents

présentés par la société civile au Sommet mondial sur la société de l'information (SMSI) des Nations Unies, dont la première phase s'est tenue à Genève en 2003. Ce Groupe, qui a publié un grand nombre de documents sur la cybersécurité et la cyberguerre, présente régulièrement des questions liées à la sécurité de l'information dans le cadre des sessions plénières de la WFS qui se tiennent chaque année au mois d'août à Erice. En août 2009, le Groupe permanent a été tellement inquiet des risques qu'une cyberguerre pouvait avoir pour la société et des dégâts et des souffrances inutiles qu'elle pouvait engendrer qu'il a rédigé la **Déclaration d'Erice sur les principes de la cyberstabilité et de la cyberpaix**. Cette déclaration a été adoptée par la plénière de la WFS à l'occasion de la 42ème session des Séminaires internationaux sur les situations d'urgence planétaires, réunie à Erice le 20 août 2009.

Cette déclaration, qui a été communiquée à tous les Etats Membres de l'Organisation des Nations Unies, peut être consultée, ainsi que les autres déclarations, publications et documents internes du Groupe permanent de surveillance sur la sécurité de l'information, sur le site web: www.unibw.de/infosecur.

Le Groupe PMP est présidé par l'ambassadeur Henning Wegener. Ceux de ses membres qui ont contribué à la présente publication sont les suivants:

Membres du groupe PMP auteurs de contributions

Mona Al-Achkar

Mme Mona Al-Achkar Jabbour, qui a un doctorat (PHD) en droit privé, a dirigé les départements juridique et de recherche de l'Université du Liban de 1998 à 2009. Elle a été consultante pour la mise en oeuvre de la base de données juridiques du Ministère de la Justice du Koweït, qu'elle a supervisée.

Elle est actuellement professeur de droit à la Faculté de droit du Liban, professeur chargé de recherches au Centre de recherche en informatique juridique de l'Université libanaise, fondatrice et présidente de l'Association libanaise des technologies de l'information (LITA), fondatrice du Centre libanais de lutte contre la cybercriminalité, membre et fondatrice de l'Observatoire panarabe pour la cybersécurité, et membre des Online Arab writers, de la Fédération arabe de l'arbitrage en ligne, de la commission juridique pour la protection en ligne des enfants au Ministère des Affaires sociales du Liban, de l'"équipe francophone" de l'ICANN et de l'IGF, du Centre Internet libanais (LINC) et du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists.

Mme Al-Achkar a publié de nombreux ouvrages et articles sur diverses questions juridiques, dont certaines concernent l'informatique juridique et le droit du cyberespace, le blanchiment d'argent et le terrorisme.

William Barletta

William Barletta est Professeur adjoint de physique au Massachusetts Institute of Technology et à l'Université de Californie Los Angeles. Il est également Professeur titulaire invité d'économie à l'Université de Ljubljana. Il est Directeur de la United States Particle Accelerator School et de la Korean Particle Accelerator School. Il est aussi coordonnateur et rédacteur en chef de la revue Nuclear Instruments and Methods. Il est conseiller principal du Président du Synchrotron de Trieste (Italie). Il copréside le Groupe permanent de surveillance (PMP) sur l'énergie de la World Federation of Scientists et est membre du Groupe permanent de surveillance sur la sécurité de l'information. Il est Président élu du Panel on Public Affairs de la American Physical Society (APS), dont il a présidé le Forum sur la physique internationale et la Division de la physique des faisceaux. Il est membre actif du Comité de l'APS pour les questions scientifiques internationales.

Il est l'éditeur de quatre ouvrages sur la science des accélérateurs et le co-auteur de quatre ouvrages relatifs à la cybersécurité, au respect de la vie privée et au droit international du cyberespace. Il est détenteur de quatre brevets et est l'auteur de plus de 170 articles scientifiques. Il a un doctorat en physique de l'Université de Chicago.

Pavan Duggal

Pavan Duggal est reconnu comme étant l'un des quatre plus grands juristes au monde spécialistes du cyberespace. Ses travaux en tant qu'expert faisant autorité sur le droit du cyberespace et du commerce électronique ont d'importantes répercussions internationales.

Pavan Duggal est avocat à la Cour suprême de l'Inde. Il est l'auteur de travaux innovants sur le droit de la convergence et le droit des communications mobiles. A ce titre, il est consultant de la CNUCED pour les questions de droit du cyberespace et de la CESAP pour les questions de cybercriminalité. Il est par ailleurs membre du Groupe de travail AFACT de UN/CEFACT, consultant expert en questions de cybercriminalité pour le Conseil de l'Europe, et membre du Groupe d'experts sur le commerce électronique de la Commission européenne. Comme en témoignent ses activités de spécialiste du droit du cyberespace pour le Groupe d'action e-ASEAN et de cyberrédacteur pour la Banque asiatique de développement, il fait autorité sur ces questions, à l'échelle mondiale. Il est aussi Président de Cyberlaw Asia et de Cyberlaws.Net.

M. Duggal a pris la parole dans le cadre de plus de 1 200 conférences, séminaires et ateliers, et est l'auteur de 42 ouvrages publiés ces dernières années sur divers aspects des législations mentionnées plus haut.

On trouvera de plus amples informations sur Pavan Duggal à l'adresse: www.linkedin.com/in/pavanduggal.

Solange Ghernaouti

Solange Ghernaouti, qui a un doctorat en informatique (Université de Paris), est professeur à l'Université de Lausanne et dirige le Swiss Cybersecurity Advisory and Research Group. Elle est une spécialiste internationalement reconnue des questions de cybersécurité, cyberdéfense, cybercriminalité et de la maîtrise des risques posés par les TIC. Elle a contribué à plusieurs initiatives mises en place par des organisations internationales, des institutions publiques ou privées, des centres de recherche et des organes d'application des lois, entre autres instances du monde entier. Ses travaux dans ce domaine portent depuis plusieurs années sur l'instauration d'une cybersécurité interdisciplinaire et jouant un rôle d'intégration, aussi bien pour les particuliers que pour les organisations et les Etats.

Mme Ghernaouti est conseillère indépendante pour les questions de sécurité. Ses analyses sont connues pour leur pertinence et elle est régulièrement invitée à s'exprimer dans les médias. Elle a été reconnue par la presse suisse comme l'une des femmes d'exception dans les milieux professionnels et universitaires. Elle est Chevalier de la Légion d'honneur et membre de l'Académie suisse des sciences techniques. Elle est l'auteur de plus de 300 publications et de 28 ouvrages, dont les suivants: "Cyberpower: Crime, Conflict and Security in Cyberspace" (Presses de l'EPFL, 2013), et en collaboration avec Judge SchjØlberg, de "A Global Treaty on Cybersecurity and Cybercrime – A contribution for peace, justice and security in cyberspace" (Cybercrimedata, 2009). Elle est membre du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists.

On trouvera de plus amples informations sur Solange Ghernaouti à l'adresse: www.scarg.org.

Gabor Iklody

Gabor Iklody est actuellement employé par le Service européen pour l'action extérieure (EEAS) de l'Union européenne à Bruxelles, où il est Directeur de la gestion et de la planification de crise. Auparavant, en tant que Secrétaire général adjoint de l'OTAN pour les défis émergents liés à la sécurité, il a créé et dirigé à l'OTAN la Division des défis de sécurité émergents, qui s'occupe par exemple de la cyberdéfense, du contre-terrorisme, de la non-prolifération des armes de destruction massive et de la sécurité énergétique, ainsi que de la politique nucléaire et de l'analyse stratégique. M. Iklody a par ailleurs présidé le Bureau de gestion de la cyberdéfense (CDMB) de l'OTAN.

Avant de prendre ses fonctions internationales, M. Iklody a travaillé pendant presque trente ans au Ministère des affaires étrangères de la Hongrie, où il a occupé en dernier lieu le poste de Directeur politique et de Secrétaire d'Etat adjoint responsable des questions multilatérales et de sécurité. Il a été Ambassadeur en Scandinavie pendant deux mandats de quatre ans, tout d'abord en Norvège de 1999 à 2003, puis en Suède de 2005 à 2009. Il a consacré une grande partie de sa carrière à l'intégration euro-atlantique, à la diplomatie multilatérale et à la maîtrise des armements.

Danil Kerimi

Danil Kerimi est chargé d'élaborer le programme technologique, de définir la stratégie de communication avec le secteur public dans le monde et de regrouper diverses initiatives du domaine des TIC pour constituer une plate-forme hyperconnectée (cybersécurité, données, technologie au service de l'humanité, TIC pour la compétitivité, gouvernance de l'Internet) au Forum économique mondial (WEF). Il gère la participation de hauts dirigeants des secteurs public et privé, d'experts du savoir et de la société civile aux projets du Forum impliquant les TIC. M. Kerimi est par ailleurs responsable du Global Agenda Council on Cyber Security et du rapport annuel publié par le WEF sur les technologies de l'information dans le monde ("Annual Global Information Technology Report"). Avant de travailler au WEF, M. Kerimi a occupé divers postes à responsabilité aux Nations Unies, à l'Organisation pour la coopération et la sécurité en Europe, à l'Organisation internationale pour les migrations, et dans d'autres grandes institutions internationales.

Axel Lehmann

Axel Lehmann est professeur émérite au Département d'informatique de l'Université des forces armées à Munich (Allemagne), où il a occupé une chaire de modélisation et de simulation jusqu'en 2011. Il est aujourd'hui directeur exécutif de l'Institut de recherche pour les systèmes intelligents (ITIS) dans cette même université. Ses principaux domaines de recherche sont très variés: modélisation et simulation informatiques, application de systèmes fondés sur les connaissances au diagnostic et à l'appui à la prise de décisions, ou encore conception d'architectures informatiques innovantes. Il a présidé la Society for Modelling and Simulation International. Il est membre de la Société allemande d'informatique et de la Federation of Asian Simulation Societies et siège au comité de rédaction de plusieurs revues scientifiques spécialisées en modélisation et simulation. Il est en outre membre de plusieurs associations internationales professionnelles et de normalisation, ainsi que de comités d'examen, par exemple pour l'Union européenne et pour l'OTAN. Il est membre du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists depuis sa création en 2001.

Stefan Lüders

Stefan Lüders est titulaire d'un doctorat et diplômé de l'Ecole polytechnique fédérale de Zürich. Il est entré au CERN en 2002. Auteur d'un système commun de sécurité utilisé dans quatre expériences effectuées dans le cadre du Grand collisionneur de hadrons du CERN, il a acquis une expérience pratique des questions de cybersécurité liées aux systèmes de contrôle. Par la suite, en 2004, il a été chargé de mettre les systèmes de contrôle de l'accélérateur et des infrastructures du CERN à l'abri des cybermenaces. Il a ensuite rejoint l'équipe de sécurité informatique du CERN pour les interventions en cas

d'urgence, qu'il dirige aujourd'hui en qualité de directeur de la sécurité informatique, chargé de coordonner tous les aspects de cette sécurité: sécurité bureautique, sécurité du centre informatique, sécurité du réseau électrique intelligent et du système de contrôle, compte tenu des besoins opérationnels du CERN. M. Lüders présente souvent des exposés sur la sécurité informatique et la cybersécurité des systèmes de contrôle devant des organismes internationaux, gouvernements et entreprises privées; il a publié plusieurs articles sur ces sujets.

Howard A Schmidt

Howard A. Schmidt est actuellement associé du cabinet de conseil stratégique Ridge-Schmidt Cyber, société de services exécutifs qui aide les dirigeants d'entreprises privées et publiques à répondre aux besoins croissants de cybersécurité. Il occupe ce poste aux côtés de Tom Ridge, premier Secrétaire au Département de la sécurité intérieure. Il est par ailleurs Directeur exécutif du Software Assurance Forum for Excellence in Code (SAFECode).

M. Schmidt réunit des compétences spécialisées dans divers domaines, acquises au long de plus de 40 années de carrière: économie, défense, renseignement, application des lois, questions de confidentialité, vie universitaire et relations internationales. Récemment, il a occupé le poste d'Assistant spécial du Président et de coordonnateur de la cybersécurité pour les Etats-Unis. Entre autres fonctions à la Maison Blanche, il a été conseiller en matière de cybersécurité auprès des Présidents Barack Obama et George W. Bush.

Auparavant, M. Schmidt était Président Directeur général de l'Information Security Forum (ISF). Il a été Vice-Président et Chef de la sécurité de l'information, ainsi que responsable des stratégies en matière de sécurité pour eBay Inc., après avoir été Chef de la sécurité pour Microsoft Corp. Il a en outre été responsable des stratégies de sécurité pour le programme US-CERT au Département de la sécurité intérieure.

M. Schmidt a une licence en administration des entreprises (BSBA) et une maîtrise en gestion organisationnelle (MAOM) de l'Université de Phoenix. Il est aussi docteur honoris causa ès lettres et Adjunct Distinguished Fellow du CyLab de Carnegie Mellon, ainsi que Distinguished Fellow du Ponemon Privacy Institute. Il a auparavant été membre du Groupe permanent de parties prenantes (PSG) de l'Agence Européenne chargée de la sécurité des réseaux et de l'information (ENISA). Il est actuellement professeur et chargé de recherche à l'Université d'Etat de l'Idaho. Il est aussi membre du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists.
M. Schmidt est radio-opérateur (W7HAS), pilote privé, pratique beaucoup d'activités de plein air et fait de la moto (sur une Harley-Davidson). Il est marié à Raemarie J. Schmidt,

spécialiste de police scientifique en retraite, chercheuse et enseignante dans le domaine de la criminalistique, et ils ont des enfants et petits-enfants.

Hamadoun I. Touré

Le Dr Hamadoun I. Touré, Secrétaire général de l'UIT depuis janvier 2007, a été réélu pour un second mandat en octobre 2010. Il bénéficie d'une vaste expérience professionnelle tant dans le secteur public que dans le secteur privé.

Ressortissant du Mali, le Dr Touré est résolu à faire de l'UIT une organisation innovante et tournée vers l'avenir qui soit en mesure de faire face aux enjeux liés au nouvel environnement des TIC et à la diriger dans l'optique de la mise en oeuvre des résolutions du Sommet mondial sur la Société de l'information (SMSI) et de la réalisation des Objectifs du Millénaire pour le développement (OMD).

Le Dr Touré est marié, a quatre enfants et deux petits-enfants.

Henning Wegener

M. Henning Wegener est ancien Ambassadeur d'Allemagne. Il a été ambassadeur pour le désarmement à Genève de 1981 à 1986, Secrétaire général adjoint pour les affaires politiques à l'OTAN, de 1986 à 1991, Directeur général à la Chancellerie fédérale allemande, de 1991 à 1994, puis Ambassadeur en Espagne, de 1995 à 1999. Il préside, depuis sa création en 2001, le Groupe permanent de surveillance sur la sécurité de l'information, dont il a été coprésident de 2009 à 2012. Ses travaux ont fait l'objet de publications dans le domaine de la politique de sécurité et de la politique étrangère, y compris en ce qui concerne la cybersécurité. M. Wegener est membre du Chapitre espagnol du Club de Rome et siège au conseil d'administration de plusieurs fondations. Entre autres diplômes, M. Wegener est Docteur en droit de la Yale Law School. henningwegener@hotmail.com.

Préface par le Dr Hamadoun I. Touré, Secrétaire général de l'UIT

Le présent ouvrage a pour objet, et c'est là une tâche de plus en plus ardue, d'instaurer la confiance dans l'utilisation des plates-formes et technologies du cyberespace, dans un contexte de violations de la sécurité, dont on a beaucoup parlé récemment, et d'une pléthore de nouvelles menaces qui fragilisent la confiance placée dans ces outils, pourtant devenus indispensables.

Il fait suite à la publication en 2009 du rapport *En quête de la cyberpaix,* axé sur la promotion de la cyberpaix dans un domaine générateur de nombreux bienfaits et progrès pour l'humanité, mais qui est aussi à l'origine d'une multitude d'activités délictueuses et a ouvert de nouvelles voies à la collecte de renseignements, à l'espionnage industriel et aux conflits.

Evidemment, le présent ouvrage revient sur ces questions articulées autour de la thématique générale de l'utilisation du cyberespace au service du bien ou du mal, en particulier en ce qui concerne les répercussions de la "face sombre" de l'Internet sur la confiance dans le cyberespace. Ici, toutefois, le thème central est celui de la cyberconfiance. Comme souligné dans le chapitre d'introduction, il n'est plus exagéré de parler de "crise de confiance" dans le cyberespace. D'ailleurs, une analyse des tendances récentes fait apparaître que la convergence de plusieurs événements nuit globalement à la cyberconfiance; ainsi, la militarisation croissante du cyberespace et l'émergence de capacités militaires offensives visant, non seulement des cibles militaires, mais aussi, par ricochet, des infrastructures civiles essentielles, sont particulièrement préoccupantes; l'élaboration du concept de cyberpaix répondait à la nécessité de contribuer à endiguer cette évolution. Encore plus important: le nombre inégalé de cas d'espionnage numérique et de violations du respect de la vie privée dans le cyberespace, qui depuis peu, préoccupent beaucoup l'opinion publique.

Tout au long de cet ouvrage, ses auteurs, sous différents angles, évoquent les raisons qui, ensemble, expliquent l'érosion de la confiance, les analysent et élaborent des stratégies de lutte contre cette érosion. A cet égard, ils privilégient trois domaines considérés comme cruciaux pour le rétablissement et l'instauration de la confiance: 1) établissement de *politiques normatives* et de *cadres réglementaires* spécifiquement applicables au numérique; 2) renforcement de la *résilience* face aux multiples cas d'utilisation abusive du cyberespace; 3) garantie des *libertés* fondamentales telles que la liberté d'accès et la liberté d'expression dans le cyberespace. Dans ces trois domaines, les auteurs mettent en avant et évaluent les initiatives en cours à l'échelle mondiale, régionale et nationale en vue d'atteindre ces objectifs.

Le présent ouvrage est un vibrant appel à agir pour tenter d'apporter une réponse à ces questions, arguments à l'appui. Tout comme l'ouvrage précédent *En quête de la cyberpaix,* il est publié avec le soutien de la World Federation of Scientists et de l'Union internationale des télécommunications, organisations qui sont toutes deux à l'avant-garde de cette initiative.

Préface du Professeur Antonino Zichichi, Président de la World Federation of Scientists

A l'aube du troisième millénaire, la science est, plus que jamais, le facteur déterminant du changement et de l'évolution historique. C'est grâce à elle que l'humanité peut explorer plus avant le fonctionnement et les secrets de l'univers. Au cours de ce processus, des systèmes déjà complexes gagnent encore en complexité. On observe de nouvelles formes d'interaction entre les êtres humains et l'environnement: les relations entre l'esprit et la machine, en pleine évolution, doivent être redéfinies. Nous entrons dans une période de découvertes, mais aussi de défis sans précédent.

Les technologies numériques jouent un rôle dans les sciences et les sciences appliquées. Ces technologies et les outils associés deviennent omniprésents, dessinant une courbe de croissance spectaculaire du savoir existant et proposant des dispositifs de contrôle et des systèmes de commande applicables à toutes les activités humaines, ou presque. Les applications informatiques spécialisées, l'informatique distribuée, en grilles et dans le nuage, fondée sur des infrastructures informatiques extrêmement évoluées, l'évolution de la microélectronique et des nouveaux capteurs, de l'interconnectivité, souvent automatique, d'une multitude d'appareils numériques, et la transformation rapide des processus de fabrication – telles sont certaines des principales caractéristiques de cette nouvelle ère.

En ma qualité de Président de la World Federation of Scientists, je voudrais, non pas me contenter d'énumérer les avantages innombrables du numérique, mais insister sur l'importance de la science et de l'évolution des technologies numériques, dans l'intérêt de la paix et pour faire face à des urgences planétaires, tâche qui est tributaire de la collecte de données en temps réel – à des fins de prévention, d'intervention, de rétablissement de la situation et de retour à la normale. Je suis à ce sujet tout à fait conscient de la responsabilité morale qui incombe aux scientifiques.

Le cyberespace ne connaît pas de frontières, son omniprésence modifie notre perception du monde et réduit drastiquement les durées et les distances. L'ambigüité inhérente aux cybertechnologies – comme à toutes les technologies modernes – autrement dit leur utilisation possible au service, soit du bien, soit du mal, revêt des dimensions mondiales. Le cyberespace est un domaine qui ouvre des possibilités infinies, mais où les dangers sont aggravés par l'absence de cadres réglementaires

solides et valables dans le monde entier. Les utilisations hostiles des technologies numériques sont de plus en plus porteuses de menaces. La cybersécurité et la protection des données deviennent donc des composantes encore plus cruciales de la gestion des risques numériques. Elles sont désormais un aspect fondamental de la révolution numérique et doivent devenir un secteur véritablement porteur face à ces menaces.

La World Federation of Scientists, en particulier son groupe multidisciplinaire sur la sécurité de l'information, travaille sur le sujet depuis une bonne dizaine d'années. Un ouvrage déjà publié en collaboration avec le Secrétaire général de l'UIT ("En quête de la cyberpaix") mettait l'accent sur les utilisations sécurisées et pacifiques des technologies numériques. Le présent ouvrage, quant à lui, traite d'un autre aspect crucial d'une société numérique fonctionnelle, à savoir la confiance. Les utilisateurs, et la société dans son ensemble, doivent non seulement être sûrs que la technologie fonctionne sans problème, mais aussi avoir confiance dans l'intégrité et la confidentialité des données et des appareils numériques et des infrastructures de réseau qui les sous-tendent. La confiance mutuelle est indispensable à une coopération utile et durable. Dans le cyberespace et dans une société mondiale de l'information de plus en plus interconnectée, la confiance est un impératif absolu. Elle renforce l'efficacité et la productivité des interactions internationales, car c'est sur elle que s'appuient les attentes mutuelles escomptant bonne foi et réciprocité. J'exprime toute ma reconnaissance au Dr Touré, Secrétaire général de l'UIT, et aux co-auteurs du présent ouvrage, qui ont si bien su évoquer les multiples dimensions de la cyberconfiance et formuler les recommandations appropriées.

Introduction: La crise de la cyberconfiance

Par Henning Wegener

Il y a trois ans, le Secrétaire général de l'UIT et les membres du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists ont publié l'ouvrage *En quête de la cyberpaix*[1], qui mettait en garde contre la prolifération des dangers dans le cyberespace et appelait toutes les parties prenantes à unir leurs efforts pour assurer une stabilité minimale de l'Internet et de ses infrastructures et pour faire progresser le concept de cyberpaix mondiale. Cet ouvrage, délibérément concis et reflétant un vaste débat public d'actualité, n'a pas pris une ride. Ses auteurs, qui sont souvent les mêmes que ceux du présent volume, sont fidèles à leurs analyses et recommandations d'alors.

---

1 *En quête de la cyberpaix*, Union internationale des télécommunications & World Federation of Scientists, Genève, janvier 2011.

Pourtant, la situation s'est aggravée depuis lors et il n'est pas exagéré de parler de menaces d'une nouvelle dimension dans le cyberespace qui évolue sous nos yeux. La publication précédente était largement axée sur la perspective inquiétante d'un cyberconflit ou d'une cyberguerre. Ces menaces, loin de disparaître, se sont encore précisées. C'est pourquoi le cyberconflit figure en bonne place dans le présent ouvrage, établissant ainsi un fil conducteur entre les deux titres. Toutefois, la thématique des contributions au présent ouvrage a évolué au même rythme que les menaces. Le thème central est le concept de cyberconfiance, l'objectif étant d'analyser les tendances qui minent cette confiance, et les stratégies et techniques à employer pour la rétablir[2].

Le concept de confiance – pilier du fonctionnement d'une société de l'information fondée sur la technologie numérique – n'a rien de nouveau. A la lecture des documents adoptés par le Sommet mondial sur la société de l'information (SMSI) lors de ses deux phases de 2003 et de 2005, on se rend immédiatement compte que le concept de confiance est le fil conducteur de ces textes et recommandations: "La confiance et la sécurité sont au nombre des principaux piliers de la société de l'information", et "Etablir la confiance et la sécurité dans l'utilisation des TIC", est-il indiqué au titre de la grande orientation C5.

Au cours des débats qui ont suivi le SMSI, le rapport du coordonnateur pour la grande orientation C5, publié en 2014, cite comme principale préoccupation (extrait du Résumé analytique): "Renforcer le climat de confiance: augmenter la confiance dans les dispositifs numériques, dans la cybersécurité, et créer un environnement de confiance entre organisations des secteurs public et privé sont des tâches fondamentales. Il est impératif d'améliorer le niveau de confiance des particuliers dans les services numériques et l'Internet"[3].

La confiance étant un élément clé de la société de l'information, il est évident qu'elle joue un rôle dans tous les aspects de l'univers numérique. C'est pourquoi, même si la thématique de la publication *En quête de la cyberpaix* est différente, cet ouvrage présente une analyse approfondie du concept de confiance et de son omniprésence dans la société[4]. Ainsi que le souligne l'auteur: "La confiance et la fiabilité sont des

---

2 Afin de démontrer la continuité entre les deux publications, le titre du présent ouvrage est *En quête de la cyberconfiance.* Pourtant, le mot *Quête* n'a pas le même sens dans les deux cas. Dans le premier ouvrage, il exprime l'aspiration à un état de paix non encore atteint, tandis que dans le second, il exprime l'idée que la confiance existe, mais qu'elle est gravement ébranlée, et qu'il convient donc de la rétablir et de la renforcer.

3 Doc. WSIS+10/4/2

4 Jacques Bus, La confiance est indispensable: Le concept de confiance et son rôle dans la société, "*En quête de la cyberpaix*", p.17.

concepts de base de l'existence humaine", sous-tendant toutes les relations sociétales et permettant de faire face aux nombreuses incertitudes et à la complexité de la vie contemporaine, et donc de réduire les risques perçus. Dans son analyse, il présente un aperçu des travaux antérieurs sur ce sujet. L'ouvrage étant toujours accessible au public, nous nous contenterons ici de le citer à titre de référence générale[5].

En anglais, les deux mots "trust" et "confidence" (tous deux traduits par "confiance" en français) sont en grande partie synonymes, mais "trust" fait davantage référence aux relations entre les personnes, tandis que "confidence" s'applique plutôt aux relations entre les personnes et une entité autre qu'humaine ou une institution. Pour le thème qui nous préoccupe, cette dernière notion inclut les dispositifs et produits numériques tels que matériels, logiciels, réseaux, infrastructures, applications et procédures de traitement. La présente publication porte donc essentiellement sur la confiance ("confidence"), sans toutefois négliger les attentes et perceptions des individus qu'implique le terme "trust".

Comme on l'a déjà fait remarquer, la confiance est le pilier du fonctionnement de l'univers numérique. Or, de récents événements ayant des répercussions sur cet univers en pleine expansion ont gravement fragilisé cette confiance. Il n'est pas exagéré de parler aujourd'hui d'une crise de la cyberconfiance.

Les facteurs qui se sont conjugués pour déclencher cette crise sont les suivants:

- La montée des inquiétudes concernant la militarisation du cyberespace et le fait qu'un nombre croissant d'Etats renforcent leurs capacités militaires offensives visant non seulement des cibles militaires, mais aussi, en réalité, des infrastructures civiles essentielles et les modes de vie de la population civile d'un adversaire, ce qui entraînerait des répercussions incontrôlables, alors que rien n'empêcherait le lancement d'une course aux armements numériques. Plus d'une centaine d'Etats renforcent actuellement leurs capacités d'attaque numérique, jouant sans retenue un jeu de plus en plus dangereux de réciprocité stratégique, dans lequel l'utilisation des capacités TIC à des fins de nuire est clairement affichée comme doctrine, afin de servir des objectifs militaires et politiques. Ces préoccupations n'excluent pas le recours à l'auto-défense lorsqu'elle est nécessaire et légitime.
- Il est, certes, primordial d'adapter le droit international à l'ère numérique et de définir les limites de l'utilisation hostile des technologies numériques, mais on constate avec inquiétude que, plutôt que de promouvoir la cyberpaix, les efforts actuellement déployés pour élaborer des outils normatifs légitiment l'intégration à grande échelle des cyberarmes dans les arsenaux militaires des

5 Les principaux auteurs cités sont O'Hara, Luhmann, Hardin et Fukuyama.

Etats, inscrivant ainsi leur déploiement opérationnel dans le cadre normal de la planification stratégique.

- Il est de plus en plus à craindre que des infrastructures civiles essentielles soient attaquées par des Etats ou des protagonistes autres que des Etats, que ce soit sous prétexte d'activités militaires légitimes ou à des fins délictueuses.
- Les incertitudes relatives aux règles et normes de comportement susceptibles de s'appliquer à tous ces événements et de servir de critères de référence pouvant contribuer à rétablir la cyberconfiance. Ces incertitudes sont encore aggravées par l'échec des efforts de normalisation qui n'ont pas réussi, ces dix dernières années, à produire des codes universellement harmonisés applicables à grande échelle.
- La complexité croissante de l'environnement technique, riche d'un fort potentiel, mais aussi toujours plus vulnérable et exposé à des conséquences imprévisibles dans un monde hyperconnecté. Les peurs sont alimentées par de nombreux facteurs: croissance exponentielle des dispositifs numériques, nouvelles failles dues à l'utilisation croissante des applications, problèmes de sécurité causés par le passage aux applications mobiles et aux applications dans le nuage, augmentation inquiétante des nouveaux composants de logiciels malveillants[6], hausse de la cybercriminalité, qui coûte des fortunes aux économies des pays touchés, aux entreprises et aux particuliers, enfin, émergence d'organisations criminelles opérant à l'échelle internationale et toujours plus puissantes, ayant les capacités et le potentiel pour jouer les mercenaires en cas de cyberdélit ou de cyberconflit. Comme indiqué plus haut, cette évolution témoigne d'une nouvelle dimension et d'un saut quantitatif des cybermenaces, susceptibles de saper encore davantage la cyberconfiance.
- Les incertitudes qui persistent à propos de la gouvernance de l'Internet, amenant à se poser des questions quant aux possibilités de conserver un "réseau mondial, interopérable, résilient, stable, décentralisé, sûr et interconnecté, accessible à tous"[7].
- La multiplication des obstacles mis à l'exercice des droits humains sur le Net, du fait de la censure massivement exercée par certains gouvernements sur l'accès et les contenus (cyberrépression) dans un nombre croissant de pays.

---

6 A l'heure où nous écrivons, il est de plus en plus fréquent que des failles majeures soient découvertes et que de nouvelles menaces se manifestent, comme en témoigne, après la découverte de la faille Heartbleed en avril 2014, l'émergence rapide du virus Shellshock, décrit comme présentant une "menace mortelle" et risquant d'infecter plus 500 millions de machines.

7 Déclaration des parties prenantes, NETmundial, 24 avril 2014.

- Enfin et peut-être surtout, et il s'agit là d'un sujet d'actualité brûlante, on assiste à l'émergence d'intrusions illimitées, sans garde-fous techniques, dans les systèmes numériques, via la recherche de mégadonnées. L'espionnage industriel numérique atteint ainsi une ampleur inégalée, de même que l'espionnage de masse pratiqué par les services de renseignement de certains Etats, allant bien au-delà de la sphère d'influence nationale et violant sans aucun scrupule la souveraineté et l'ordre juridique d'autres nations[8].

Sans aucun doute, le rétablissement de la confiance est un défi que doivent relever toutes les parties prenantes du numérique, et il est à espérer que la présente publication pourra y contribuer, en collaboration avec d'autres institutions et organisations qui poursuivent un même objectif, à savoir rétablir la confiance de manière concertée et équilibrée[9].

La méthode adoptée dans la présente publication consiste à se focaliser sur trois grands sujets qu'il importe de traiter d'urgence pour restaurer la cyberconfiance, et qui font par ailleurs l'objet de débats publics approfondis.

Le lecteur de ces trois chapitres doit être conscient que la présente publication n'est ni un manuel, ni un traité visant à examiner en détail un sujet complexe, ni un document qui ambitionne de donner un avis unique et faisant autorité sur tous les aspects qui s'y rapportent. Elle est structurée de manière à associer différents textes rédigés par l'UIT à des contributions présentées par des membres de la World Federation of Scientists, qui s'expriment à titre personnel. En-dehors de la Mention légale et de l'Avertissement figurant au début de l'ouvrage, il est à souligner que les éditeurs ont délibérément cherché à élargir les perspectives en vue d'enrichir le débat, tout en veillant à ce que les opinions exprimées soient dans l'ensemble compatibles.

La première partie traite de la recherche d'un cadre normatif exhaustif visant à réguler les comportements dans le cyberespace et à les rendre plus prévisibles et quantifiables. Elle est plus particulièrement consacrée aux efforts déployés sur le plan international pour élaborer, faire accepter et mettre en pratique des mesures de renforcement de la confiance et des codes de conduite – de même que des outils juridiques de plus grande ampleur visant à améliorer la cyberconfiance – en termes d'harmonisation des prescriptions juridiques et de coopération au niveau de l'application des lois sur le plan international. L'ambition est de tracer une voie à suivre pour parvenir progressivement,

---

8 A propos de l'importance de la confiance dans ce domaine, voir Leif-Eric Easley, *Spying on Allies*, SURVIVAL, Vol. 56, numéro 4, août-septembre 2014, p. 141.

9 Récemment, des conférences internationales suivies par de nombreux participants ont également porté sur le thème de la confiance, par exemple le deuxième Sommet sur la cybersécurité, organisé par la Munich Security Conference et Deutsche Telekom, à Bonn en novembre 2013, avec la participation de Howard A. Schmidt – l'un des co-auteurs du présent ouvrage – qui y a prononcé une allocution.

mais systématiquement, à un consensus international et national dans le domaine normatif.

La deuxième partie met l'accent sur la cyberdéfense et sur la capacité des systèmes numériques à résister aux attaques et conflits, ainsi que sur les moyens de réduire les vulnérabilités, d'atténuer les effets des attaques ou de les réduire à néant, ou de rétablir les capacités des systèmes ayant subi des dégâts causés par des attaques, ou des perturbations causées par des défaillances, erreurs et échecs dans le cyberespace. Le terme clef à cet égard est celui de résilience[10]. Après une analyse des menaces existantes ou prévisibles, ce chapitre décrit toute une palette de techniques et de stratégies qui, utilisées conjointement, peuvent faire pencher la balance vers la réussite des tactiques de défense, dans le cadre de la joute qui les oppose de longue date aux tactiques d'attaque et qui se rejoue sous nos yeux dans l'univers numérique.

Le dernier chapitre traite de la manière de concilier la liberté de l'Internet – et de toutes les autres communications sur support numérique – et les ingérences d'origine gouvernementale, autrement dit de concilier le respect de la vie privée dans l'univers numérique et la sécurité d'Etat. Est-il vrai que "le respect de la vie privée n'existe plus", si l'on pense aux innombrables moyens techniques qui permettent d'espionner impunément tout lieu de stockage de données, chez un particulier ou dans une entreprise? Le présent chapitre vise à préciser l'étendue des activités de surveillance légitimes par les services de renseignement étrangers et nationaux, et les fondements juridiques – en particulier concernant les pays autre que ceux qui organisent cette surveillance – autorisant une surveillance de cette ampleur. Il traite en outre des éventuelles sanctions contre les pratiques abusives. Il est à espérer que ce document contribuera à l'adoption d'un cadre de mesures concertées, à valeur juridique obligatoire, qui concilie les préoccupations légitimes en matière de sécurité et les droits fondamentaux, la validité des législations nationales assurant la protection et la sécurité des données, et le concept fondamental de liberté de l'Internet. Ce sujet brûlant, tout comme celui de la censure illégitime de l'Internet par des gouvernements, doit être examiné plus avant dans une perspective internationale.

Bien sûr, la finalité globale de ce texte est d'empêcher que l'érosion de la cyberconfiance ne s'aggrave et de rétablir cette confiance de manière efficace et pérenne. Il est impératif de surmonter la crise de la cyberconfiance.

---

[10] La résilience, ou capacité de résister à l'adversité, de persévérer et de revenir à la normale, est davantage que la simple addition d'ajustements techniques. Ce terme implique aussi l'idée de solidité globale – par opposition à la fragilité – des systèmes dans la durée. Voir Dhruva Jaishankar, *Resilience and the Future Balance of Power*, Survival, Vol. 56, juin-juillet 2014, p. 217.

Chapitre I: Cybernormes

Introduction

Ce chapitre brosse un tableau général des efforts déployés pour définir une série de normes, principes et bonnes pratiques régissant la cybersécurité à l'échelle internationale et des enjeux que cela représente. Les menaces émergentes, comme l'espionnage ou les attaques assimilables à des actes de guerre et les spécificités de l'Internet (réseau transnational à caractère technique, qui implique de multiples parties prenantes) font que les Etats se trouvent dans le cyberespace en terrain inhabituel: les gouvernements des différents pays font face à une situation sur laquelle ils n'ont habituellement guère de prise, mais qui leur impose de protéger leurs citoyens, surtout sur le plan des droits humains. Des efforts sont actuellement déployés, de manière exhaustive sur le plan régional, mais plus limitée à l'échelle mondiale, en vue d'établir des normes de base communes pour mettre en place cette protection.

Les technologies de l'information et de la communication (TIC) deviennent omniprésentes et leur utilisation augmente de manière exponentielle dans les pays développés comme dans les pays en développement. La confiance dans l'utilisation des TIC passe par la création de TIC sûres et fiables. Or, plusieurs tendances actuelles fragilisent cette confiance:

- l'espionnage à grande échelle à des fins de sécurité nationale, facilité par la forte baisse des coûts de la collecte et du stockage des données personnelles;
- l'utilisation de codes informatiques pour des actes assimilables à des actes de guerre qui transcendent les frontières nationales;
- l'existence d'un groupe apparemment hétérogène et incontrôlable de personnes malintentionnées, allant des spammeurs aux développeurs de botnets qui louent leurs services;
- les difficultés pour faire en sorte que les cybercriminels répondent de leurs actes alors qu'ils opèrent depuis une juridiction différente de celle où se trouve le système victime de leurs attaques.

Pour relever ces défis, fort complexes, il est impératif de passer par la coopération transnationale. Le présent chapitre décrit les efforts en ce sens, notamment ceux qui sont entrepris par les organisations du système des Nations Unies et d'autres organismes intergouvernementaux, ainsi que des recommandations de base en vue de la conclusion d'un accord mondial sur la cybersécurité. Les mesures de renforcement de la confiance – terme utilisé pour la première fois lors de la Guerre froide – sont un élément central de ces initiatives.

Ce chapitre comporte quatre sections. Tout d'abord, il met en avant la nécessité pour les Etats de prendre des mesures de renforcement de la confiance, dont il décrit les inconvénients et les avantages potentiels. Il expose ensuite la ligne de conduite des Nations Unies concernant les normes, règles et principes en matière de cybersécurité, y compris les principes et recommandations pour l'avenir, et l'applicabilité du droit international au secteur des TIC. Une troisième section, plus particulièrement consacrée à ce dernier point, présente un aperçu des similarités entre les acteurs et actes dans le cyberespace et ceux d'autres domaines de la guerre et de l'espionnage, ainsi qu'une vaste série de lignes directrices pour l'élaboration d'un instrument international à valeur de traité en matière de cybersécurité. Enfin, la quatrième section décrit la façon dont l'Organisation des Nations Unies envisage la cybersécurité, en mettant l'accent sur les mécanismes, mis en place ou à l'état de projet, des institutions spécialisées et sur une vision à long terme du rôle du système international relativement à la cybersécurité et à la cybercriminalité.

Il aurait été tentant – voire, à certains égards, nécessaire – d'inclure une autre section consacrée à la gouvernance de l'Internet. En effet, le présent ouvrage établit que les incertitudes sur l'avenir de l'Internet figurent parmi les causes évidentes de l'érosion de la cyberconfiance. Pourtant, le débat international en cours sur la gouvernance, qui n'a pas encore permis de surmonter des positions gouvernementales divergentes, fait qu'il est difficile pour l'UIT d'adopter des avis tranchés. On notera toutefois avec satisfaction que les débats qui ont récemment permis la négociation de la Déclaration des parties prenantes, adoptée à la conférence NETmundial tenue au Brésil en avril 2014, ont débouché sur des progrès tangibles et que – même si ce document est volontairement sans force obligatoire – on constate un début de consensus mondial sur certaines questions de base. Du fait de sa vocation internationale, l'UIT peut certainement soutenir tous les efforts visant à conserver à l'Internet son caractère de "réseau mondial, interopérable, résilient, stable, décentralisé, sûr et interconnecté, accessible à tous" en tant qu'espace unifié et indivisible. Dans le même esprit, elle peut confirmer la Déclaration de la conférence NETmundial, selon laquelle "la surveillance de masse et la surveillance arbitraire ébranlent la confiance dans l'Internet et dans l'écosystème de la gouvernance de l'Internet".

1.1 Le rôle des mesures de renforcement de la confiance dans une nouvelle vision de la cybersécurité internationale: réaction mondiale et traité international envisageables

Par Solange Ghernaouti

La cyberconfiance – un impératif

En seulement quelques années, l'Internet est devenu un élément omniprésent et pour ainsi dire indispensable de notre vie quotidienne. Nul n'échappe à ce raz-de-marée. Avec les dispositifs intelligents, un nombre croissant de services sont dématérialisés, y compris dans les domaines de la santé et de la médecine, de l'informatique en nuage et de l'Internet des objets. Nous nous habituons donc à être connectés en permanence et à devenir tributaires des TIC. Aujourd'hui, l'Internet peut être considéré comme une sorte de prothèse numérique, et le cyberespace comme une extension "naturelle" de notre environnement. En tant qu'agent du changement et de la civilisation, l'Internet structure la société de l'information que nous édifions à l'échelle mondiale. Il fait partie intégrante du processus continu d'évolution et d'invention humaine constitutif de notre histoire.

L'adoption des technologies numériques a modifié en profondeur et de façon irréversible nos modes de communication, de comportement, de pensée, de loisirs, d'apprentissage, de transactions économiques, ainsi que la façon dont nous pouvons exercer une influence, déstabiliser ou nuire, et même surveiller, mener une guerre ou faire régner l'ordre. On constate que la technologie, qui s'accompagne de changements structurels qui nous touchent directement, n'est pas neutre.

Nous utilisons tous le même Internet, que ce soit pour des applications privées, personnelles ou professionnelles, dans les domaines de la santé, de l'énergie, de l'approvisionnement, de la culture ou de la sécurité. Des loisirs à la finance, et pour tous les systèmes de commande d'infrastructures, d'information et de télécommunications essentielles, on ne peut s'en passer.

L'Internet et tous ses accessoires ont accéléré la dépendance de la société et, dans une certaine mesure, des personnes, à la technologie. Nous créons et traitons des volumes croissants d'informations, de données et d'interactions. Nous consommons toujours plus d'informations, de ressources informatiques et d'énergie, et en conséquence, en jetons toujours plus au rebut.

Les technologies de l'information sont donc devenues le dénominateur commun de toutes les disciplines et la mémoire de notre patrimoine (patrimoine culturel numérique, patrimoine numérique des entreprises et des particuliers). Le savoir et la science n'existent plus sans elles. En outre, les grands principes fondateurs de notre

société, tels que la démocratie, l'identité individuelle et la souveraineté de l'Etat, sont, eux aussi, tributaires jusqu'à un certain point de ces technologies – qui, mal utilisées ou piratées, peuvent servir à les déstabiliser.

Signalons au passage le rôle que les médias sociaux et les divers outils de communication sur l'Internet peuvent jouer dans le cadre de stratégies visant à exercer une influence, que ce soit à l'instigation d'Etats, de groupes de pression, ou de groupes terroristes ou criminels. S'il est utilisé pour détruire une réputation, influencer des personnes, des foules ou des dirigeants, désinformer et manipuler l'opinion, l'Internet devient un véritable champ de bataille de l'information. Parallèlement, grâce aux technologies de l'information, des organisations malintentionnées ou criminelles peuvent donner libre cours à leur imagination et mener de nouvelles guerres dans le cyberespace, y compris des guerres de l'information. Nier cette réalité revient à s'exposer inutilement au risque de perte de compétitivité économique, de stabilité, de souveraineté nationale et de crédibilité internationale. Les médias, de même que les spécialistes de la question, font état d'une série interminable de cas d'entreprises victimes de vols de données à grande échelle, de cyberattaques ou de captations d'informations qui seront délivrées contre rançon.

La confiance dans la cybersécurité est donc devenue fondamentale, non seulement vis-à-vis des infrastructures TIC, des services offerts et des informations traitées, mais aussi de leur sécurité.

Au-delà de la complexité, le cyberespace fait évoluer le concept de territoires à sécuriser

Le monde actuel est un univers complexe et globalisé, avant tout caractérisé par l'utilisation intensive des appareils, infrastructures et services TIC. La dépendance vis-à-vis de ces infrastructures essentielles et leur interdépendance exposent la société à de nouveaux risques. Il est donc de plus en plus complexe de sécuriser, protéger et défendre les activités cruciales dans les domaines politique, économique, social et individuel. Par ailleurs, l'interdépendance entre les risques nuit au cadre global de la résilience, que ce soit au niveau national ou international. Si la cybersécurité – qu'on l'appelle sous ce nom, ou sécurité de l'information, ou encore sécurité numérique – a acquis aujourd'hui une telle importance, c'est en raison de préoccupations d'ordre politique, économique, juridique et technologique. Sa gestion est donc déterminante, et les différents éléments qu'implique la recherche de solutions en la matière sont complexes.

Le cyberespace est un domaine à la fois virtuel et réel, comprenant les technologies, services et données Internet. Il est devenu – tout au moins pour la jeune génération – un élément du paysage au même titre que la terre, la mer, l'air et l'espace, aussi naturel que l'est pour nous l'électricité. Certains le considèrent comme un territoire dynamique

en constante évolution, ou un territoire à conquérir, maîtriser ou contrôler. Pour d'autres, il est un domaine où le pouvoir peut s'exprimer et s'exercer, ou une source d'enrichissement personnel ou économique, légal ou non, ou encore une citadelle de la liberté – ou un champ de bataille. En réalité, il constitue à divers égards une sorte de patchwork de tous ces éléments pris ensemble. Globalement, il reflète notre réalité politique, économique et sociale, et n'est ni meilleur ni pire que cette réalité. Il témoigne de la réalité de la mondialisation, dont l'unification technico-économique fait partie intégrante.

S'il est difficile de définir le concept de territoire dans un monde hyperconnecté, il est encore plus difficile de le faire en relation avec la sécurité et la défense des territoires numériques. Les modes traditionnels de penser la sécurité ne sont plus applicables. Par suite de l'évolution des technologies (données sur mobile, dispositifs intelligents et informatique en nuage) et de leur utilisation (réseaux sociaux, paiement électronique, etc.), il est devenu impossible de mettre en place un périmètre de sécurité pour isoler les sources d'information. La mise en oeuvre de techniques de chiffrement freine souvent l'intégration des services, rend l'utilisation moins conviviale et diminue la qualité de fonctionnement. Le chiffrement reste assez peu employé et n'inspire guère confiance. L'affaire "Heartbleed"[11] en avril 2014 a révélé l'existence d'une importante faille de sécurité dans la mise en oeuvre de l'une des solutions les plus couramment utilisées dans les services web. Une nouvelle fois, le public a pris conscience de failles dans les services censés améliorer la robustesse des infrastructures et la sécurité des transactions électroniques.

Une confiance fragile

Sur Internet, les particuliers, les organisations et les Etats sont confrontés à de nouvelles cybermenaces et à de nouveaux risques. Le cyberespace connaît des pannes et des dysfonctionnements et est exposé à des criminels et à des agresseurs. Trop souvent, les cybermenaces sont insuffisamment reconnues ou mal comprises et font peur. En outre, on ne peut pas toujours prévoir quand et comment elles deviennent réalité, ni les réactions en chaîne ou les séquences d'événements qu'elles suscitent, pas plus qu'on ne peut en identifier les auteurs ou ceux qui se cachent derrière eux.

Depuis les affaires Wikileaks en 2010[12] et Prism en 2013[13], nous savons avec certitude que, dans l'univers numérique, le secret n'existe pas et que nous sommes suivis, observés et surveillés à distance par des moyens électroniques. Il nous faut reconnaître

---

11 www.schneier.com/blog/archives/2014/04/heartbleed.html

12 www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points.

13 washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

que cette surveillance s'exerce à très grande échelle et que nous y participons activement par l'utilisation de certains services web ou de nos téléphones mobiles. Nous ne pouvons plus ignorer que nos données personnelles, nos comportements, nos goûts et nos relations constituent le socle des modèles économiques adoptés par la plupart des fournisseurs de services dits "gratuits", que ces informations intéressent au plus haut point.

Aujourd'hui, les capacités de surveillance, de la part tant des technologies de l'information que de leurs fournisseurs, entraînent une crise de confiance globale, dans les unes comme dans les autres. Nous prenons conscience de la fragilité des environnements numériques, de la fragilité de notre confiance dans les techniques et les professionnels de la cybersécurité.

Pour rétablir la confiance dans les infrastructures TIC, il faut au préalable surmonter des difficultés à plusieurs niveaux:

- Difficultés qu'ont les particuliers, les organisations et les autorités à comprendre les menaces, à identifier les risques et à mettre en place des contre-mesures efficaces et efficientes, à quoi s'ajoute la nécessité de débloquer suffisamment de fonds pour lutter contre la cybercriminalité.
- Difficulté à empêcher les abus de toute sorte dans le cyberespace et à gérer les incidents, voire les crises, qui peuvent en résulter.
- Difficulté à protéger les particuliers, les consommateurs, les enfants, ainsi que notre patrimoine numérique et nos secrets.
- Difficulté à exprimer nos besoins en matière de cybersécurité et à établir les droits et obligations des différents acteurs, et à veiller à ce qu'ils soient respectés.

Surmonter les difficultés et insuffisances: identifier les besoins réels

Le cyberespace expose à de nouvelles vulnérabilités, qui peuvent être exploitées par des menaces toujours plus variées. L'actualité nous le rappelle chaque jour en donnant des informations sur des vols de données, pertes de contrôle, prise en otage de sources d'information contre rançon, piratages de comptes mail, escroqueries de toutes sortes et abus de confiance. Des termes comme "hackeurs", "Anonymous", ou "virus informatique" sont entrés dans le langage courant et les cybernuisances sont une réalité pour tous les internautes.

- Il nous faut tenir compte des insuffisances:
- sur le plan des mesures de sécurité en vigueur;
- sur le plan de la résilience des infrastructures et de la capacité de gérer les crises complexes qui peuvent survenir;

- sur le plan des mesures prises pour sensibiliser le grand public et dans le cadre des structures éducatives, de l'école primaire à l'université, y compris de l'apprentissage tout au long de la vie, et sur le plan des tentatives d'élaboration de solutions "nationales";
- sur le plan des cybercompétences et des ressources humaines dans chaque domaine d'activité;
- sur le plan des moyens attribués aux systèmes judiciaires et à la police pour faire face à l'expansion de la cyberdélinquance et de la cybercriminalité.

Il faut aussi souligner l'insuffisance des connaissances et d'une approche globale, pluridisciplinaire et systématique de la gestion des cyberrisques, ainsi que celle de la coopération et de la collaboration nationales et internationales, de l'entraide judiciaire et des partenariats entre secteur public et secteur privé, ainsi qu'entre civils et militaires.

J'ai évoqué les concepts de fragilité, de difficulté et d'insuffisance, qui sont tous liés à la notion de complexité. Je veux parler de la complexité d'une tâche qui revêt des dimensions politiques, diplomatiques, économiques, de gestion, judiciaires, technologiques et humaines, pour protéger contre tous les cyberrisques. Nous le savons maintenant, la société de l'information doit reposer sur la confiance et la sécurité, la surveillance n'est pas synonyme de sécurité, et la sécurité doit être étayée par des mesures de contrôle fiables et conformes à un cadre juridique adapté, et non pas imposée par des technologies, des fournisseurs ou des acteurs du marché en position de force. Il faut aussi poser des limites face à la mondialisation et à l'impérialisme technologiques.

Il faut bien comprendre que les cyberrisques font désormais figure d'urgence planétaire, amplifiant tous les risques traditionnels liés, par exemple, aux installations nucléaires, à la pollution ou au terrorisme, et qu'il est **indispensable** d'agir en conséquence. Il est primordial d'allier volonté individuelle et volonté collective, d'élaborer et de mettre à disposition des moyens pour relever les défis de la sécurité au XXIème siècle.

Il est donc urgent de dégager des ressources et de mettre en place des structures organisationnelles et des procédures ad hoc à tous les niveaux – cantonal, régional, national et international – afin de maximiser les avantages des technologies de l'information et de tirer parti des nouvelles possibilités qu'elles offrent. En parallèle, il faut remédier à leurs inconvénients, essentiellement pour assurer la compétitivité et la sécurité économique des pays, dont notre bien-être à tous est tributaire.

Il est urgent de disposer d'un instrument international

Si on considère le cyberespace comme un bien commun, au même titre que la Terre, l'air, les mers ou l'espace, il est urgent d'en assurer la coordination, avec la coopération de toutes les nations.

Nous sommes convaincus qu'il est nécessaire et urgent de parvenir à un accord international traitant de manière cohérente et globale des questions de cybersécurité. Les organisations, les entreprises et les Etats font face à des risques non négligeables en lien avec la divulgation ou l'utilisation abusive et la destruction de données ou d'informations. De tels incidents, vus à l'échelle macroscopique, peuvent être considérés comme autant de menaces potentielles, non seulement pour la compétitivité ou la réputation d'une entreprise, mais aussi pour la sécurité publique ou la démocratie dans un pays.

Si l'on pense que le cyberespace fait de plus en plus figure de champ de bataille économique et militaire mondial, où les cyberconflits – reflets de la concurrence politique et économique – peuvent se déchaîner, l'heure est donc venue de définir et d'approuver en commun ce qui est ou non acceptable et d'élaborer un instrument international de contrôle efficace. Sans approche commune et accords internationaux, il sera impossible de mettre en place des mesures de sécurité pour protéger efficacement les ressources TIC (y compris les infrastructures essentielles de l'information), lutter contre la cybercriminalité et préserver les droits humains fondamentaux. Une telle démarche nécessite une détermination sans faille de tous les protagonistes et parties prenantes sur les plans national et international.

Des stratégies nationales et internationales devraient être en place, non seulement pour réagir aux cyberattaques – définir les moyens de riposte – mais aussi pour définir par anticipation des mesures visant à éviter les failles de sécurité et à empêcher les incidents indésirables. On peut, par exemple, instaurer une culture efficace de la cybersécurité en limitant le nombre de points faibles d'où partent les attaques contre les systèmes, en tenant systématiquement compte de tous les facteurs qui peuvent conduire, entre autres, à des comportements déviants, des crises, des actes de vengeance ou des délits, et en renforçant la mise en place de mesures complémentaires et concertées.

Tous ces problèmes ne peuvent être traités efficacement d'un point de vue exclusivement national. Tout comme le Protocole de Kyoto[14] est un accord international lié à la Convention-cadre des Nations Unies sur les changements climatiques, il serait utile de définir un Protocole mondial sur la cybersécurité et la cybercriminalité. Un tel instrument permettrait de limiter les risques et les menaces dans le cyberespace à une échelle véritablement universelle. Il devrait constituer un cadre de base pour que soient prises, sur les plans national et international, des mesures efficaces de lutte contre les cyberattaques, et devrait inclure une définition des comportements acceptables et inacceptables, ainsi que les moyens de contrôle nécessaires.

Encourager le dialogue international

En mai 2007, l'UIT a lancé le Programme international cybersécurité (GCA)[15], cadre de coordination internationale pour réagir face à la multiplication des attaques contre la cybersécurité. Afin d'aider l'UIT à élaborer cette stratégie, il a été établi un Groupe d'experts de haut niveau (HLEG), dont les membres étaient nommés par le Secrétaire général de l'UIT, compte dûment tenu de la diversité géographique et des compétences requises, afin d'assurer une représentation multipartite. Ce Groupe se compose de plus de cent spécialistes de réputation mondiale, venant de divers horizons[16]: représentants d'administrations membres de l'UIT, d'Etats Membres, du secteur privé, d'organisations régionales ou internationales, d'organismes de recherche et d'établissements universitaires[17]. En novembre 2008, l'UIT[18] a publié le *Rapport stratégique mondial* du Groupe HLEG[19], qui définissait des stratégies dans cinq domaines: mesures juridiques, mesures techniques et de procédure, structures organisationnelles, renforcement des capacités et coopération internationale. Ce programme établit un cadre de base en vue de l'élaboration de mesures efficaces sur les plans national et international, qui encouragent les pays à mettre en place des programmes nationaux de cybersécurité et à coopérer à l'échelle internationale. Ce programme doit être considéré comme une

---

14 unfccc.int/essential_background/kyoto_protocol/items/1678.php.

15 www.itu.int/osg/csd/cybersecurity/gca/index.html.

16 http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html.

17 Le Juge Stein Schjolberg (Norvège) en était le Président. Solange Ghernaouti était co-responsable des domaines de travail consacrés aux structures organisationnelles et au renforcement des capacités.

18 Par ailleurs, en 2008, l'UIT a créé le Partenariat multilatéral international contre les cybermenaces (IMPACT) – initiative internationale commune aux secteurs public et privé et visant à renforcer la capacité de la communauté internationale à prévenir les cybermenaces, s'en protéger et y riposter (www.itu.int/osg/csd/cybersecurity/gca/impact_index.html.

19 www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

première étape importante sur la voie d'une stratégie mondiale de la cybersécurité. Depuis lors, cette question fait l'objet de débats intensifs dans le monde entier[20].

La proposition de "Traité mondial sur la cybersécurité et la cybercriminalité. Contribution à la paix, à la justice et à la sécurité dans le cyberespace" est le fruit de cette longue période de concertation internationale[21].

Pour un instrument au service de la communauté internationale

Afin de contribuer à atteindre l'objectif universellement reconnu qui consiste à gérer les cyberrisques et à lutter contre les cyberattaques, la cybercriminalité et les utilisations abusives ou inappropriées de l'Internet, nous tenterons d'identifier la nécessité d'une nouvelle vision de la cybersécurité internationale, fondée sur un dialogue et des accords internationaux efficaces. Nous espérons ainsi contribuer à rendre le cyberespace et, au-delà, le monde réel, un peu plus pacifiques, justes et sûrs. On pourrait envisager la création d'un traité international, ou d'un ensemble de traités, en rapport avec le cyberespace.

Ce traité ou cet ensemble de traités au niveau des Nations Unies sur la cybersécurité et la cybercriminalité devrait poser les bases de la paix, de la justice et de la sécurité dans le cyberespace et faciliter l'élaboration d'une stratégie globale visant à dissuader les cybermenaces, d'où qu'elles viennent. La négociation d'un tel traité devrait permettre de définir une vision commune de tous les aspects de la cybersécurité dans les pays, à différents niveaux de développement économique.

Toutes les parties prenantes doivent parvenir à s'entendre sur ce qui constitue la cybercriminalité, le cyberterrorisme et d'autres cybermenaces – condition préalable indispensable à l'élaboration de solutions nationales et internationales visant à harmoniser les mesures en matière de cybersécurité. En outre, un accord contribuerait à réduire l'écart entre les perceptions de la cybersécurité, qui ne sont pas les mêmes

---

20 On trouvera de plus amples informations dans le document "The baseline review ICT-related process and events, Implications for international and regional security", ICT for Peace Foundation. Voir: http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security.

21 En 2009, le Juge Schjolberg et le Prof. S. Ghernaouti ont publié une première proposition de traité international sous forme d'ouvrage intitulé "A global treaty on cybersecurity and cybercrime: a contribution for peace, justice and security in cyberspace" ("Traité mondial sur la cybersécurité et la cybercriminalité. Contribution à la paix, à la justice et à la sécurité dans le cyberespace"), disponible sur www.cybercrimedata.net. Cet ouvrage a été présenté au Forum sur la gouvernance de l'Internet tenu à Sharm El Sheikh: www.intgovforum.org/cms/2009-igf-sharm-el-sheikh. Voir aussi Ahmad Kamal, The Law of CyberSpace. An Invitation to the Table of Negotiation. UNITAR, 2005. L'Ambassadeur Kamal était membre du Groupe permanent lorsqu'il a écrit cet ouvrage et l'UNITAR est un organisme des Nations Unies.

dans les pays développés et dans les pays en développement. Les comportements criminels dans le cyberespace étant répandus dans le monde entier, il est impératif d'harmoniser les législations relatives à la cybercriminalité, d'assurer l'efficacité de la justice internationale et de la coopération entre les polices, et de faire preuve d'une détermination sans faille en ce sens.

Un traité sur le cyberespace conclu au niveau des Nations Unies devrait consacrer le principe selon lequel les graves atteintes à la paix et à la sécurité sur l'Internet et dans le cyberespace sont des crimes en droit international, qu'ils soient ou non punissables en droit national. Nous sommes profondément convaincus que les atteintes les plus graves commises dans le cyberespace devraient être définies et sanctionnées par le droit international.

Il est à noter que la Convention du Conseil de l'Europe sur la cybercriminalité (2001), entrée en vigueur le 1er juillet 2004, marque un tournant dans la lutte contre la cybercriminalité[22]. Ce document n'est qu'un exemple d'initiative régionale, européenne en l'occurrence, et de nombreux pays préfèrent s'en servir uniquement comme d'un instrument de référence. Autrement dit, il reste nécessaire d'établir, dans un cadre mondial et au niveau des Nations Unies, un traité ou un ensemble de traités qui incluent les normes et principes largement acceptés dans ladite Convention, auxquels s'ajouteraient d'autres dispositions importantes[23]. En fait, comme le fait clairement apparaître le rapport stratégique du Président du Groupe UIT-HLEG, les mesures pertinentes sont liées aux dimensions juridiques, techniques et de procédure qui sont tributaires des structures organisationnelles, des capacités effectives et de la coopération internationale.

La négociation d'un traité international serait considérée comme faisant suite à la parution des rapports du Groupe HLEG et marquerait un pas en avant pour le Programme GCA de l'UIT, qui incite les pays à mettre en place des programmes nationaux de cybersécurité et à promouvoir la coopération internationale. Un traité de portée mondiale les obligerait à tenir leurs engagements.

---

22 www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

23 Plusieurs pays ne reconnaissent pas certains de ces normes et principes, en particulier le principe énoncé dans l'Article 32 sur l'Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public. La position de ces pays doit être respectée (Source: Rapport du Président du Groupe HLEG, UIT, 2008).

Perspectives d'avenir

L'édification d'un cyberespace sûr et fiable nécessitera des ressources et des compétences multiples. Ce projet devra reposer, non seulement sur des technologies et des procédures de gestion spécialisées, sur un cadre juridique précis qui soit applicable au niveau national et compatible sur le plan international, mais aussi sur des moyens de gouvernance et de contrôle reconnus et vérifiables à l'échelle internationale.

Certains principes fondamentaux devront être identifiés, adoptés et largement reconnus par la communauté internationale, comme ce fut le cas pour la Déclaration universelle des droits de l'homme en 1948[24].

Il ne sera pas simple de définir ces valeurs communes, compte tenu des différences de pays, de cultures, et des intérêts économiques et politiques. L'élaboration d'un traité international sera sans nul doute un travail de longue haleine. Il est d'autant plus urgent de créer dès aujourd'hui un mécanisme qui facilitera l'établissement d'un dialogue international susceptible d'aboutir dans des délais proportionnels à l'urgence des enjeux.

En dépit des difficultés liées à la négociation d'un tel traité et à la probabilité qu'il ne soit pas toujours respecté, comme l'illustre tristement l'exemple de la Déclaration universelle des droits de l'homme, cet instrument pourrait servir à lutter contre les comportements préjudiciables de particuliers, d'organisations ou d'Etats. Il devrait aussi empêcher de s'écarter des valeurs communes, ou à tout le moins, mettre en relief les divergences et autoriser, s'il y a lieu, des dédommagements par voie légale.

Une sorte de "traité de non-prolifération de la cybertechnologie" pourrait toutefois s'avérer insuffisant, dans la mesure où il réduirait les technologies de l'information à l'état d'outils militaires analogues à des armes. Mais les frontières entre militaire et civil ne sont pas clairement établies; les deux mondes utilisent les mêmes technologies et le même Internet, du plus jeune au plus âgé des internautes.

On pourrait établir une analogie avec le Traité de 1968 sur la non-prolifération des armes nucléaires[25], dont les avantages ne sont plus contestés, même si son application ne va pas sans difficultés; ce Traité a été inutile pour prévenir la catastrophe nucléaire de Fukushima en mars 2011, qui n'était pas le résultat d'opérations militaires. Par

---

24 www.un.org/en/documents/udhr/

25 Traité sur la non-prolifération des armes nucléaires. Ouvert à signature à Londres, Moscou et Washington le 1er juillet 1968. www.un.org/en/disarmament/instruments/npt.shtml

(UNODA Bureau des affaires du désarmement des Nations Unies: http://www.un.org/disarmament/

UNIDIR – Institut des Nations Unies pour la recherche sur le désarmement: http://www.unidir.org/html/en/home.html)

ailleurs, une organisation telle que l'Agence internationale de l'énergie atomique (AIEA) a fait la preuve de son utilité pour la coordination du suivi d'une catastrophe et la création ultérieure de mesures de sécurité. Une structure équivalente devrait exister et être appliquée pour le cyberespace, afin d'encourager le public à utiliser de façon sûre et pacifique les technologies de l'information et de la communication.

Cette analogie, certes audacieuse, avec les armes et les centrales nucléaires, ne s'étend pas à la nécessité d'adopter une politique globale face aux problèmes de sécurité du cyberespace. Ces problèmes justifient l'adoption d'un traité (ou d'un ensemble de traités) reconnaissant, entre autres, la dimension militaire de cette politique.

Le cyberespace abrite toutes sortes de délinquants dont les activités, comme le blanchiment d'argent ou le trafic d'êtres humains, touchent aux aspects aussi bien militaires que civils. En tout état de cause, est-il acceptable que les droits de l'homme n'y soient pas respectés?

L'Internet et le cyberespace sont devenus, dans le monde entier, des éléments de la civilisation que nous laisserons en héritage aux générations futures. Il est donc de notre devoir et de notre responsabilité, individuelle et collective, de définir d'un commun accord les valeurs communes que nous voulons promouvoir et de mettre en place et faire respecter des mécanismes de contrôle à cette fin.

Mesures de renforcement de la confiance

Chaque maillon de la chaîne numérique, et chaque pays, ont un rôle à jouer dans la cybersécurité et la cyberconfiance. La sécurité a un prix, mais l'insécurité et l'absence de confiance dans le numérique aussi. Aujourd'hui, ces coûts sont essentiellement supportés par les utilisateurs et la société en général, qu'il s'agisse de financer les systèmes policier et judiciaire de lutte contre la cybercriminalité, ou de la déstabilisation de l'économie causée par les cyberattaques, les fuites de données et le cyberespionnage. Les risques encourus sont divers: faillites d'entreprises, dégâts d'image, perte de confiance du client, perte de parts de marché et perte d'emplois.

Le cyberespace ne doit pas être un champ de bataille ou une zone de criminalité organisée, et c'est pourquoi nous devons collaborer à la recherche d'une solution visant à le sécuriser, pour nous et pour les générations futures. Je suis convaincue que nous y parviendrons au moyen d'un traité international, d'une véritable Déclaration des droits de l'homme (de la femme et de l'enfant) dans le cyberespace. Un tel traité contribuera à instaurer la confiance dans le cyberespace, pour autant que les particuliers, les organisations et les Etats aient la volonté et la détermination nécessaires pour le respecter et pour élaborer des pratiques en conséquence.

Même s'il faut être conscients des limites d'une telle entreprise et de la création d'un traité international supplémentaire, celui-ci aurait toutefois pour principal avantage de faire prendre conscience de la nécessité de renforcer la sécurité et la confiance.

Inscrit dans un ensemble de mesures de renforcement de la confiance, par exemple un traité, le dialogue international pourrait devenir:

- un moyen efficace pour communiquer et sensibiliser l'opinion aux questions de paix et de sécurité dans le cyberespace et dans le monde réel;
- un travail de référence qui encourage les acteurs économiques et institutionnels (y compris la police et le pouvoir judiciaire) à adopter de bonnes pratiques;
- un point de départ à la création de services et de technologies qui permettent de renforcer la confiance et les mécanismes judiciaires et de mieux lutter contre la cybercriminalité;
- un instrument qui aide à faire respecter un minimum de sécurité sur l'Internet et qui abaisse le seuil de tolérance des populations à la cyberviolence.

Conclusion

Le moment est venu de prendre des mesures pragmatiques pour préserver et protéger notre patrimoine numérique et le faire prospérer, pour contribuer au développement de la sécurité économique, de l'emploi et de la compétitivité. Ce sont là quelques-uns des impératifs et des enjeux pour les particuliers, sans qu'il soit nécessaire d'insister sur le respect des droits fondamentaux qui est, en dernière analyse, identique sur le plan de la sécurité, avec des degrés d'importance différents, pour les particuliers, les organisations et les Etats.

Ensemble, nous serons plus forts et pourrons améliorer la cohérence et l'homogénéité des mesures de sécurité. Les territoires numériques ne peuvent plus être protégés isolément les uns des autres, car les virus, électroniques comme biologiques, ignorent les frontières, de même que les cyberattaques, qui infiltrent de nombreuses infrastructures, y compris celles qui appartiennent à nos alliés et voisins traditionnels.

La protection des infrastructures, le développement de la résilience, la lutte contre la cybercriminalité et la consolidation des positions nationales en matière de cybersécurité et de cyberdéfense – voilà ce que les citoyens bien informés devraient aujourd'hui exiger, dans l'optique de la création d'une société de l'information viable sur la durée.

Comme le dit la sagesse populaire, c'est par beau temps qu'il faut construire le toit qui nous protégera de la pluie: en d'autres termes, dépêchons-nous d'agir avant qu'il ne soit trop tard!

Il serait à la fois naïf et dangereux d'attendre que les failles disparaissent d'elles-mêmes et que les menaces qui exploiteront ces failles se matérialisent. Nous devons anticiper et renforcer la sécurité pour éviter, entre autres, que d'autres s'accaparent nos ressources d'information, connaissances, propriété intellectuelle et données personnelles, ainsi que d'éviter que certains acteurs renforcent leur hégémonie, qu'ils soient des entités légitimes ou des associations de malfaiteurs.

Sans vouloir faire preuve de naïveté ou de paranoïa, on peut dire que le moment est venu d'intégrer dans nos stratégies de sécurité le fait que l'Internet a modifié en profondeur les façons d'exercer le pouvoir et a créé de nouveaux types de conflit entre les particuliers, les institutions, et les Etats.

1.2 Les normes, règles et principes applicables à l'Internet vues par les Nations Unies et les Etats Membres: évaluation du rapport du Groupe d'experts gouvernementaux des Nations Unies

Par Henning Wegener

Il apparaît clairement, à la lecture des analyses précédentes, que les pays ont pris conscience de la nécessité de mettre de l'ordre dans le cyberespace et, à l'intérieur de cet espace, d'établir des normes de comportement responsable des pouvoirs publics et des autres parties prenantes. Même si, au départ, le cyberespace n'était pas en soi livré à l'anarchie, il a continué d'être caractérisé par l'absence de cadre juridique détaillé et consensuel applicable non seulement aux Etats, mais aussi à toutes les parties prenantes. L'essentiel était, et est toujours, d'adopter au fil du temps un comportement convivial incitant à la création de normes universelles. Dans l'exercice de cette tâche, et dans cette optique, la présente contribution met l'accent sur les activités récentes de l'Organisation des Nations Unies, en particulier sur les résultats des travaux d'un Groupe spécialisés d'experts gouvernementaux.

Depuis lors, plusieurs tentatives concertées ont eu lieu ces dernières années pour réguler le cyberespace: la série de résolutions adoptées par les Nations Unies depuis 1998; l'adoption en 2001 de la Convention de Budapest sur la cybercriminalité; le processus du SMSI; des législations nationales utiles sur le plan des régimes de droit civil applicables aux délits civils et dommages, le droit pénal; les règlements administratifs, et le droit international privé applicable. De l'avis général, ce n'est que depuis 2008 qu'on observe une activité diplomatique systématique et approfondie dans le domaine du cyberespace. Depuis lors, on a observé une grande quantité d'activités dans plusieurs

pays, et une profusion étonnante d'initiatives et de processus qui, confondus, font évoluer différemment le consensus sur les besoins de normes. Il serait trop long d'énumérer et d'analyser ici[26] toutes ces nouveautés, mais il est à espérer qu'elles contribueront à un processus "par étapes, chacune d'elles préparant la suivante"[27]. Nombre d'entre elles ont recours à des moyens utiles comme l'élaboration de mesures propres à renforcer la confiance ou de codes de conduite, ou encore les techniques de négociation analysées dans d'autres parties de la présente publication[28].

Fort heureusement, ces activités ont déjà donné lieu à un grand nombre d'excellents rapports analytiques qui facilitent l'examen et la poursuite des travaux[29].
Les deux années 2013 et 2014 ont été particulièrement fertiles à cet égard. Elles ont vu la parution, entre autres, d'au moins trois documents fondamentaux: Le Manuel de Tallinn sur l'applicabilité du droit international aux cyberconflits[30], le document de NetMundial sur la gouvernance de l'Internet[31], et surtout le rapport du Groupe

---

26 Au lieu de fournir une liste complète, nous faisons référence ci-après aux documents les plus pertinents dans leur contexte.

27 Doc. A/68/98, p.11.

28 Le concept de codes de conduite, ou selon certains, de transparence, et de mesures propres à renforcer la confiance, a visiblement remplacé la fascination qu'exerçait autrefois le concept de Convention globale sur le cyberespace, comparable à la Convention des Nations Unies sur le droit de la mer établie en 1982. On s'est peu à peu rendu compte que les obstacles à la création d'un tel instrument étaient gigantesques. Le cyberespace pourrait s'avérer encore plus complexe que le monde des océans. Les technologies numériques et leurs utilisations continuent à progresser rapidement. L'élaboration d'un traité à valeur universelle serait freinée par des divergences encore plus nettes dans les positions de chaque pays. La négociation d'un traité prendrait beaucoup de temps, de même que les procédures de ratification sur le plan national. La durée du processus serait disproportionnée par rapport à la nécessité urgente de combler le vide juridique et face à la prise de conscience générale du fait que la menace de cyberconflit et de cyberdégâts irréparables s'aggrave dangereusement. Ainsi, alors qu'un traité/une législation universels sur le cyberespace seraient préférables, à ce stade et pour le moment, une autre méthode serait souhaitable pour des raisons pratiques.

29 Camino Kavanagh, Tim Maurer et Eneken Tikk-Ringas "**Baseline Review. ICT-Related Processes and International and regional Security** (2011-2013)" www.ict4peace.org, Genève, mars 2014; *Annegret Bendieck,* "Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit", DGAP, Berlin, décembre 2013. Voir aussi *Henning Wegener,* "Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures", Erice, août 2012, sur www.unibw.de/infosecur

30 "Manuel de Tallin sur l'applicabilité du droit international à la cyberguerre", édité par Michael N. Schmitt. Etabli par un Groupe international d'experts, à l'initiative du Centre d'excellence de coopération pour la cyberdéfense de l'OTAN. Cambridge University Press 2013.

31 Déclaration multi-parties prenantes de NetMundial, http://netmundial.br.

intergouvernemental d'experts des Nations Unies, établi à l'été 2013 et soumis à l'Assemblée générale des Nations Unies à sa 68ème session[32]. Ces trois documents de base sont analysés dans le présent ouvrage. Le présent article est plus particulièrement centré sur le troisième d'entre eux, mais fait aussi, si nécessaire, référence aux deux autres.

Le rapport établi en 2013 par le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale n'est pas un document unique en son genre. Ce groupe avait pour mandat "[….] de continuer d'examiner les risques qui se posent dans le domaine de la sécurité de l'information ainsi que les principes internationaux pertinents, et de proposer des mesures de coopération qui pourraient renforcer la sécurité des systèmes téléinformatiques mondiaux, y compris les normes, règles ou principes de comportement responsable des Etats et les mesures visant à renforcer la confiance en ce qui concerne le cyberespace, ainsi que l'étude des principes susceptibles de renforcer la sécurité des systèmes mondiaux dans le domaine de la téléinformatique". Ce document s'appuie sur les résultats obtenus par le 2ème Groupe d'experts gouvernementaux, qui avait établi un rapport en juillet 2010 (Document A/65/201). Il tire aussi parti des évolutions amorcées par une série de conférences multi-parties prenantes organisées avec l'appui de gouvernements, de Londres à Budapest, et particulièrement consacrées aux débats sur les normes et le renforcement de la confiance, comme indiqué dans le mandat du Groupe d'experts. Les nombreuses consultations menées au sein d'organisations régionales et d'instances internationales de premier plan, comme l'Assemblée générale des Nations Unies, l'Union européenne, le G8, l'OTAN et les organisations régionales des Nations Unies, ont, elles aussi, alimenté les débats. Dans son rapport, le Groupe d'experts se fait l'écho de points de vue communs, qui évoluent, et dans certains cas, des consensus qui se dégagent. Il marque en même temps une nouvelle étape dans la mesure où des problèmes déjà examinés dans d'autres instances sont présentés sous un autre jour, de manière synthétique, par un groupe représentatif de gouvernements du monde entier. La poursuite du processus est en outre assurée par la création d'un nouveau (4ème) Groupe d'experts, composé d'un encore plus grand nombre de pays (20, en l'occurrence), chargé d'examiner plus avant les recommandations du rapport (A/RES/68/243), et dont le mandat élargi inclut l'examen "[…] des questions de l'utilisation des technologies de l'information et des communications dans les conflits". La poursuite de ce processus est d'ailleurs assurée dans le cadre de différentes manifestations internationales qui ont un rôle de suivi: en 2015, les Pays-Bas accueilleront une série de grandes conférences sur le cyberespace, dans le cadre desquelles chaque gouvernement contribuera à faire encore progresser ce consensus. La Conférence de Séoul sur le cyberspace, tenue en octobre 2013, immédiatement après la parution du rapport du Groupe d'experts, a réuni quelque 90 Etats et a

32 Document ONU A/68/98

approuvé par consensus la plupart des recommandations contenues dans le rapport, dans le Cadre et les engagements de Séoul pour un cyberespace ouvert et sûr. Même si le rapport du Groupe d'experts n'a – tout comme la Déclaration multi-parties prenantes de NetMundial – pas force obligatoire, il imprime une dynamique qui permet d'espérer que le consensus international n'en restera pas là.

Les deux derniers chapitres du rapport du Groupe d'experts contenant des recommandations sont pour nous d'un intérêt capital. Ils comportent des recommandations sur les normes, règles et principes de comportement responsable des Etats, ainsi que des recommandations sur les mesures visant à renforcer la confiance et les échanges d'informations. Etant donné que le rôle de ces mesures dans une nouvelle vision de la cybersécurité internationale fait l'objet d'une autre contribution à la présente publication, nous n'en traiterons que brièvement.

Les mesures visant à renforcer la confiance ont essentiellement pour vocation de lutter contre les menaces, d'améliorer la transparence, de permettre de prévoir le comportement des Etats. Ces mesures laissent une grande marge de manoeuvre, sont d'application volontaire, permettent une participation à géométrie variable (possibilité de participation d'acteurs autres que ceux du secteur public) et prévoient un suivi. Contrairement à ce qui se passe avec l'élaboration de traités – qui est un processus cohérent – les participants sont libres d'adopter des solutions partielles et de leur donner effet immédiatement et indépendamment, ou conjointement avec d'autres parties prenantes partageant les mêmes vues. Les mesures de renforcement de la confiance adoptées par les Etats n'ont pas besoin d'être ratifiées; elles sont faites pour servir d'exemples et ont au maximum – et dans le meilleur des cas – valeur obligatoire sur le plan politique. Elles sont donc idéales pour promouvoir la recherche du consensus international, de manière évolutive. Un ensemble bien négocié de telles mesures, adoptées par un nombre suffisant de personnes, peut enclencher un processus de changement progressif et d'amélioration de la prise de conscience. Une meilleure compréhension des normes de comportement peut encourager à aller plus loin.

Le concept de mesures de renforcement de la confiance, qui est né dans le contexte de la confrontation Est-Ouest, dans le cadre de ce qui était alors la CSCE et des Nations Unies, a aujourd'hui une application universelle[33].

---

33 Concernant les débuts de ce concept en Europe et au-delà, voir Henning Wegener "CBMs: European and Global Dimensions", dans: F. Stephen Larrabee and Dietrich Stobbe, réd., "Confidence-Building Measures in Europe", Institute for East-West Studies, New York, 1983. Les lignes directrices adoptées par les Nations Unies sont réimprimées dans le document des Nations Unies A/S15/3. Pour d'autres applications, voir par exemple, le Document de Montreux sur les obligations juridiques pertinentes et les bonnes pratiques pour les Etats en ce qui concerne les opérations des entreprises militaires et de sécurité privées opérant pendant les conflits armés www.icrc.org, ou le projet de code de conduite pour les activités menées dans l'espace extra-atmosphérique, http://register.consilium.europa.eu

Les recommandations contenues dans le rapport du Groupe d'experts sont centrées sur la coopération internationale, la transparence, les échanges d'informations urgentes sur le plan international, les procédures d'alerte avancée 24 heures sur 24 et 7 jours sur 7 et les mécanismes CERT, l'harmonisation des prescriptions légales, l'application des lois, le dialogue institutionnalisé et d'autres considérations "pratiques". Elles mettent aussi en avant la nécessité de faire participer le secteur privé et la société civile, s'attachant ainsi à promouvoir le concept de multiples parties prenantes. Ces recommandations sont inscrites dans des cahiers des charges préconisant un renforcement de la confiance dans d'autres activités internationales et s'inspirent de documents tels que le Programme mondial cybersécurité de l'UIT, qui définit des tâches en matière de coopération mondiale aboutissant à "[…] un cadre pour une stratégie mondiale multi-parties prenantes de coopération et de dialogue au niveau international".

Parmi les mesures recommandées, nombre d'entre elles s'inspirent aussi de celles qui ont été présentées par le G8 en 1998, de la Décision-cadre de l'Union européenne en 2003, ou du chapitre pertinent de la Convention de Budapest. On relèvera l'intérêt tout particulier de la Série initiale de mesures de confiance de l'OSCE visant à réduire les risques de conflit découlant de l'utilisation des technologies d'information et de communication[34], récemment adoptée par le Conseil permanent de l'OSCE. En effet, cette organisation, composée de membres représentant aussi bien l'Est que l'Ouest, englobe un grand nombre de nations situées sur un vaste territoire et qui affichent habituellement des points de vue différents. Sous l'angle non gouvernemental, l'analyse la plus complète et la plus systématique du renforcement des mesures de confiance dans le cyberespace est sans aucun doute la compilation effectuée par ICT4Peace, à Genève en 2013, en partie sur la base des résultats de la conférence convoquée à Zurich par la même excellente organisation[35].

Les recommandations relatives aux normes, règles ou principes sont peut-être même encore plus utiles pour la gestion du cyberespace et de la cybersécurité; il faut donc les examiner plus en détail. Il faut aussi démontrer les lacunes et les ambigüités du texte et, à partir d'une première analyse, signaler les tâches toujours en suspens et les difficultés qui attendent le 4ème Groupe d'experts – et d'autres instances travaillant sur la cybersécurité – dans ses travaux.

Le fait que les représentants gouvernementaux des cinq membres permanents du Conseil de sécurité de l'Organisation des Nations Unies, ainsi que de l'Inde et du Japon, se soient associés au consensus, témoigne de L'importance de cette brève liste de normes et principes essentiels. En dépit de son caractère non contraignant, il s'agit donc d'un document qui fait autorité.

---

34 OSCE, Document PC.DEC/1106 du 3 décembre 2013.

35 "Confidence Building Measures and International Cyber Security", www.ict4peace.org.

Il a été souligné à plusieurs reprises que la conclusion du Groupe, selon laquelle le droit international, en particulier la Charte des Nations Unies, s'applique pleinement à l'utilisation des TIC, revêt une importance particulière. Ce principe avait déjà été évoqué dans plusieurs accords internationaux, mais jamais de façon aussi nette. Il s'agit là d'un progrès décisif, malgré l'adjonction immédiate de deux phrases signalant qu'il faut encore examiner la façon dont ces normes s'appliquent au comportement des Etats et que de nouvelles normes adaptées aux spécificités des TIC pourraient être élaborées dans l'avenir.

Ces précautions reflètent des différences bien connues et persistantes parmi les grands pays quant à la conception de la gestion des TIC sur le plan mondial. Les rédacteurs du rapport ont donc dû, tout au long de celui-ci, faire preuve d'esprit de compromis. Le paragraphe sur l'applicabilité du droit international est donc immédiatement suivi d'un paragraphe affirmant l'applicabilité de la souveraineté des Etats aux activités et infrastructures en rapport avec les TIC relevant de la compétence de l'Etat.

La réaffirmation de l'applicabilité du droit international dans le cyberespace s'étend, comme indiqué plus loin dans le texte, au respect des droits de l'homme et des libertés fondamentales au titre des conventions internationales pertinentes. Même s'il est déjà rappelé dans de nombreux accords internationaux depuis la tenue du SMSI, ce principe est d'une grande importance pour l'avenir de la liberté sur l'Internet et la lutte contre la censure de l'Internet par les gouvernements.

L'applicabilité de la Charte des Nations Unies s'étend aussi à ses dispositions fondamentales relatives au maintien de la paix et de la sécurité internationales, à l'injonction à s'abstenir de recourir aux menaces ou à la force, et au droit à l'auto-défense contre les cyberattaques armées. Cependant, dans l'attente d'un "complément d'étude", le rapport n'aborde pas la question de l'utilisation hostile des TIC. Même s'il a certainement connaissance du projet de code de conduite international pour la sécurité de l'information présenté en 2011 par la Russie, la Chine et d'autres pays[36] – document expressément cité dans le chapitre sur les recommandations et les normes – le Groupe n'a pas inclus l'équivalent du projet antérieur de norme, comme suit: "Ne pas utiliser les technologies de l'information et de la communication, y compris les réseaux, afin de mener des activités hostiles ou des actes d'agression et de menacer la paix et la sécurité internationales, ou diffuser l'arme informationnelle ou les technologies correspondantes". Il s'agit là d'une omission regrettable, du point de vue de l'auteur du présent article. Néanmoins, les autres normes et principes énoncés sont tout à fait louables et théoriquement incontestables, en particulier les recommandations concernant le renforcement de la coopération contre l'utilisation des TIC à des fins criminelles ou terroristes, l'harmonisation des approches juridiques et la collaboration en vue de l'application des lois ainsi qu'entre les parquets.

---

[36] A/66/359.

Il faut aussi se féliciter de la liste des normes et principes dressée au paragraphe 23 du rapport: les Etats sont tenus d'honorer leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables – même s'il est bien difficile de définir les auteurs des actes malveillants commis dans le cyberespace. Ils s'interdisent d'utiliser leurs agents pour commettre de tels actes et "veillent à ce que" des agents non étatiques n'utilisent pas leur territoire pour faire un usage illégal des outils informatiques. Le fait qu'un grand nombre de pays aient pour obligation d'adopter ces normes et de les transposer dans les législations nationales pourrait constituer un instrument efficace dans la lutte contre les activités des opérateurs de botnets et des gangs de cyberdélinquants. En outre, il est à espérer que les pressions internationales facilitent l'application sur le plan international des mesures nécessaires pour faire appliquer les lois.

Enfin, le texte fait référence au rôle du secteur privé et de la société civile dans le renforcement de la cybersécurité, "notamment en ce qui concerne la chaîne logistique des produits et services informatiques". Il nous rappelle que la cybersécurité, au niveau de l'ensemble de la société, implique la participation de multiples parties prenantes, dont les responsabilités vont au-delà du "comportement responsable des Etats".

Considérées dans leur globalité, les différentes sections du rapport – outre la partie consacrée aux normes et principes et le chapitre sur les mesures de renforcement de la confiance, il compte aussi un chapitre sur les mesures de renforcement des capacités qui contient des recommandations utiles, quoique moins passionnantes – constituent indiscutablement un progrès. Le rapport n'élimine pas certaines divergences fondamentales entre les pays à propos de la gestion future du cyberespace, mais les atténue. Les différences quant aux conceptions de base posent un problème épineux, surtout quand l'on sait qu'à sa prochaine réunion, le Groupe d'experts "étudiera plus avant" le début de consensus qui se dégage et entreprendra d'établir une recommandation détaillée.

Pourtant, ce rapport, qui s'inscrit dans le prolongement d'une série de grandes conférences internationales (Londres, Budapest, Séoul, etc.) et des travaux d'organisations régionales et internationales, consacre une double stratégie: d'une part, élaboration de mesures de renforcement de la confiance et d'autre part, élaboration de normes et de principes en vue de l'établissement d'un – ou de plusieurs – code(s) de conduite dans le cyberespace. Quelles que soient les modalités de négociation qui seront adoptées, la stratégie retenue rendra le comportement de l'Etat plus prévisible, laissera une certaine marge de manoeuvre, sera d'application volontaire, permettra une participation à géométrie variable (Etats et instances non étatiques) et facilitera le suivi: à la différence de ce qui se passe dans un processus cohérent de négociation de traité, les participants seraient libres d'adopter des solutions partielles et de les mettre en application sans tarder et indépendamment ou en association avec d'autres parties

prenantes partageant les mêmes valeurs. Or, le Groupe d'experts n'est parvenu qu'à un consensus partiel, et la tâche du Groupe suivant sera immense.

Ce Groupe, créé fin juillet 2014, a élu Président le représentant du Brésil, a mis au point un calendrier de travail et a réparti les tâches entre ses 20 experts gouvernementaux, qui vont maintenant établir ou réviser leurs positions et présenter des projets de contribution en conséquence. Le Groupe se réunira une nouvelle fois en janvier 2015 afin de pouvoir présenter son rapport avant l'été 2015.

L'une des tâches essentielles – et les plus complexes – sera pour le groupe de définir plus en détail les règles de droit international relatives à la sécurité et à la paix internationales, notamment de définir ce qui constitue une "attaque armée" dans le cyberespace, ce qu'est la souveraineté dans ce même espace, comment les utilisations hostiles de la cybertechnologie ("cyberarmes", y compris les logiciels malveillants conçus pour attaquer et endommager des infrastructures militaires) peuvent être endiguées et intégrées dans un cadre réglementaire. Ces questions, qui se posent à nous depuis le début de l'ère de l'informatique, sont de plus en plus préoccupantes. La réalité actuelle est qu'un nombre croissant d'Etats se livrent à une course effrénée aux cyberarmements, sans que l'on sache comment leur imposer des limites sur le plan juridique ou politique.

Le Manuel de Tallinn – qui sera analysé dans une autre partie du présent ouvrage – offre sans nul doute des idées et lignes directrices intéressantes permettant d'établir des analogies avec le droit international classique. Toutefois, il a été rédigé par un groupe d'experts juristes d'inspiration principalement "occidentale", et souffre de l'absence de perspectives plus mondialisées. Une évaluation critique de ce Manuel fait par ailleurs apparaître le problème suivant: une analyse qui prend pour point de départ le droit des conflits armés a tendance à considérer comme une option ordinaire les utilisations hostiles ou militaires de la cybertechnologie, même si les auteurs du Manuel énoncent plus ou moins clairement les limites et modalités de cette utilisation potentielle. Il n'est donc pas surprenant que ce Manuel, en dépit de son libellé prudent, ait été interprété par beaucoup comme un "appel à la cyberguerre". Il aurait évidemment été souhaitable d'introduire une mise en garde soulignant le refus catégorique de la cyberguerre et des dangers qu'elle comporte.

Une autre difficulté a trait au caractère – par nécessité – général des recommandations du rapport. Dans chaque cas, il sera d'autant plus difficile de les mettre en pratique et de s'acquitter des obligations correspondantes que l'intégration des divers processus régionaux et de l'ensemble des parties prenantes doit être gérée dans l'idée d'obtenir des résultats compatibles.

Dans ce contexte, la création d'une ou de plusieurs tribune(s) servant de cadre à des discussions intensives, puis à des négociations, est une tâche complexe. Dans son rapport, le Groupe d'experts recommande d'établir un dialogue institutionnel régulier

faisant intervenir un grand nombre de participants, sous l'égide des Nations Unies, ainsi qu'un dialogue dans le cadre d'instances bilatérales, régionales et multilatérales et d'autres organisations internationales. Cette recommandation va dans le bon sens, mais est encore trop vague pour permettre la prise de décisions rapide. Il serait sans doute judicieux de restreindre les choix institutionnels en convenant d'abord des critères que devrait remplir cette tribune (inclusion et ouverture, pleine participation d'un grand nombre de parties prenantes, fourniture d'un appui par un secrétariat international disposant de compétences dans le domaine des TIC, etc.). Il serait nettement préférable d'avoir une tribune unique à vocation universelle. Par ailleurs, des initiatives sont déjà lancées au niveau régional, et il conviendrait de profiter de la dynamique ainsi créée. Une conférence autonome des Etats, capable d'établir son propre règlement intérieur et les modalités d'une large participation des parties prenantes pourrait constituer une instance appropriée.

Pour en revenir au chapitre du rapport présentant des recommandations sur les normes, règles et principes, il faut signaler, malgré tout le respect que nous avons pour ses auteurs, que, compte tenu du contexte politique aux Nations Unies et de la nécessité de parvenir à un consensus dans des délais serrés, la liste qu'ils dressent est forcément sélective, et même incomplète. Il est à espérer que le 4ème Groupe d'experts examinera de près d'autres normes et principes récemment proposés[37].

Il est particulièrement nécessaire d'établir des normes plus précises dans les domaines clés de la sécurité, de la cyberstabilité et de la cyberpaix[38]. Diverses lacunes restent à combler, par exemple dans les domaines suivants: appel à conclure un accord contraignant sur le principe fondamental selon lequel une cyberattaque dirigée contre un autre Etat, soit directement, soit par l'intermédiaire de délinquants recrutés à cette fin, constitue une violation du droit international; engagement pris par tous les Etats de ne pas avoir recours en premier à des cyberarmes contre un autre Etat, sous réserve de ne pas avoir été attaqués par des armes conventionnelles. Les Etats devraient aussi souscrire, sur le plan national et international, à une politique de prévention des cyberconflits, privilégiant la cyberdéfense, restreignant et délégitimant le développement, l'utilisation et l'exportation de cybermoyens offensifs, notamment les logiciels d'attaque spécialisés. Les infrastructures essentielles devraient être protégées, plus encore que ne le préconise le paragraphe 26 (e) relatif au renforcement de la coopération internationale, en vertu du principe selon lequel les Etats sont responsables

---

37 En complément des travaux des organisations régionales énumérées en partie au paragraphe 27 du rapport du Groupe d'experts, voir la référence antérieure aux travaux d'ICT4Peace (note de bas de page 6); l'article d'Henning Wegener (note de bas de page 3); les cinq principes en matière de cyberpaix énoncés par le Secrétaire général de l'UIT dans la Déclaration d'Erice sur les *principes régissant la cyberstabilité et la cyberpaix*, 2009, repris dans l'ouvrage *En quête de la cyberpaix*, p. 118.

38 Le mandat du 4ème Groupe d'experts, désormais constitué, met l'accent sur les scénarios de "conflit".

de la protection de ces infrastructures essentielles sur leur territoire national et les attaques visant ces infrastructures sont interdites, ce qui a pour objet d'assurer l'inviolabilité des structures numériques transnationales du Net. Autre principe passé sous silence: la responsabilité qui incombe aux Etats de protéger leurs ressortissants dans le cyberespace. Allant au-delà de la recommandation citée au paragraphe 23, il faudrait énoncer clairement qu'il est interdit d'utiliser des botnets et d'autres pratiques contraires aux règles et relevant de la cybercriminalité/cyberguerre, et que les Etats sont tenus de faire appliquer cette interdiction sur leur territoire national. Enfin, la neutralité continue à être un concept valable dans le cyberespace, et aucune cyberattaque – même en cas d'auto-défense – ne doit être perpétrée par l'intermédiaire des structures du Net dans des Etats neutres.

1.3 Le droit international s'applique-t-il au cyberespace?

Par Gábor Iklódy

L'ère numérique, qui ouvre des possibilités quasiment infinies, fait aussi planer de nombreuses menaces qui peuvent être à l'origine de perturbations profondes, voire de destructions. Le principal problème est de trouver comment protéger le cyberespace et lui conserver sa fiabilité pour qu'il demeure un environnement dans lequel nous pouvons naviguer librement et dont nous pouvons tirer pleinement parti – en nous préoccupant toutefois davantage de la sécurité. Pour ce faire, il nous faut trouver le juste équilibre entre liberté et sécurité. Nous ne devons ni négliger les risques en matière de sécurité, ni nous abriter derrière ce prétexte pour justifier des restrictions de la liberté et des libertés publiques. Pour que la confiance l'emporte, il importe de veiller à ce que les organismes publics respectent pleinement les impératifs de responsabilité démocratique dans leurs efforts visant à prévenir les activités délictueuses dans le cyberespace.

La confiance est capitale pour les particuliers comme pour les Etats dans leurs relations internationales – thème du présent ouvrage. Nous sommes aujourd'hui témoins d'une cyber "guerre froide" menée à grand renfort d'espionnage dans le cyberespace et d'investissements dans des capacités offensives, au premier chef de la part des pays avancés et disposant de ressources suffisantes.

Pour les militaires, il est essentiel de pouvoir manoeuvrer librement dans le cyberespace – nécessité qui est prise en compte dans un nombre croissant de stratégies de défense nationale, pour lesquelles le cyberespace constitue "un nouvel espace de guerre qui a acquis une importance aussi critique pour les opérations militaires que le sol, les mers

et l'espace"[39]. La conclusion est parfaitement claire: la guerre moderne se livre aussi dans le cyberespace, et dorénavant, tous les conflits à grande échelle se joueront aussi dans le cyberespace, ainsi qu'on l'a abondamment constaté ces dernières années.

Pour que l'on continue à avoir confiance dans le cyberespace, il importe d'instaurer une coopération dans le cadre de laquelle s'appliquent des règles couramment acceptées. Les normes internationales régissant le comportement des Etats sont des facteurs indispensables dans un tel environnement, mais elles ne sont pas suffisantes. Le cyberespace est un domaine spécifique faisant intervenir de multiples parties prenantes où les Etats ne sont qu'un acteur parmi d'autres. Plus encore que dans tout autre domaine, il est impératif dans le cyberespace d'établir et de maintenir un véritable partenariat public-privé. "C'est le secteur privé qui possède et exploite la plupart des infrastructures du cyberespace et c'est lui qui produit la technologie nécessaire. Le secteur privé représente la première ligne de défense, tandis que les entreprises privées et les scientifiques conçoivent l'environnement technologique de demain dans lequel les Etats vont opérer"[40]. Cela ne diminue en rien les responsabilités des Etats en matière de souveraineté, dont ils ne peuvent s'affranchir.

Il n'existe actuellement pas de dispositions de traité ou de normes traitant spécifiquement du cyberespace. Cela signifie-t-il pour autant qu'il doive être considéré comme un domaine non assujetti à réglementation, une sorte de jungle dans laquelle aucune norme ne s'applique? Est-il justifié d'affirmer qu'il est urgent d'élaborer une série de normes juridiquement contraignantes – et est-ce réalisable dans la pratique? Ou devrions-nous plutôt partir de l'hypothèse énoncée par le Secrétaire d'Etat aux Affaires étrangères du Royaume-Uni William Hague, pour qui: "Un comportement inacceptable hors ligne est aussi inacceptable en ligne, qu'il soit le fait de particuliers ou de gouvernements"[41].

Applicabilité du droit international dans le cyberespace

Les experts débattent depuis un certain temps de la question de savoir si les instruments internationaux mis au point pour les contextes traditionnels s'appliquent également dans le cyberespace. Ce débat, qui avait quelque peu perdu de sa vigueur après le 11 septembre 2001, lorsqu'on a préféré mettre l'accent sur la guerre contre le terrorisme, a fait un retour en force en 2007-2008. La nécessité de combattre le terrorisme a justifié à beaucoup d'égards le renouveau de ce débat, avec des questions d'une actualité

---

39 Politique de l'OTAN sur la cyberdéfense, Bruxelles, 8 juin 2010.

40 Gabor Iklody: Discours prononcé dans le cadre du NATO Information Assurance Symposium, 11 septembre 2012, Mons.

41 William Hague, Secrétaire d'Etat aux Affaires étrangères du Royaume-Uni, dans son discours du 11 novembre 2011 lors de la première Cyberspace Conference, organisée à Londres.

brûlante du type: "Comment attribuer les actes d'entités non-étatiques à un Etat?", ou "Quelles sont les responsabilités d'un Etat vis-à-vis des activités de groupes opérant sur son territoire et à l'origine d'attaques visant des biens situés dans un autre Etat?", "Comment utiliser la force légalement contre des entités non étatiques résidant dans un Etat différent?", ou encore "Peut-on avoir recours à la force pour prévenir une attaque potentiellement dévastatrice et si oui, selon quelles conditions?".

Il semblerait approprié d'élaborer un accord mondial et juridiquement contraignant qui énonce les principales normes à appliquer dans le cyberespace et décrive les conséquences du non-respect de ces normes. Mais à présent, cela n'est pas du domaine du possible, ni même du souhaitable, et ce pour plusieurs raisons. Premièrement, la situation évolue si vite qu'il serait pour ainsi dire impossible de convenir d'un ensemble complet et pérenne de normes relatives au cyberespace. Deuxièmement, il est indéniable que les positions nationales divergent sur des questions décisives ayant des conséquences pratiques, comme la définition de seuils, les moyens de réaction et de mise en application. Le fait de 'graver dans le marbre' notre interprétation actuelle du cyberespace et les éventuelles concessions que nous serions prêts à faire nous lierait en quelque sorte les mains et pourrait même s'avérer avoir un effet contre-productif (en particulier dans les pays ayant une culture plus légaliste). Troisièmement, la validité d'obligations légales dont l'application est pratiquement invérifiable est sujette à caution.

Comme le montre l'expérience dans d'autres domaines, par exemple pour le contrôle des armements et le désarmement nucléaire, si les parties se méfient les unes des autres, il est préférable de procéder par petites étapes afin de bâtir et de consolider la confiance progressivement plutôt que de placer la barre trop haut et d'essayer de passer en force. L'expérience acquise dans le domaine du contrôle des armes nucléaires est riche d'enseignements à cet égard. Des mesures qui laissent ouvertes les voies de communication, offrent une certaine transparence et contribuent à atténuer les tensions en temps de crise permettraient d'atteindre l'objectif recherché. Des initiatives bilatérales et régionales comme les travaux de l'OSCE sur la cyberconfiance et les mesures de renforcement de la sécurité vont dans le bon sens, mais témoignent aussi de la difficulté de parvenir à un accord, même si elles restent modestes et d'application strictement volontaire.

Cela ne signifie pas pour autant qu'il soit prématuré d'envisager dès maintenant des négociations et une coopération internationales. En complément des mesures de renforcement de la confiance pouvant ouvrir la voie à d'autres mesures plus strictes, il existe des domaines dans lesquels des activités pourraient être entreprises relativement facilement. Pour citer Joe Nye: "Les domaines les plus prometteurs pour la coopération internationale ne sont pas les conflits bilatéraux, mais les problèmes posés par les tiers, comme les criminels et les terroristes"[42]. Avec le temps, les intérêts des pays avancés

---

42 Joseph S. Nye: "Nuclear Lessons for Cyber Security", dans *Strategic Studies Quarterly*, hiver 2011.

(et donc aussi les plus vulnérables) vont vraisemblablement converger, limitant les dégâts causés par les groupes criminels et terroristes, ce qui facilitera une meilleure coopération en matière de criminalistique et de contrôles. "Pour commencer, les Etats pourraient accepter d'être tenus pour responsables des attaques qui traversent leur territoire, et s'engager à coopérer en matière de criminalistique, d'information et de mesures correctives"[43].

En ce qui concerne les normes internationales, la voie à suivre consiste évidemment à accepter comme point de départ les instruments juridiques existants, aussi bien pour le *jus ad bellum* ou *droit à la guerre* (droit relatif au recours à la force) que le *jus in bello* ou *droit dans la guerre* (droit réglementant la conduite des conflits armés) et à étendre leur application au cyberespace. On pourrait ensuite progresser et évaluer une par une les dispositions de ces instruments qui appellent une interprétation commune et celles qui appellent un complément.

Ces deux dernières années, deux grandes tentatives ont eu lieu à l'échelle internationale pour promouvoir une interprétation commune des cyberattaques. Tant le Manuel de Tallin, établi par un groupe de juristes internationaux indépendants, sous l'égide du Centre d'excellence de l'OTAN pour la cyberdéfense en coopération (CDC) que les recommandations élaborées par le Groupe d'experts gouvernementaux des Nations Unies dans le domaine de la télématique affirment que le droit international existant s'applique bel et bien au cyberespace. Par conséquent, la question n'est pas de savoir si les lois existantes s'appliquent, mais comment elles s'appliquent. Certes, les conclusions de ces deux instances n'ont pas valeur obligatoire et n'ont pas été avalisées par les Etats – tout au moins pas encore. Cependant, on peut à juste titre qualifier d'historique l'accord auquel sont parvenus les experts.

Le Manuel de Tallinn[44] est une étude poussée et ambitieuse, rédigée à l'invitation du Centre d'excellence de coopération pour la cyberdéfense de l'OTAN, basé à Tallinn, dans laquelle l'applicabilité des normes juridiques à la cyberguerre est minutieusement examinée. Ce document ne reflète que les vues des experts indépendants qui ont pris part aux travaux du Groupe. Il peut être considéré comme une tentative visant à amorcer la réflexion sur une série de problèmes importants et extrêmement délicats. Autrement dit, il constitue une invitation à participer à cette réflexion et marque le début, et non la fin, des efforts déployés pour arriver à une interprétation commune.

Qu'est-ce que le "recours à la force" ou une "agression armée" dans le cyberespace?

Nous savons assez bien à quoi ressemble un acte de guerre, mais comment définir, juridiquement parlant, le "recours à la force" ou l'"agression armée" dans le cyberespace? Un acte non cinétique – comme une cyberattaque – peut-il être qualifié

---

43 Eneken Tikk: "Ten Rules of Security", *Survival*, juin-juillet 2011.

44 "Manuel de Tallin sur l'applicabilité du droit international à la cyberguerre".

d'"agression armée" ou ne mérite-t-il cette appellation que s'il s'inscrit dans le cadre d'une opération de grande envergure? Quel type de riposte à une telle attaque peut être considéré comme légitime? Cette riposte inclut-elle le droit de recourir à la force militaire?

Il n'existe pas de définition communément acceptée du terme "cyberguerre", qui est généralement employé pour décrire des hostilités dans le cyberespace "[…] ayant des répercussions équivalentes à une violence physique majeure ou amplifiant cette violence"[45]. Ce n'est donc pas le simple déploiement de cybermoyens offensifs, mais plutôt les conséquences de leur utilisation qui peuvent nous aider à déterminer si on affaire à une cyberguerre. A ce jour, nul n'a vu de cyberguerre *stricto sensu*. On a observé des attaques massives par déni de service visant un pays ou ses infrastructures essentielles dans le cadre d'un vaste offensive cinétique, ou encore des attaques ciblées visant des systèmes de contrôle dans l'industrie. "Mais dans la mesure où l'on n'a pas eu à affronter de répercussions non-intentionnelles et d'effets en cascade, on peut dire que l'on n'a pas fait l'expérience de ce que serait toute la gamme des attaques et des ripostes dans le cadre d'une cyberguerre entre Etats"[46].

La Charte des Nations Unies ne prévoit que deux exceptions à l'interdiction générale du recours à la force: premièrement, au Chapitre VII, lorsque le Conseil de sécurité constate l'existence d'une menace contre la paix et est autorisé à prendre les mesures qu'il juge nécessaires pour rétablir cette paix; et deuxièmement, à l'Article 51, lorsqu'un pays exerce son droit de légitime défense, individuelle ou collective, ce qui revient à reconnaître son droit inhérent de recourir à la force contre l'agresseur.

Il faut à ce stade émettre quelques observations. Il est souvent difficile de parvenir à un accord au sein du Conseil de sécurité des Nations Unies relativement à l'autorisation du recours à la force. En effet, il faut compter avec l'unanimité des "grandes puissances" ou, en d'autres termes, le droit de veto des membres permanents du Conseil de sécurité. Il est parfois difficile de parvenir à l'unanimité, surtout dans les cas où un ou plusieurs membres permanents du Conseil sont parties au conflit en question. Outre le fait que cela nuit au caractère démocratique du processus, le risque est aussi que les pays choisissent de de faire passer pour agression armée un cas de recours à la force – ce qui, à son tour, justifie le recours à la force contre l'agresseur. Autre élément qui plaide en faveur d'une application élargie de l'Article 51: le droit des Etats à l'auto-défense en cas d'attaque terroriste, de plus en plus invoqué.

Que se passe-t-il lorsque l'attaquant n'est pas un Etat, mais une entité non étatique, ou semble en être une? Les rédacteurs de la Charte des Nations Unies ont laissé le concept d'agression armée délibérément ouvert à l'interprétation des organes et des Etats

---

45 Joseph S. Nye, ibid.

46 Ibid.

Membres de l'ONU. En outre, le libellé de l'Article 51 est suffisamment vague pour autoriser les Etats Membres faisant l'objet d'une agression à exercer leur droit de légitime défense, même si cette agression est commise par une entité non étatique. La réponse aux attaques du 11 septembre est à cet égard un exemple significatif, tant sous l'angle de la prise de décision par le Conseil de sécurité des Nations Unies que sous celui des décisions opérationnelles de l'OTAN.

La question est de savoir si des opérations non cinétiques dans le cyberespace constituent un "recours à la force", voire une "agression armée" ou si, selon la logique des rédacteurs de la Charte des Nations Unies, ces définitions ne s'appliquent qu'au recours à la force militaire. On s'est efforcé à maintes reprises ces dernières années d'établir si la coercition politique et économique équivalait au recours à la force. La plupart de ces tentatives ont échoué, par crainte d'ouvrir une véritable boîte de Pandore. Mais est-il vraiment justifié de ne prendre en compte que les instruments utilisés ou ne devait-on pas plutôt accorder plus de poids et d'attention aux conséquences?

Les gouvernements se soucient sans doute moins des instruments précis utilisés dans tel ou tel cas que des conséquences de leur application. Il suffit de se rappeler des attaques du 11 septembre, lorsque des avions civils ont été utilisés pour causer délibérément un maximum de dégâts et faire des victimes. La règle empirique pourrait être la suivante: si une cyberattaque entraîne des dégâts considérables comparables à ceux causés par une attaque cinétique, elle devrait être considérée comme constituant un recours à la force, voire une agression armée, au même titre qu'une offensive militaire. A cet égard, il importe peu que cette attaque soit aérienne, terrestre ou maritime, ou se produise dans le cyberespace; c'est son impact qui détermine la façon dont elle sera perçue et donne au pays attaqué le droit de se défendre en retour. Le cas de la Syrie illustre un autre exemple. Le rejet de substances chimiques mortelles est généralement considéré comme un acte non cinétique. Mais l'emploi de ces substances en Syrie contre les populations locales, qui a fait un très grand nombre de morts et de blessés, pourrait sans doute être qualifié de recours à la force.

L'offensive subie par la compagnie pétrolière Saudi Aramco en 2012 présente un problème plus complexe. Il est indéniable que la disparition pure et simple de toutes les données stockées sur les plus de 30 000 ordinateurs de la compagnie lui a été extrêmement préjudiciable, y compris financièrement, mais de nombreux experts préfèrent ne pas parler à ce propos d'agression armée, avec toutes les conséquences qui s'ensuivent.

Donc, comment peut-on définir si un événement a franchi le seuil qui autorise le "recours à la force", pouvant aussi équivaloir à une "agression armée"? Comment évaluer les dégâts, la douleur et la peur causés avant de conclure à la nécessité d'une riposte?

Malheureusement, il n'existe pas de réponse tranchée à cette question. Il n'en est pas moins vrai, comme on l'a vu plus haut, que si les répercussions d'une attaque sont aussi graves que celles d'une attaque conventionnelle, elle peut être considérée comme constituant un recours à la force[47]. Il existe une nette corrélation entre la gravité des dégâts et le nombre de victimes de l'attaque. Les événements qui causent un grand nombre de victimes relèvent certainement de cette catégorie, de même, probablement, que les attaques qui paralysent des secteurs clés de la vie d'un pays. Mais peut-on fixer un seuil? Evidemment, non. La décision d'appeler l'événement en question "recours à la force" ou "agression armée" est toujours ponctuelle et prend en compte divers facteurs. De ce point de vue, la décision concernant ce qui équivaut à un acte de guerre a un caractère plus politique que militaire ou juridique. Même dans le domaine du terrorisme, après l'horreur du 11 septembre, on ne pouvait être plus précis. Pourrait-on, par exemple, conclure que si une attaque terroriste prend pour cible des civils innocents et fait plus de 3 000 victimes, il s'agit incontestablement d'une agression armée? Voulons-nous en déduire que tel n'est pas le cas si le nombre de victimes est inférieur à 3 000? Est-ce là le type de message que nous voulons transmettre aux criminels en puissance? Je ne le pense pas.

Les opérations dans le cyberespace peuvent être classées selon plusieurs critères. Un modèle couramment accepté est celui de la CIA, qui repose sur trois éléments (confidentialité, intégrité et disponibilité) et qui a été élaboré pour identifier les problèmes et solutions en matière de technologies de l'information[48]. Les attaques ciblant l'intégrité, conçues spécifiquement pour saboter le fonctionnement ordinaire des systèmes de contrôle (par exemple, le virus Stuxnet) ou ciblant la disponibilité (paralysie des systèmes de contrôle du trafic aérien ou des réseaux militaires, comme en Géorgie) peuvent faire des victimes et leur impact peut être comparable à celui d'une attaque cinétique. Elles peuvent donc facilement être qualifiées de recours à la force. En revanche, les attaques ciblant la confidentialité (cyberespionnage) peuvent se traduire par des pertes très importantes (pour les seuls Etats-Unis, le vol de propriété intellectuelle coûterait, selon les estimations, quelque 250 milliards USD par an), mais elles relèvent d'une autre catégorie et la parade est principalement diplomatique.

L'espionnage, ou deuxième plus vieux métier du monde, est pratiqué à grande échelle – quelquefois même entre alliés très proches. "Globalement, chaque Etat doit concilier des objectifs quelquefois irréconciliables, à savoir accorder la plus grande liberté d'action possible et réduire au minimum les risques d'actes malveillants. La surveillance des comportements malveillants a pour objectif général de réduire au minimum les

---

47 Voir les "critères de Schmitt", ensemble de règles qui aident un Etat à déterminer si une cyberattaque est ou non un acte de guerre.

48 Voir Darril Gibson "Understanding the Security Triad", *Pearson*, 27 mai 2011.

dégâts, c'est-à-dire de repérer les menaces suffisamment tôt pour qu'il n'y ait pas de perturbation"[49]. A une époque où la prévention et la détection anticipée des intentions délictueuses et des activités malveillantes sont de plus en plus importantes et où on s'efforce de prévenir les incidents plutôt que de remédier à leurs conséquences, le renseignement devient un facteur-clé. Il ne serait donc pas réaliste, sur le plan des relations internationales, de prohiber les activités de renseignement dans le cyberespace. Il est toutefois "[…] envisageable d'imaginer un échange de procédés qui permette d'élaborer un 'code de la route' susceptible de limiter les dégâts dans la pratique" [50].

L'utilité d'abaisser le seuil du recours à la force afin de contenir l'expansion de l'espionnage est très présente à l'esprit de plusieurs pays, en particulier des pays les moins avancés. Le tableau est plus nuancé en ce qui concerne les pays développés, qui sont souvent les premières victimes de cet espionnage. En même temps, ils sont souvent aussi ceux qui ont le plus intérêt à conserver une grande marge de manoeuvre, et ne sont donc généralement pas favorables à l'abaissement de ce seuil. Ces pays, qui veulent avoir plus de liberté d'action pour prendre des mesures de rétorsion et ont les moyens de le faire sont aussi les plus déterminés à réduire l'écart entre les seuils de déclenchement du "recours à la force" et de "l'agression armée".

Riposter à une cyberattaque

Si un pays est victime d'une grave cyberattaque, dans l'immédiat, son principal objectif est de mettre un terme à cette attaque et de la repousser, ainsi que de rétablir aussi vite que possible le fonctionnement des systèmes endommagés. La protection de la population et le rétablissement des réseaux numériques essentiels sont prioritaires. Dans la plupart des cas, on s'efforce d'assurer une nouvelle escalade du conflit, sauf si le recours à la force est considéré comme nécessaire pour empêcher et prévenir de nouvelles attaques.

Une grave cyberattaque à l'aide, par exemple, de logiciels malveillants qui paralysent le contrôle du trafic aérien, ce qui peut entraîner des accidents d'avion et causer de nombreuses victimes, serait probablement considérée comme une agression armée nécessitant une riposte adaptée. Mais même dans ce cas, conformément au droit humanitaire international, la riposte doit respecter certains critères. Elle doit être proportionnée, justifiée et nécessaire et doit se conformer aux principes de distinction et de précaution. Pour ce qui est du contenu, cette riposte peut revêtir différentes formes. Elle peut être militaire, en ligne, ou peut consister à dénoncer publiquement l'attaquant devant les Nations Unies. On peut riposter par voie diplomatique ou imposer des sanctions. Il se peut aussi qu'il n'y ait aucune riposte.

---

[49] Entretien avec Kah-Kin Ho, Chef de la cybersécurité, CISCO.

[50] Joseph S. Nye, ibid.

Les exercices calqués sur des situations de la vie réelle le démontrent clairement: les cyberattaques massives et concentrées, lancées par des adversaires capables et ingénieux, déterminés à infliger des dégâts importants, ne peuvent être stoppées par les seuls cybermoyens, et ce, encore moins si elles s'inscrivent dans le cadre d'une vaste offensive. Les cybermesures défensives peuvent contribuer à la remise en état des réseaux endommagés et aider à détecter les attaques, mais ne peuvent faire disparaître les menaces. Pour ce faire, un pays doit avoir en réserve d'autres moyens.

Agir par anticipation

Une autre dimension intéressante du problème est liée aux spécificités du cyberespace, à savoir le fait que les facteurs temps et espace n'y ont guère d'importance: les délais d'avertissement sont inexistants ou très brefs. Le temps qui s'écoule entre le moment où un ordinateur détecte qu'il va être attaqué par un logiciel malveillant et celui où des mesures sont prises pour repousser cette attaque peut n'être que de quelques millisecondes. Pour assurer une défense efficace, il faut donc avoir mis en place des ripostes automatiques, ce qui en soi pose plusieurs problèmes. Vu la vitesse de l'attaque, la question est de savoir si un Etat doit attendre que se produise une cyberattaque massive – analogue à une agression armée (acte ponctuel ciblant ses infrastructures essentielles ou faisant partie intégrante d'une opération cinétique visant à détruire ses centres vitaux de commande et de contrôle) ou s'il peut être autorisé à y riposter par anticipation. Si tel est le cas, à quel moment les gouvernements peuvent-ils intervenir pour empêcher des cyberattaques destructrices – quelles sont les conditions d'une auto-défense par anticipation?

Nombre d'experts juridiques semblent avoir convenu d'une norme appelée "dernière occasion d'agir possible", conformément à laquelle l'inaction à un moment donné risquerait de nuire gravement à l'efficacité de la défense. Le Manuel de Tallinn parvient à la conclusion qu'un Etat peut agir en auto-défense "[…] lorsque l'attaquant est clairement déterminé à lancer une agression armée et que l'Etat qui en est la victime perdra l'occasion de se défendre efficacement, sauf s'il agit"[51].

Le recours aux cybermoyens est parfois considéré comme préférable à une solution qui serait pire. Les pays évolués et puissants peuvent être tentés d'intensifier leur utilisation stratégique des cyberarmes pour convaincre leurs adversaires de changer de comportement ou de mettre fin à des activités dangereuses. Cette mesure peut être souhaitable si elle sert à empêcher une guerre. Par contre, elle pourrait rendre d'autres pays vulnérables en les plaçant à la merci d'entités plus évoluées. La crainte de déboucher sur une course aux cyberarmements généralisée, avec des nations qui se livrent concurrence ou ont recours à des mercenaires du cyberespace n'est pas

---

[51] Manuel de Tallinn sur l'applicabilité du droit international à la cyberguerre.

totalement infondée. Autre motif d'inquiétude: le code utilisé par des cyberattaques sophistiquées est souvent accessible sur l'Internet à des entités non étatiques.

Quel est le niveau de preuve requis pour imputer une cyberattaque?

Le fait d'imputer une cyberattaque à un auteur avec une certitude suffisante est souvent cité comme étant un problème majeur, qui rend d'ailleurs presque impossible de qualifier d' "agression armée" une opération menée dans le cyberespace. Il serait erroné de négliger ce problème, bien réel, mais il ne faut pas non plus en surestimer l'importance. Le renforcement de la coopération internationale et des relations entre les milieux du renseignement et ceux des cybertechniques et, surtout, l'évolution technologique peuvent contribuer à améliorer cette situation.

Si le but recherché est que soient fournies des preuves claires et convaincantes, pouvant soutenir un examen en justice, d'un lien entre une attaque et son auteur, l'imputation pose effectivement un problème presque insurmontable. Mais cette notion est relative. Il faut accepter que, dans l'éventualité d'une cyberattaque, il soit pratiquement impossible d'établir une preuve incontestable. Il est rare de pouvoir parvenir à une certitude complète et absolue même des semaines après l'attaque, dans le meilleur des cas. Il faut plutôt s'attendre à accumuler des preuves en provenance de diverses sources (milieux du renseignement, techniciens, etc.) et constituant des "preuves indirectes". L'imputation est aussi une notion relative en termes de Realpolitik. Les préoccupations associées aux difficultés que posent l'imputation d'une attaque à un auteur sont proportionnelles au nombre de victimes. Autrement dit, plus le nombre de morts est élevé, plus les pressions exercées sur les Etats pour qu'ils ripostent énergiquement à l'attaque sont fortes.

Il faut aussi souligner que l'imputation ne suffit pas à qualifier un acte d'agression armée. Nous rappellerons à cet égard la réaction de l'OTAN aux événements du 9 septembre 2011, lorsque dans un délai de 24 heures, l'Alliance a, pour la première fois de son histoire, invoqué le mécanisme de défense collective de l'Article 5. Dans sa formulation, l'OTAN n'a pas fait référence à la possibilité d'attribuer l'acte terroriste à un Etat, mais s'est simplement demandé si l'attaque visant les Etats-Unis était dirigée depuis l'étranger – condition visant à s'assurer que la clause relative au mécanisme de défense collective n'était pas utilisée à l'encontre des ressortissants de pays membres. On conclut souvent que la dissuasion ne fonctionne pas dans le cyberespace à cause des difficultés posées par l'imputation. Cela est vrai en partie – mais pas dans le sens traditionnel lorsqu'il suffit d'afficher sa force pour dissuader un agresseur potentiel. Toutefois, la dissuasion fonctionne dans les situations où elle permet de nier les avantages d'une attaque plutôt que d'essayer de la faire payer par le biais de représailles – tout comme la défense antimissile balistique rend l'attaque inefficace ou trop

coûteuse. "Si les pare-feux sont solides, ou si la perspective d'une réaction auto-exécutoire semble possible, les attaques perdent de leur intérêt"[52].

Acteurs autres qu'étatiques

Dans le cybermonde, la plupart des évaluations du renseignement convergent pour affirmer que seul un petit nombre d'Etats nations ont actuellement la capacité de mener à bien des attaques complexes et soutenues pouvant causer de graves dégâts. Dans le même temps, comme l'a dit W.J. Lynn, Secrétaire adjoint de la Défense, […] "les Etats ont, certes, les plus importantes capacités, mais il est vraisemblable qu'une attaque ayant des conséquences catastrophiques sera lancée par des acteurs autres qu'étatiques"[53].

A ce stade, je souhaiterais faire une pause et établir une nette distinction entre l'espionnage, d'une part, et les perturbations et destructions dévastatrices, d'autre part, même si, techniquement, les deux sont très proches. Bien sûr, tout doit être fait pour rendre plus difficile l'espionnage et le vol de renseignements précieux sur l'Etat et l'industrie, mais la priorité absolue consiste à éliminer le risque d'attaques ayant des conséquences extrêmement dévastatrices.

La bonne nouvelle est que, dans le domaine du dispositif nucléaire, les Etats nations capables pensent essentiellement en termes rationnels et s'efforceront probablement de ne pas franchir les lignes rouges pour ne pas provoquer de réactions violentes. Pour que les pays comprennent cette situation, ils doivent d'abord savoir qu'une ligne rouge existe réellement. Le message doit donc être transmis haut et fort: une attaque dévastatrice pourrait déclencher des mesures de rétorsion nationales ou collectives susceptibles d'utiliser n'importe quel outil à disposition[54]. Ensuite, il est possible de mettre progressivement en place des mesures de confiance, de désescalade, et certaines règles de base, comme indiquées plus haut – là encore, en tirant parti de l'expérience acquise dans le domaine nucléaire.

Il est plus difficile d'attendre un comportement rationnel de la part de certains "Etats voyous" qui ont pour ambition de mettre en place des cybercapacités offensives, qu'ils acquièrent au prix de lourds investissements. Ces Etats sont difficiles à dissuader et – comme nous le rappellent certains analystes des régions où la situation est explosive – pour certains pays et certaines cultures, un scénario où tout le monde est perdant peut être une option tout à fait acceptable.

---

52 Joseph S. Nye, Ibid.

53 W.J. Lynn, Secrétaire adjoint de la Défense, Remarques prononcées lors du 28ème Atelier international annuel sur la sécurité mondiale, Paris, 16 juin 2011.

54 Discours de Gabor Iklody devant le Global Intelligence Forum de l'AFCEA, Bruxelles, les 10 et 11 décembre 2013.

Toutefois, le plus inquiétant concerne le potentiel des acteurs autres qu'étatiques. Le cauchemar absolu serait que la capacité de nuire s'allie à l'intention de nuire, à tout prix. Nous n'en sommes pas encore là, mais la crainte que des terroristes n'utilisent des cyberarmes ne relève pas du domaine de l'impossible. On trouve sur l'Internet des kits "prêts à l'emploi" qui peuvent être améliorés, il existe des marchés noirs du "jour zéro" et des cybermercenaires, des pirates très capables qui louent leurs services pour voler des sommes d'argent ou des secrets industriels ou encore, en utilisant pratiquement les mêmes outils et techniques, pour causer des perturbations massives.

1.4 La cybersécurité vue par les Nations Unies

Par Hamadoun I. Touré

Le présent chapitre explique comment les Nations Unies envisagent la cybersécurité. Les TIC jouent aujourd'hui un rôle central dans le développement et la sécurité de ces systèmes, d'une importance décisive. Les économies des pays développés sont très fortement tributaires des TIC, y compris pour leurs infrastructures essentielles, et la cybersécurité devient en conséquence une priorité absolue, ce dont de nombreux pays sont tout à fait conscients. Les pays en développement ont une occasion exceptionnelle de créer une infrastructure de l'information sécurisée et ainsi, de progresser à pas de géant dans leur développement.

Cependant, la cybersécurité est loin d'être une priorité pour tous les pays, et souvent, les stratégies nationales en matière de TIC et de développement ne la mentionnent même pas. En intégrant la cybersécurité dans les programmes de développement et en la considérant comme "un moyen au service d'une fin" plutôt que comme une fin en soi, les Nations Unies s'emploient à changer la donne. Le présent article est axé sur les besoins actuels dans le monde en matière de cybersécurité, sur la façon dont les Nations Unies envisagent son développement et sur les mécanismes existants, et décrit succinctement les initiatives, en cours ou en projet, dans le domaine de la cybersécurité.

La cybersécurité: un impératif dans le monde entier

Les TIC ont un "pouvoir de transformation"[55] qui s'est étendu à chaque branche d'activité, ou presque, dans les pays développés, et a entraîné des transformations rapides dans les pays en développement. Toutefois, l'omniprésence des réseaux informatiques a un coût, à savoir la vulnérabilité croissante de secteurs économiques entiers aux cyberattaques. Ces menaces revêtent diverses formes (petits délits, vols de

---

55 Discours du Secrétaire général de l'UIT Hamadoun I. Touré – Sommet Transformer l'Afrique, Union internationale des télécommunications, 28 octobre 2013. Web. 24 juillet 2014.

numéro de carte de crédit, ou attaques concertées d'envergure mondiale, comme celle du ver informatique Conficker). Les délinquants oeuvrent souvent dans l'anonymat[56], ce qui rend encore plus difficiles d'éventuelles poursuites. En outre, les services traditionnellement chargés de la répression ne disposent que de ressources limitées dans le domaine de la cybersécurité, et les attaques sont souvent lancées depuis d'autres pays. Ces facteurs se combinent pour aboutir à une situation complexe qui pose des problèmes techniques et stratégiques à tous les pays: il est impératif de protéger l'intégrité, la confidentialité et l'existence même des informations critiques et des données personnelles.

Plusieurs pays développés font de la cybersécurité une priorité nationale[57]. Face à un réseau conçu au départ dans un esprit d'ouverture, et non sécuritaire, les pays dépensent des sommes très importantes pour sécuriser leurs réseaux (selon les estimations, plus de 70 milliards USD en 2014)[58]. Or, ces dépenses sont massivement le fait des pays à revenu élevé; en outre, elles semblent d'autant plus insuffisantes que les attaques ciblent en permanence de nouveaux secteurs[59].

Motivées par des raisons aussi diverses que l'appât du gain ou l'activisme politique, les cybermenaces peuvent émaner de pratiquement tous les pays et concernent de vastes secteurs économiques. Aucune entité – ni aucun Etat – ne peut à elle seule y parer efficacement. Il est donc d'autant plus urgent de déployer, dans le monde entier, des efforts concertés pour assurer la cybersécurité.

Toutefois, ce terme va bien au-delà des simples "cyberarmes" ou "cyberattaques". Une stratégie globale consisterait à protéger à la fois le droit à l'information et le droit au respect de la vie privée dans le cyberespace – deux droits humains fondamentaux consacrés par des traités internationaux. La sécurisation de cet espace doperait donc le développement économique et renforcerait la confiance, permettant ainsi de créer un environnement qui protège les particuliers de toute intrusion dans les données les concernant. C'est pourquoi la communauté internationale doit accélérer ses efforts visant à faire de la cybersécurité une priorité absolue, dans le monde entier.

---

56 Nazil Choucri, Stuart Madenick et Jeremy Ferwerda, Information Technology for Development (2013): "Institutions for Cyber Security: International Responses and Global Imperatives, Information Technology for Development," DOI: 10.1080/02681102.2013.836699.

57 "Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy". *Organisation de coopération et de développement économiques,* 2012.

58 Defending the Digital Frontier." *The Economist*, 12 juillet 2014.

59 "Hackers Inc." *The Economist*, 12 juillet 2014.

Pour les Nations Unies, la cybersécurité repose sur quatre grands piliers: (1) protection des réseaux de chaque organisation; (2) fourniture d'une assistance (coordonnée) aux Etats Membres[60] pour l'élaboration et la mise en oeuvre de politiques nationales en matière de cybersécurité; (3) intégration de la cybersécurité dans les programmes de développement; et (4) appui à la coopération internationale pour les questions relatives à la cybersécurité, à la cybercriminalité et à la protection des droits humains en ligne – en particulier concernant le respect de la vie privée et l'accès à l'information. Le présent article est axé sur les trois derniers de ces piliers, les plus pertinents pour l'étude du thème "En quête de la cyberconfiance". Nous les examinerons un par un.

Pour les Nations Unies, ces trois priorités sont fondées sur des principes communs. Premièrement, pour sécuriser efficacement les technologies de l'information, les Nations Unies préconisent une approche globale, "au niveau de l'ensemble des gouvernements" et multi-parties prenantes. Dans ses travaux internes, l'Organisation des Nations Unies devrait suivre cette doctrine et passer à une stratégie "inter-institutions" dans laquelle les entités concernées coordonnent leurs activités, gagnant ainsi en efficacité et évitant les doublons. Deuxièmement, compte tenu du caractère dynamique des technologies de l'information, les Nations Unies recommandent d'adopter des politiques souples et qui seront fréquemment réexaminées et, autant que possible, technologiquement neutres. Enfin, l'élaboration des politiques doit accorder une attention prioritaire aux incidences des mesures sécuritaires sur d'autres priorités définies à l'échelle mondiale, comme la protection de la vie privée.

Assistance aux Etats Membres

Les institutions des Nations Unies aident depuis longtemps les Etats Membres à élaborer des politiques dans le domaine des TIC. Toutefois, la cybersécurité n'est considérée comme prioritaire que depuis peu. Avec l'élaboration d'un Cadre à l'échelle du système des Nations Unies sur la cybersécurité et la cybercriminalité, approuvé en 2013, le Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination[61] est parvenu à un accord sur certains principes communs devant être suivis en vue de prêter assistance aux Etats Membres. Ce Cadre, qui représente une première étape sur la voie de l'harmonisation des efforts déployés en interne par les Nations Unies en matière de cybersécurité, sera examiné en détail plus loin[62].

Intégration de la cybersécurité dans les programmes de développement

Le développement des TIC (dont fait partie la cybersécurité) est généralement considéré comme une priorité distincte des autres domaines traditionnels du développement, qui

---

60 Dans le cadre du mandat de chaque institution et dans le respect de la souveraineté nationale.

61 Voir le § 85 du Rapport de la deuxième session ordinaire du CCS pour 2013 (novembre 2013).

62 Voir le chapitre "Mécanismes des Nations Unies pour la cybersécurité".

sont vus comme appelant davantage l'attention et de manière plus urgente. Or, il n'y a pas de contradiction entre le développement des TIC et la thématique globale du développement durable: le développement technique n'est pas tant une fin en soi qu'un moyen qui permet aux pays, en particulier aux pays en développement et aux pays les moins avancés (PMA) de renforcer leurs capacités dans divers secteurs économiques, tout en améliorant les conditions de vie générales. Les exemples ne manquent pas de cas où la technologie a permis d'améliorer l'accès à une eau salubre, à l'éducation et à des soins de santé abordables, en plus de doper la croissance économique et de stimuler/faciliter le commerce international.

Il est donc impératif d'inscrire la cybersécurité dans les priorités de développement *existantes:* plus les systèmes sont sécurisés et fiables, plus les chances d'adoption sont grandes. A ce propos, les pays en développement et les PMA bénéficient de circonstances exceptionnellement favorables: en s'efforçant de développer des réseaux informatiques intrinsèquement sécurisés, ils peuvent brûler les étapes et faire l'économie de systèmes qui font d'ores et déjà l'objet d'attaques. Les investissements dans le domaine de la cybersécurité peuvent contribuer à réduire encore la "fracture numérique". Les organisations du système onusien peuvent jouer un rôle essentiel à cet égard en tirant parti des mécanismes internationaux existants pour intégrer les programmes de cybersécurité.

Autre priorité à l'échelle mondiale: il est impératif d'empêcher l'apparition et l'escalade des cyberconflits. Même si, à ce jour, les pays ont fait preuve de retenue dans leur réaction aux cyberattaques[63], il n'est pas certain qu'il en ira de même à moyen et à long terme. Les activités de recherche et d'éducation de l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) ont pour objet de contribuer à prévenir l'escalade des conflits, l'UNIDIR "[…] servant de passerelle – à la fois en vue de créer les synergies nécessaires pour atténuer et lutter contre les effets de l'insécurité aux niveaux international, régional et local".

Encourager la coopération internationale en matière de cybersécurité

Bien que les activités en ligne soient soumises à diverses réglementations d'un pays à l'autre, l'Internet en soi reste pour l'essentiel un réseau mondial. Cela est particulièrement vrai en ce qui concerne la cybersécurité, domaine où les attaques et menaces transcendent quotidiennement les frontières nationales. Tel fut le cas, par exemple, du ver informatique Conficker, qui a causé des dégâts dans plus de 180 pays[64]. Aucun pays ne peut à lui seul résoudre les problèmes de cybersécurité, et les Nations

63 Valeriano, B., & Maness, R. C. (2014). "The dynamics of cyber conflict between rival antagonists, 2001-11." *Journal of Peace Research*. doi:10.1177/0022343313518940.

64 "Conficker." ShadowServer. Shadowserver Foundation, n.d. Web. 4 novembre 2013.

Unies considèrent comme prioritaire, sur le plan mondial, d'encourager la coopération internationale dans ce domaine.

L'une des tâches prioritaires des Nations Unies, pour donner confiance dans le cyberespace, est de réfléchir à la protection des droits humains en ligne, en particulier au respect de la vie privée et au droit à l'information. Le respect de la vie privée fait l'objet de menaces telles que les fuites constantes de données et souffre de l'insuffisance des investissements affectés à la protection des données. Le droit à l'information, pour sa part, est tributaire de l'accès à des TIC sécurisées autorisant la liberté d'expression et le libre accès aux contenus publics. Les programmes de sécurité en matière de TIC doivent tenir compte de ces intérêts divergents, comme le montrent les politiques nationales de nombreux pays, principalement des pays développés[65]. Les principes DOAM, selon lesquels l'Internet doit être fondé sur les Droits humains, Ouvert, Accessible à tous et impliquant de Multiples acteurs, sont un bon point de départ à la poursuite des travaux dans ce domaine. L'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) – institution des Nations Unies qui dispose d'une vaste expérience en matière de protection des droits humains dans le monde entier – considère cette vision de la cybersécurité au sens large comme l'une des priorités du développement durable.

Compte tenu de la primauté des acteurs du secteur privé dans l'économie de l'Internet, et même dans la gestion du réseau proprement dit, les efforts déployés pour atteindre ce niveau de protection doivent être coordonnés avec des parties prenantes autres que les gouvernements, par exemple le secteur privé, les milieux techniques et la société civile. Le renforcement de la coopération joue un rôle particulièrement déterminant sur le plan des enquêtes judiciaires, dans le cadre desquelles une assistance mutuelle peut être utile à toutes les parties intéressées.

Lignes directrices fondamentales en matière de cybersécurité

Si l'émergence du cyberespace en tant qu'espace global des communications internationales s'accompagne des multiples avantages qu'apporte un monde interconnecté, elle fait aussi peser de graves menaces pour la sécurité et la stabilité des Etats Membres de l'Organisation des Nations Unies. La confidentialité des données, les systèmes informatiques, les infrastructures essentielles et les services en réseau sont tous vulnérables aux attaques sur Internet, lancées à intervalles réguliers depuis

---

65 Voir *supra, §* 2.

n'importe quel point du monde. En de telles circonstances[66], sécuriser le cyberespace nécessite d'adopter une stratégie:

- Globale (ou "au niveau de l'ensemble des gouvernements") puisque la prévention67 et la détection des cyberattaques, l'atténuation de leurs effets et les poursuites contre leurs auteurs font intervenir une multitude de gouvernements et d'entités du secteur privé.
- Qui inclut les parties prenantes du secteur des TIC, y compris les décideurs, les prestataires de services Internet et de télécommunication, les organisations techniques et les organisations non gouvernementales de protection des droits de l'homme (ou "société civile").
- Favorable à des politiques dynamiques pouvant s'adapter en souplesse à l'évolution constante des technologies et permettant de faire face à des menaces inédites, sans pour autant paralyser l'innovation.
- Respectueuse des droits humains, notamment du droit au respect de la vie privée et du droit d'accès à l'information.

Mécanismes des Nations Unies pour la cybersécurité

Il existe déjà divers cadres régissant la cybersécurité sur le plan mondial au niveau des Nations Unies, par exemple le Cadre ONU pour la cybersécurité et la cybercriminalité, la grande orientation C5 ("Etablir la confiance et la sécurité dans l'utilisation des TIC") du Sommet mondial sur la société de l'information (SMSI), et le Réseau information, communication et technologie (Réseau TIC). Chacun d'eux sera décrit dans les paragraphes suivants. Nous présentons également certains mécanismes de cybersécurité en cours d'élaboration dans le système des Nations Unies.

Cadre ONU pour la cybersécurité

Au titre des efforts déployés pour faire face aux cybermenaces, les Nations Unies ont créé, à l'échelle du système onusien, un cadre sur la cybersécurité et la cybercriminalité, qui propose à toutes les entités membres de l'ONU des lignes directrices destinées à répondre aux préoccupations des Etats Membres à ce sujet et à renforcer la coordination entre eux, en vue d'améliorer la confiance et la sécurité dans le cyberespace.

Les activités criminelles sur Internet ont une ampleur et une fréquence très variables. Le Cadre a pour but de tenter de parer à une grande partie de ces menaces en

---

66 La présente section ne constitue pas un recensement complet des lignes directrices des Nations Unies en matière de cybersécurité, mais se présente plutôt comme un résumé succinct des grandes tendances communes recensées dans les ouvrages consultés.

67 Y compris le renforcement des capacités au niveau de l'utilisateur.

établissant des principes de base qui devraient être suivis par toutes les entités des Nations Unies, dans le cadre de leurs mandats respectifs. Les travaux sont centrés sur la prévention de la criminalité et l'alerte avancée, le renforcement des capacités à l'échelle nationale, l'efficacité de la dissuasion et l'importance de la justice dans la lutte contre la cybercriminalité. Ce Cadre inclut des volets consacrés aux questions techniques et au renforcement des capacités pour ce qui est de l'assistance aux Etats Membres et utilise une stratégie globale pour sensibiliser l'opinion et faire mieux connaître les capacités de réaction face aux cybermenaces.

Telle que définie dans ce Cadre[68], la cybersécurité fait référence à l'ensemble des documents, pratiques, politiques et technologies utilisés pour "[…] garantir que les propriétés de sécurité" des organisations, des informations, des systèmes et des actifs "sont assurées et maintenues". Mais contre quoi la cybersécurité assure-t-elle une protection? En plus de renforcer la confiance dans la technologie de l'information, elle combat les activités criminelles en lien avec l'informatique, autrement dit la cybercriminalité[69]: ensemble de "[…]thèmes [qui] comprennent les violations de la confidentialité, de l'intégrité et de la présence de données informatiques" et d'infrastructures; et un ensemble "… d'agissements [malfaisants] en lien avec l'informatique", ainsi qu'en lien avec les données.

Principes en lien avec la cybersécurité et la cybercriminalité

Afin de mieux délimiter la portée de ce Cadre à l'échelle du système des Nations Unies, ce document est articulé autour de sept grands principes pouvant aisément trouver une traduction politique, comme suit:

1. Les entités des Nations Unies devraient aider les Etats Membres à faire face aux cyberincidents de manière globale, y compris en fournissant un appui technique au pouvoir judiciaire et en renforçant la coopération internationale.
2. Il faudrait prendre en compte les mandats de ces entités lors de l'examen des besoins des Etats Membres, et s'efforcer de coopérer avec d'autres organisations concernées du système des Nations Unies.
3. Tous les programmes des Nations Unies en matière de cybersécurité et de cybercriminalité devraient respecter les droits de l'homme et la primauté du droit.
4. Les programmes mis en place par les Nations Unies devraient, si possible, aider les Etats Membres à adopter une stratégie fondée sur les faits lors de l'évaluation des délits et des risques.

---

68 Le Cadre utilise la définition de l'Union internationale des télécommunications figurant dans la Recommandation UIT-T X.1205.

69 Comme définie dans le Cadre.

5. Il faudrait, autant que possible, inciter à adopter un modèle de riposte "au niveau de l'ensemble des gouvernements" impliquant toutes les principales parties prenantes sur le plan national, ainsi que des acteurs non étatiques, par exemple ONG, établissements universitaires et milieux techniques.
6. L'appui fourni aux Etats Membres devrait viser à renforcer les mécanismes formels et informels de coopération internationale en matière de cybersécurité et de cybercriminalité.
7. La coopération public-privé au sein des Etats Membres, ainsi que l'harmonisation et l'adoption de normes techniques et de lignes directrices en matière de politiques et de sécurité à l'échelle régionale et internationale, devraient être encouragées pour permettre de réagir efficacement aux cybermenaces

L'assistance aux Etats Membres est donc au coeur de ce Cadre: l'objectif est d'améliorer la cybersécurité et de renforcer la sécurité et la fiabilité de l'Internet. Des recommandations visant à mettre en application les principes mentionnés ci-dessus et à fournir une telle assistance sont présentées dans ce Cadre. Ces lignes directrices peuvent être subdivisées en trois catégories: mesures d'ordre juridique et de politique générale, assistance technique et mécanismes de mise en oeuvre.

Assistance technique

Dans un domaine de nature aussi technique que le cyberespace, le renforcement des capacités et la formation aux compétences fondamentales en matière de cybersécurité sont considérés comme capitales pour les Etats Membres. Dans le Cadre, il est recommandé de procéder, dans les pays, à des évaluations détaillées des capacités techniques – point de départ indispensable – et d'élaborer des politiques nationales de cybersécurité. Plus précisément, l'assistance technique fournie par les entités des Nations Unies pourrait comprendre les éléments suivants: publications techniques sur la cybercriminalité et son économie; mécanismes de partage d'informations (bonnes pratiques et autres formes de savoir pouvant être diffusé); formation aux techniques d'investigation numérique et autres techniques d'enquête sur la cybercriminalité, y compris formation des consommateurs à l'utilisation en toute sécurité des ordinateurs et des réseaux; coopération avec les fournisseurs privés de services Internet (ISP) et d'autres parties prenantes dans le domaine de la collecte et de l'analyse de données; méthodes d'intervention en cas d'incident informatique, par exemple création d'instances permanentes chargées de gérer ces incidents (telles que les équipes nationales d'intervention en cas d'incident informatique ou équipes CIRT) et "points de contact chargés de répondre aux demandes formulées depuis l'étranger".

Grande orientation C5 du SMSI

Comme indiqué dans les documents établis par le SMSI à sa phase de 2003[70] et réexaminés lors de la manifestation de haut niveau SMSI+10 en 2014, la grande orientation C5 du SMSI est axée sur l'établissement de la confiance et de la sécurité dans l'utilisation des TIC, dont la coordination a été confiée à l'UIT. En 2007, l'UIT a lancé le Programme mondial cybersécurité (GCA) "[…]conçu comme un cadre permettant de coordonner la réponse internationale aux enjeux croissants de la cybersécurité" en collaboration avec les Etats Membres et d'autres parties prenantes. A cet égard, l'UIT a conclu des partenariats avec des parties prenantes du monde entier pour faire progresser la cybersécurité, entre autres, en publiant des lignes directrices pour l'établissement de politiques nationales dans ce domaine[71], en fournissant une assistance technique aux Etats Membres pour les aider à renforcer leurs capacités, et en encourageant les débats sur les normes techniques nécessaires afin d'améliorer la sécurité.

Réseau TIC

L'un des mécanismes mis au point par le Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination est le réseau TIC. Ce réseau, qui regroupe les capacités TIC de nombreuses entités des Nations Unies pour ce qui est de la prise de décision, joue un rôle de coordination et de tribune pour l'élaboration et la mise en oeuvre des politiques relatives aux TIC. Aux fins de la présente publication, l'élément qui nous intéresse le plus est son Groupe d'intérêt pour la sécurité informatique, qui étudie les questions liées à la cybersécurité "[…] dans le cadre de présentations d'experts et d'études de cas [et l'examen de] domaines dans lesquels les institutions ont une action commune, par exemple les interventions en cas d'incident, la sécurité et les politiques de l'information et la sensibilisation à la sécurité de l'information"[72].

Travaux en cours

Ainsi que l'ont reconnu aussi bien les Etats Membres de l'Organisation des Nations Unies que le CCS[73], il est impératif de coordonner, dans le système des Nations Unies, les

---

70 Sommet mondial sur la société de l'information www.itu.int/wsis/index.html, dernière mise à jour le 13.10.2014.

71 ITU National Cybersecurity Strategy Guide (Guide UIT sur les stratégies nationales en matière de sécurité), septembre 2011.

72 Groupe d'intérêt pour la sécurité informatique. Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination, 21 novembre 2022. Web. 22 juillet 2014.

73 "Action on Cybersecurity/Cybercrime and Policies on Information". CCS des Nations Unies, 21 novembre 2011. Web. 22 juillet 2014.

travaux relatifs à la cybersécurité et à la cybercriminalité. Suite à l'approbation du Cadre ONU sur la cybersécurité et la cybercriminalité en 2013, le Secrétaire général de l'Organisation des Nations Unies Ban-Ki moon a appelé l'UIT – aux côtés de l'UNESCO, de l'UNODC, du PNUD et de la CNUCED, et en étroite coordination avec le Comité de haut niveau sur la gestion (HLCM), le Comité de haut niveau sur les programmes (HLCP) et le Groupe des Nations Unies pour le développement (GNUD) – à mettre au point, dans l'ensemble du système, une stratégie complète et cohérente qui permette de résoudre les questions, et qui fera l'objet des débats du CCS à sa deuxième session ordinaire en novembre 2014[74].

Conclusion

Tous les pays s'accordent sur la nécessité de réagir de manière globale et concertée aux problèmes de cybersécurité. Les Nations Unies traitent ces questions dans leur globalité, avec le concours de multiples parties prenantes, dans le respect des droits humains et suivant un modèle souple et dynamique. Même si aucun accord ne s'est dégagé jusqu'à maintenant sur une vision de la cybersécurité, on relève, dans le travail des entités des Nations Unies, certaines tendances et éléments communs qui mettent en lumière la priorité accordée depuis peu au thème de la cybersécurité. Il est désormais admis que la sécurisation du cyberespace est une nécessité universelle qui a des retombées manifestes sur le développement social et économique, alors même qu'il importe de concilier des intérêts divergents et de respecter la souveraineté nationale. Les perspectives de la cybersécurité semblent prometteuses, comme le reconnaissent Choucri et collaborateurs[75]: "Certes, le système actuel d'accords institutionnels [internationaux][sur la cybersécurité] donne des signes de faiblesse, mais il n'en est pas moins vrai que la concertation et la coopération ne cessent de progresser".

Cette tendance encourageante est un facteur supplémentaire qui incite tous les pays à coopérer en matière de cybersécurité. L'Internet étant, par nature, un réseau mondial, seuls les efforts de portée mondiale (ou quasi-mondiale) peuvent en effet aboutir à sécuriser le cyberespace. Les perturbations causées par des cyberattaques peuvent avoir des coûts très élevés, en particulier dans des secteurs critiques comme l'alimentation électrique ou la finance, mais ces coûts sont largement compensés par les avantages qu'il y a à investir dans la cybersécurité. C'est encore plus vrai pour les pays développés, dont les infrastructures sont fortement interconnectées. Les pays en développement, eux, ont là une occasion historique de brûler une étape de leur développement, et le fait d'accorder la priorité à la cybersécurité peut sans nul doute améliorer leurs perspectives.

---

74 Voir § 85 du rapport de la deuxième session ordinaire du CCS, novembre 2013.

75 Voir ci-dessus, § 2.

Ces changements ne deviendront toutefois réalité que lorsque la cybersécurité aura véritablement acquis le rang de priorité mondiale. Les Nations Unies, qui disposent de compétences spécialisées dans le développement, sont idéalement placées pour jouer le rôle de coordonnateur des activités de cybersécurité dans le monde; les Etats, le secteur privé et la société civile ont tout intérêt à y contribuer.

Chapitre II: Cyberrésilience

Introduction

En février 2005, le Comité consultatif sur les technologies de l'information placé sous l'égide du Président des Etats-Unis a lancé un appel à l'action[76] en faveur du renforcement de la sécurité dans le cyberespace[77] en publiant un rapport historique intitulé "Cyber Security: A Crisis of Prioritization". Sur un thème analogue, l'Académie nationale américaine d'ingénierie a publié en 2008 une liste des "14 grands défis qui nous attendent au XXIe siècle". Ces dernières années, de nombreuses autres entités se sont elles aussi intéressées à ce défi que constitue l'instauration de la cyberconfiance dans le monde numérique de demain.

Depuis, notre dépendance vis-à-vis de tout ce que nous offre l'ère numérique ne cesse d'augmenter de manière exponentielle, à mesure que les équipements et les systèmes informatiques et de communication sont de plus en plus omniprésents et essentiels dans presque tous les aspects de notre quotidien.

Par conséquent, il importe au plus haut point de veiller à ce que le cyberespace reste sûr d'instaurer la résilience pour faire face à la menace grandissante que sont les cyberattaques, qui peuvent avoir des effets dévastateurs et destructeurs à grande échelle.

En progression constante, l'utilisation des technologies de capteurs, des systèmes cyberphysiques, des services en nuage, des mégadonnées ou des systèmes auto-adaptatifs intelligents[78] élargira considérablement les fonctionnalités des TIC et aura

---

76 President's Information Technology Advisory Committee, "Cyber Security: A Crisis of Prioritization" (février 2005).

77 National Academy of Engineering: "Grand Challenges for Engineering"; www.engineeringchallenges.org/cms/challenges.aspx.

78 Markus Luckey Gregor Engels: "High-Quality Specification of Self-Adaptive Software Systems". Dans: Proceedings of the 8th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. ACM (New York, NY, USA), SEAMS'13, pp. 143-152; (2013).

une incidence sur notre quotidien, alors que l'avènement de l'Internet des objets est en route.

Cette tendance est entretenue non seulement par les nouveautés technologiques, mais aussi par la demande incessante de nouveaux marchés et de nouveaux produits. Le développement de la cyberinfrastructure et des cyberservices multipliera les possibilités et les retombées, mais il s'accompagnera également de nouvelles vulnérabilités et de nouvelles menaces risquant de mettre à mal la sûreté et la sécurité privées et publiques de nos sociétés.

Les enjeux sont considérables, en particulier car la confiance dans l'ère numérique et même notre bien-être en général dépendent pour beaucoup de notre capacité de recenser et de gérer un large éventail de cybermenaces. Après une analyse et une évaluation rigoureuse des vulnérabilités et des risques, il faudra définir des mesures adéquates pour garantir la cybersécurité – ou tout du moins une cyberrésilience suffisante – en particulier pour les infrastructures essentielles telles que les réseaux électriques, les réseaux d'approvisionnement en eau, les réseaux de transport, les systèmes de santé et les systèmes financiers[79].

La complexité croissante et l'utilisation accrue des infrastructures et des services TIC sont des sources de risques potentiels pour la cyberstabilité et la cybersécurité. Des événements extérieurs, tels que les catastrophes naturelles ou les attaques lancées par des gouvernements, des organisations criminelles ou des particuliers, représentent des menaces encore plus grandes. Les études montrent que les concepteurs des systèmes, les opérateurs et les utilisateurs peuvent eux-mêmes être une source importante de vulnérabilité pour les TIC, que ce soit ou non intentionnel. A cet égard, les problèmes scientifiques et techniques de base qu'il faut impérativement résoudre concernent les questions "complexité-urgence-résilience" dans le cyberespace.

Le présent chapitre explique tout d'abord la terminologie se rapportant à la complexité des TIC, les cyberrisques et les comportements systèmes inattendus qui en découlent, et pourquoi il est de plus en plus nécessaire d'élaborer des stratégies pour assurer la cyberrésilience. Il présente ensuite les nombreuses sources potentielles de cyberrisques – erreurs ou défaillances physiques, techniques ou environnementales ou encore causes organisationnelles, institutionnelles ou législatives – et traite de l'identification des cyberrisques, de leur analyse et des stratégies de résilience jusqu'au niveau de l'information d'un point de vue informatique et technique. On abordera ensuite les enjeux de la résilience en élargissant la réflexion aux applications des mégadonnées et de l'informatique en nuage, ainsi qu'à la nécessité de disposer de systèmes de cybercontrôle résilients. En dernier lieu, le présent chapitre contient des contributions

---

79 US Executive Order 13636: "Improving Critical Infrastructure Cybersecurity" (février 2013): www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

concernant la cyberrésilience du point de vue du secteur privé, traite d'un cyberrisque non technique majeur et expose une proposition de cadre juridique international requis de toute urgence pour lutter contre les risques existants autres que ceux liés à la simple protection des données.

La section 2.4 traite d'un cyberrisque non technique majeur et contient une proposition de cadre juridique international requis de toute urgence pour lutter contre les risques existants autres que ceux liés à la simple protection des données.

2.1 Cyberrésilience: Principes de base

Par Axel Lehmann

Terminologie

Comme nous l'avons déjà indiqué, la complexité croissante du monde numérique qui influence notre quotidien, dans la sphère publique comme privée, pose un véritable problème du point de vue de l'élaboration de mesures d'instauration de la confiance. En général, la **complexité d'un système (numérique)** dépend du nombre et des fonctionnalités de ses composants qui déterminent l'espace d'état du système.

Les supercalculateurs sont les équipements les plus puissants, et les plus performants d'entre eux devraient permettre de traiter quelque 1 000 PetaFLOPS – 100 millions de milliards d'opérations à virgule flottante par seconde – d'ici à 10 ans[80]. Les systèmes cyberphysiques (pour la plupart des micro-dispositifs de calcul invisibles et intégrés) n'offrent que des capacités de calcul très spécialisées et limitées.

Une connectivité plus large entre les différents systèmes permet de créer ce que l'on appelle des "systèmes de systèmes" (utilisés par exemple pour gérer les systèmes d'alimentation en énergie, de communication ou de régulation du trafic)[81]. Le stockage d'informations est un autre service global important, dont il faut tenir compte du point de vue de la cyberconfiance, puisque les technologies de stockage évoluent encore plus vite que les technologies informatiques (d'où une hausse constante des capacités de stockage associée à une diminution considérable des coûts).

Etant donné que le nombre de composants et de fonctionnalités d'un système, de même que le nombre de systèmes interconnectés au sein d'un "système de systèmes" redimensionnable augmentent, la complexité générale des systèmes qu'il faut maîtriser augmente elle aussi de manière exponentielle.

---

80 Calculateur exascale: voir: http://en.wikipedia.org/wiki/Exascale_computing.

81 Mo Jamshidi: "System-of-systems engineering: a definition"; dans: IEEE SMC; (2005).

Ces évolutions technologiques constantes exigent des méthodes de conception, de développement et de contrôle de la qualité solides pour garantir la stabilité du système, sa disponibilité – sans oublier des stratégies de résilience en cas de situation non souhaitée[82] – et la cyberconfiance. L'application la plus fréquente de méthodes bien définies pour la spécification et la conception des systèmes peut permettre de détecter et d'éviter certains états de système (vulnérables ou critiques), si des mesures d'identification et de prévention adaptées sont mises en oeuvre. Néanmoins, des événements ou des dangers qui ne pouvaient être anticipés au stade de la conception risquent d'entraîner, de la part du système, un comportement inattendu ou émergent qu'il sera peut-être difficile, voire impossible, de contrôler ou d'ajuster. Dans le pire des scénarios, le système pourrait s'effondrer sans qu'il soit possible de le ramener à un état opérationnel. Pour toutes ces raisons, il faut élaborer et appliquer des méthodes adaptées pour assurer la cyberrésilience.

Il faut recenser, analyser et évaluer ces menaces, vulnérabilités et risques et définir les contre-mesures correspondantes. La conception de systèmes numériques selon des méthodes éprouvées de conception et de tolérance aux pannes, rendra ces systèmes bien plus résistants et plus faciles à contrôler, mais n'empêchera cependant pas complètement les comportements émergents, en particulier dans le cas d'un système de systèmes. Par conséquent, il faut étudier et mettre en oeuvre des méthodes et des procédures d'ajustement pour accroître **la résilience des systèmes et des processus**, étape importante pour parvenir à établir la confiance dans ces systèmes et processus et dans le cyberespace en général.

Selon la définition qu'en donne Wreathall[83], "[…] la résilience est la capacité d'une organisation (d'un système) à conserver, ou retrouver rapidement, un état stable, lui permettant de continuer à fonctionner pendant et après un incident majeur ou malgré des pressions importantes continues**".** Lors du Forum économique mondial de 2012, l'initiative "Partenariat pour la cyberrésilience" a été créée et plusieurs "Principes et lignes directrices concernant les risques et les responsabilités dans un monde hyperconnecté" ont été formulés[84]. Vu l'immense diversité des acteurs qui composent ce monde numérique complexe (utilisateurs humains, concepteurs, opérateurs, dispositifs numériques et systèmes), et étant donné que les études montrent que les

---

82 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; publié par Ashgate Publishing Limited; (2006).

83 John Wreathall: "Properties of Resilient Organizations: An Intitial View"; In: Resilience Engineering – Concepts and Precepts, Ashgate Publishing Limited; (2006).

84 Forum économique mondial: "Partnering for Cyber Resilience"; Bulletin d'information de février 2013 – Davor Special Edition;www3.weforum.org/docs/WEF_RRHW_PartneringCyberResilience_NewsletteFebruary_2013.pdf; (2013).

plus vulnérables d'entre eux sont les humains, les mesures d'instauration de la confiance doivent tenir tout particulièrement compte de leurs activités.

Identification et classification des cyberrisques

Dans un monde où l'homme s'appuie considérablement sur les cyberressources, les analyses des risques et de la résilience dans le cyberespace doivent tenir compte d'un grand nombre de points de vue différents se rapportant aux acteurs humains ainsi qu'à la diversité et à la complexité du monde numérique. Les différentes ressources dans le cyberespace vont des infrastructures et des services numériques internationaux pouvant être utilisés partout dans le monde aux équipements de calcul ou cyberphysiques indépendants.

Par ailleurs, s'agissant de l'homme et de ses activités dans le cyberespace – par exemple, en tant que concepteur, développeur ou utilisateur – nous devons faire une distinction entre son rôle et ses capacités selon qu'il utilise les systèmes numériques depuis l'intérieur ou depuis l'extérieur de ces systèmes. En ce qui concerne la hiérarchie, et dans un souci de classification de l'identification, de l'analyse et de la prévention des cyberrisques, on peut distinguer les niveaux d'abstraction ou couches énumérés ci-après. Etant donné que les interruptions et les défaillances se produisant à des niveaux inférieurs peuvent avoir une incidence importante sur le comportement et le fonctionnement du système à des niveaux supérieurs, une analyse et une évaluation globales des risques doivent impérativement tenir compte de tous les facteurs suivants en vue de l'élaboration de stratégies de résilience des systèmes[85, 86]:

- niveau global;
- couche entreprise/niveau institutionnel/privé;
- niveau de l'information;
- niveau technique;
- niveau physique.

---

85 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; publié par Ashgate Publishing Limited; (2006).

86 Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; dans: K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg; (2012).

Analyse des cyberrisques et cyberrésilience d'un point de vue informatique et technique

Afin de procéder à une analyse rationnelle des cyberrisques et de définir des stratégies de cyberrésilience efficaces, il faut tout d'abord identifier les principales sources de cyberrisques à chacun des niveaux susmentionnés. La deuxième étape consiste à analyser et à évaluer de manière rigoureuse les éventuelles conséquences indirectes (dépendances), dans la mesure où une erreur, une panne, une défaillance ou une intrusion à un niveau inférieur risque d'avoir des incidences sur les fonctionnalités, la fiabilité ou la confidentialité et la sécurité à des niveaux supérieurs. Pour ce faire, on utilise des graphes de dépendance[87] pour repérer les dépendances mutuelles en suivant, dans un sens et dans l'autre, les trajets entre les niveaux, ce qui permet de détecter les causes de dysfonctionnement, de panne, de défaillance, de fuite ou de corruption des données.

Comme on le voit dans la Figure 1 ci-après, chaque niveau fournit certaines capacités, certaines fonctionnalités ou certains services (cx), qui comprennent ou utilisent des attributs des niveaux inférieurs, comme le montrent les flèches. Les flèches en pointillés indiquent que la mise en oeuvre de chaque capacité (cx) exige le respect de normes, de règlements ou de règles spécifiques. Dans la Figure 1, une défaillance est identifiée au niveau de l'entreprise, défaillance qui est peut-être due à une erreur, une panne ou une intrusion dans ce noeud ou dans un noeud à un niveau inférieur. En suivant la structure du graphe (en amont ou en aval), il est possible de localiser les origines potentielles d'une erreur, d'une panne ou d'une défaillance.

87 Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: "Basic Concepts and Taxonomy of Dependable and Secure Computing"; IEEE Transactions on Dependable and Secure Computing; (2004).

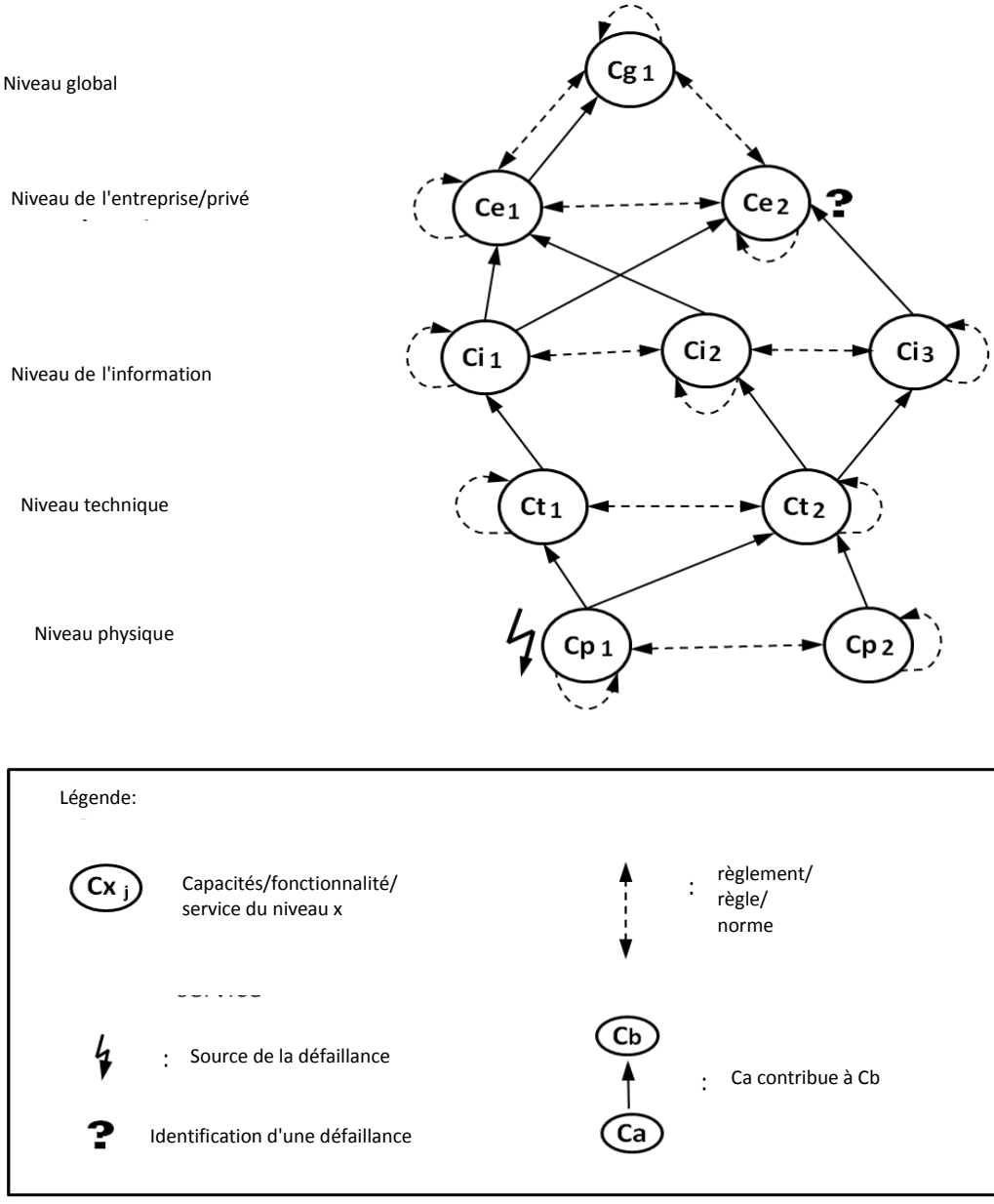

Figure 1: Exemple de graphe de dépendance

Comme nous l'avons déjà vu, l'évolution rapide des TIC permet d'importantes avancées techniques, mais elle est également synonyme de nouvelles sources et de nouvelles causes de cyberrisques, qui nuisent à la stabilité et à la sécurité dans le cyberespace. Outre les défauts physiques et techniques, la tendance à la virtualisation des ressources de calcul, de communication et de stockage sous l'effet d'une demande d'amélioration de qualité de fonctionnement, de la fiabilité et du rapport coût-efficacité pour la communauté des utilisateurs entraîne l'apparition de cyberrisques majeurs. Les technologies qui évoluent à un rythme soutenu, comme les mégadonnées, l'informatique en nuage et les ressources de logiciel en tant que service (SaaS) utilisant le nuage[88], les systèmes de systèmes [89] et les "hyperréseaux"[90], attestent de cette tendance.

Ces évolutions technologiques vont également de pair avec l'apparition de nouveaux problèmes de cybersécurité en rapport avec la vie privée, la confidentialité et l'authenticité. Outre l'utilisation abusive, la manipulation et la corruption des données et des infrastructures TIC, il existe de nouveaux risques concernant la collecte, l'utilisation et le regroupement non autorisés de données personnelles ou d'autres données confidentielles. Le risque, déjà avéré dans certains cas, est que différents types de données protégées appartenant à des individus, à des organisations ou même à des Etats deviennent "visibles", ce qui nuirait à la confiance dans le cyberespace.

En général, les risques peuvent être calculés comme suit:

Risque: = Probabilité* Impact

D'un point de vue technique, les cyberrisques peuvent être dus à des erreurs de conception, à des anomalies, à une défaillance des composants numériques pendant le fonctionnement, à des dysfonctionnements ou à des comportements système émergents, en particulier dans le cas de systèmes "hyperconnectés". Une utilisation erronée ou à des fins malhonnêtes d'un système numérique, une attaque venant de l'intérieur du système ou d'un utilisateur, un accident soudain ou un événement environnemental peuvent également être à l'origine de risques. Pour réduire au minimum ces risques liés aux TIC, il faut prendre en considération une relation plus précise d'analyse des risques, à savoir: Risque-TIC: = f (Menace, Vulnérabilité, Actif).

Dans le contexte des TIC, la vulnérabilité d'un système TIC est liée aux failles ou aux défauts de conception ou de mise en oeuvre ou due à sa mauvaise application, ce qui

---

88 Nicolas Gold, Andrew Mohan; Clair Knight, Malcolm Munro: "Understanding Software-Oriented Software"; dans: IEEE Software; (2004).

89 Mo Jamshidi: "System-of-systems engineering: a definition"; dans: IEEE SMC; (2005).

90 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; publié par Ashgate Publishing Limited; (2006).

peut entraîner des anomalies, une réduction des capacités, un dysfonctionnement des éléments du système ou même l'effondrement du système. Avant d'envisager les solutions possibles, il faut tout d'abord identifier et classer ces vulnérabilités. A cet égard, on effectue une évaluation des risques liés aux TIC, puis on classe les vulnérabilités de l'infrastructure et des services TIC et les contre-mesures correspondantes par ordre de priorité. Une analyse quantitative des risques pourrait ensuite être menée, par exemple de la manière suivante:

Risque TIC: = ((Vulnérabilité*Menace/Note de la contre–mesure) *Valeur de l'actif.

Condition indispensable pour l'élaboration d'une stratégie de résilience pour les TIC, il faut effectuer des analyses de fiabilité et de disponibilité, qui devraient tenir compte des méthodes génériques ci-après pour améliorer la fiabilité et la disponibilité du système[91]:

- *Prévention des anomalies* – éviter que des erreurs ou des anomalies se produisent grâce à une conception et à une mise en oeuvre rigoureuses.
- *Suppression des anomalies* – repérer les erreurs qui pourraient entraîner une anomalie ou une défaillance en appliquant des méthodes de test, de vérification et de validation.
- *Tolérance aux anomalies* – prévoir un système redondant (par exemple, avec plusieurs fois une même ressource et/ou une diversification des mises en oeuvre) pour prendre le relais ou permettre un ajustement en cas d'anomalie.
- *Anticipation des anomalies/défaillances* – analyser et évaluer les conséquences des anomalies pouvant entraîner une défaillance du système, ainsi que les conséquences sur le fonctionnement du système[92].

D'un point de vue analytique, les graphes de dépendance (comme la Figure 1) ou les schémas fonctionnels de fiabilité sont des solutions simples pour analyser les effets et les conséquences indirectes des erreurs, des anomalies, des défaillances ainsi que des contre-mesures précises, comme indiqué ci-dessus[93].

---

91 Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: "Basic Concepts and Taxonomy of Dependable and Secure Computing"; IEEE Transactions on Dependable and Secure Computing; (2004).

92 Ibid.

93 Ibid.

En plus de ces vulnérabilités liées aux TIC, d'autres menaces dues à des défauts doivent être prises en considération en ce qui concerne la cyberconfiance. "Une menace est un danger potentiel qui peut exploiter une vulnérabilité pour mettre à mal la sécurité et, de cette manière, causer des dégâts. Par conséquent, d'autres menaces dues aux activités d'utilisateurs humains impliquant les ressources du système, à des accidents, à des catastrophes naturelles ou à d'autres événements extérieurs inattendus doivent être examinées et évaluées"[94].

Les activités humaines constituant une menace peuvent être menées de manière intentionnelle (par exemple, par des utilisateurs internes, des pirates) ou être le résultat non intentionnel d'une opération ou d'un comportement de l'utilisateur. Aux fins de l'analyse des risques, il faut recenser les activités humaines les plus à risques et analyser les vulnérabilités correspondantes. Outre les vulnérabilités et les menaces, les analyses des cyberrisques doivent tenir compte des incidences sur les capacités, les actifs et la valeur des différents actifs d'un système.

Les approches ci-après pourraient être envisagées pour mettre en place la cyberrésilience[95]:

- Prévention des défauts – éviter que des défauts tels que des erreurs, des anomalies et des défaillances se produisent aux niveaux physique et technique en concevant, en mettant en oeuvre et en exploitant de manière méthodique le système et les procédures de fonctionnement; aux niveaux supérieurs, on peut pour ce faire appliquer, à chaque niveau, des normes, des règlements ou des règles de comportement acceptés spécifiques.
- Suppression des défauts – repérer les défauts qui pourraient entraîner une anomalie, une défaillance, un dysfonctionnement ou une mauvaise utilisation en appliquant des méthodes de test, de vérification et de validation.
- Tolérance aux défauts – prévoir un système redondant, par exemple avec plusieurs fois une même ressource et un même service et une diversification des mises en oeuvre, pour prendre le relais ou permettre un ajustement en cas de défaut.
- Anticipation des défauts – étudier les vulnérabilités dans des scénarios plausibles en effectuant de nombreuses simulations, en analysant les risques correspondants et en évaluant les conséquences de la mise en oeuvre des stratégies de résilience dans ce contexte.

---

94 Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; dans: K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg; (2012).

95 Ibid·

L'élaboration d'une stratégie globale de résilience s'appuyant sur ces analyses des risques et de la fiabilité suppose en outre des mécanismes d'ajustement et de rétablissement, qui permettent à un système de se rétablir complètement de lui-même à partir d'un état indisponible, d'états de qualité de fonctionnement dégradée ou après une intrusion. La plupart des systèmes naturels ou biologiques ont développé des mécanismes d'autorégénération ou d'autoreconfiguration. Dans le cas des systèmes techniques, par exemple pour les processus ou les organisations fonctionnant comme des organismes biologiques (appelés capacités informatiques organiques), des méthodes de couverture, d'ajustement et de rétablissement correspondantes doivent être étudiées et utilisées comme hypothèse au stade de la conception du système. Les études scientifiques concernant l'informatique et la communication organiques portent sur des méthodes d'inspiration biologique susceptibles d'améliorer la résilience des systèmes TIC et cyberphysiques – concepts à utiliser pour la mise en oeuvre de systèmes numériques à auto-x (x pouvant être remplacé par exemple par protection, régénération, optimisation ou configuration)[96]. Conformément aux résultats des travaux de recherche menés dans des domaines comme le génie cognitif ou l'exploration des données, les principes de conception des systèmes intelligents ont évolué et peuvent être appliqués pour l'identification et l'évaluation des risques permanents, ainsi que pour l'application de mesures prédictives pour permettre la résilience du système.

Les mesures ci-après, qui sont présentées de la base vers le haut du système, sont des exemples de mesures qui peuvent être prises à chaque niveau pour éviter les anomalies, les dysfonctionnements, les défaillances ou les interruptions ou assurer le rétablissement lorsque de telles situations se produisent, ou encore pour améliorer la cyberrésilience du point de vue de l'ingénierie informatique[97],[98],[99]:

- au niveau physique – restrictions concernant l'utilisation de matériel et d'équipements uniquement dans des conditions environnementales prédéfinies (par exemple, en ce qui concerne les températures, les rayonnements). En outre, il est possible d'assurer une certaine redondance

---

96 "Organic Computing"; Ed. Rolf Würtz; dans: Springer series Understanding Complex Systems; Springer (2008).

97 Yue Yu, Michael fry, Alberto Schaeffer-Filho et.al.: "An Adaptive Approach to Network Resilience: Evolving Challenge Detection and Mitigation"; dans: 8th IEEE Internat. Workshop on the Design of Reliable Communication Networks; (2011).

98 Dorothy Reed, Kailash Kapur, Richard Christie: "Metzhodology for Assessing the Resilience of Networked Infrastructure"; dans: IEEE Systems Journal, Vol. 3 No. 2; (2009).

99 Piotr Cholda, Anders Mykkeltveit et. al.: "A Survey of Resilience Differentiation Frameworks in Communication Networks"; dans: IEEE Communications, Surveys, Vol.9 No.4; (2007).

en utilisant du matériel supplémentaire, des processus d'exploitation optionnels, etc. ou en diversifiant la mise en oeuvre d'un composant;

- au niveau technique – des dispositifs de calcul (n sur m), des concepts de transmission et de codage des données redondants ou l'utilisation de protocoles de transmission sécurisés différents mais normalisés sont des solutions non seulement pour éviter la propagation des anomalies, mais aussi pour permettre l'auto-ajustement. Par ailleurs, la diversification, moyennant, par exemple, la mise en oeuvre d'algorithmes de calcul différents, de plusieurs noeuds de calcul ou l'utilisation de différents concepts de stockage, sont autant de mesures propres à éviter la propagation des anomalies, à renforcer la fiabilité d'un système et à permettre la résilience au niveau technique[100];
- au niveau de l'information – l'objectif est la "protection de la confidentialité, de l'intégrité et de la disponibilité de l'information; en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées." – (ISO/CEI 27000[101]). On peut, par exemple effectuer un codage redondant ou utiliser des algorithmes de cryptage/décryptage forts ou des protocoles de transmission de données sécurisés pour empêcher les anomalies, les utilisations abusives ou la corruption; en ce qui concerne les outils, il est possible d'installer des systèmes et des réseaux SCADA (contrôle de surveillance et acquisition de données)[102] au niveau de l'entreprise/privé, afin respecter les bonnes pratiques, les processus-métier, les flux d'opérations et les normes, les règles et les restrictions en matière de sécurité établis et d'appliquer des codes de conduites internes[103];
- au niveau de l'entreprise/institutionnel/privé – ensemble de lois et de règles de fonctionnement; codes de conduite institutionnels, régionaux et culturels; éducation adaptée; diffusion de l'information et formation pour mieux faire connaître les questions de cybersécurité;
- au niveau global – respecter les accords de politique acceptés à l'échelle mondiale et, dans la mesure où ils existent, les codes de conduite

---

100 Département de l'énergie des Etats-Unis: "21 Steps to Improve Security of SCADA Networks"; (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf.

101 Norme ISO/CEI: Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire; (2014).

102 Département de l'énergie des Etats-Unis: "21 Steps to Improve Security of SCADA Networks"; (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf.

103 Amy Lee, John Vargo, Erica Seville: "Developing a Tool to Measure and Compare Organizations Resilience"; dans: Nattural Hazards Review; ASCE, February (2013).

internationaux; plus précisément, créer un ensemble de lois et de règles de fonctionnement internationales, mettre en place et appliquer des codes de conduites régionaux et culturels; assurer une éducation adaptée; diffuser le matériel didactique et proposer des formations pour mieux faire connaître les questions de la cybersécurité.

Cette liste de mesures et de méthodes destinées à renforcer la cybersécurité et, partant, la cyberconfiance est loin d'être exhaustive.

2.2 Accroître la résilience des systèmes d'informatique en nuage et de mégadonnées

Par Vladimir Britkov

Les mégadonnées et l'informatique en nuage représentent les principales nouveautés dans le domaine des TIC. Selon les estimations du cabinet Gartner, 64% des organisations dans le monde ont investi dans les mégadonnées ou prévoient de le faire. Ces mégadonnées sont des quantités énormes d'information numérique sur les êtres humains et notre environnement, dont le volume devrait doubler tous les deux ans. La technologie des mégadonnées comprend le nouveau domaine de "l'informatique décisionnelle", qui permet une plus grande cyberrésilience dans les domaines des mégadonnées et de l'informatique en nuage.

Les infrastructures en nuage à grande échelle, le nombre et la diversité des sources et des formats de données, le caractère ininterrompu de l'acquisition des données ainsi que la circulation d'un volume important de données d'un nuage à l'autre entraînent autant de vulnérabilités de sécurité particulières. Par conséquent, les mécanismes de sécurité traditionnels, qui sont conçus pour sécuriser des données statiques (et non fournies en continu) à petite échelle, sont inadaptés. Dans la présente contribution, nous mettons en avant les dix principaux points qui permettront d'assurer la sécurité et la confidentialité des mégadonnées, lesquels, nous l'espérons, feront que l'on se concentrera davantage sur le renforcement des infrastructures de mégadonnées.

La confiance, facteur incontournable d'une relation commerciale fructueuse entre un fournisseur de services de nuage et un client, est l'une des principales questions liées à la sécurité. Toutefois, il n'existe pas de lien de confiance particulier permettant de garantir qu'aucune attaque venant de l'intérieur ou aucun autre incident de sécurité ne visera les informations stockées dans le nuage. Ce point est tout naturellement considéré comme un facteur essentiel pour les entreprises lorsqu'elles décident de faire appel à un fournisseur de services en nuage. Les clients peuvent cependant conclure avec le fournisseur de services en nuage, un accord de niveau de service (SLA) définissant les termes et les conditions de la relation contractuelle entre le client et le

fournisseur de services en nuage. Les accords SLA présentent un intérêt particulier en ce qui concerne la protection des données du client hébergées dans le nuage mais, le nuage étant international par nature, il s'étend généralement sur de nombreuses juridictions, où les prescriptions juridiques applicables sont souvent différentes.

Traditionnellement, les infrastructures de mégadonnées étaient officiellement privées et isolées des réseaux généraux. Combinées à l'adoption des méthodes d'exploration des données, les mégadonnées sont aujourd'hui accessibles facilement et pour un coût modique pour les organisations, qu'elles soient grandes ou petites, grâce à l'infrastructure publique en nuage. Les infrastructures logicielles permettent aux développeurs de mettre facilement à profit des milliers de noeuds de calcul pour le traitement parallèle de données. Pour protéger l'infrastructure des systèmes de mégadonnées, il faut sécuriser les opérations de calcul réparties et les mémoires de données. Pour sécuriser les données, la dissémination d'information doit préserver la confidentialité et les données sensibles doivent être protégées grâce à l'utilisation de la cryptographie et d'un contrôle d'accès granulaire.

La gestion du volume énorme de données nécessite des solutions redimensionnables et réparties, à la fois pour sécuriser les mémoires de données et pour permettre des audits efficaces et connaître la provenance des données. Enfin, le flux de données continu en provenance de différents points d'extrémité doit être vérifié du point de vue de l'intégrité et peut être utilisé pour procéder à des analyses en temps réel des incidents de sécurité afin de garantir l'intégrité de l'infrastructure.

On trouvera ci-après les dix principaux points qui permettront d'assurer la sécurité et la confidentialité des mégadonnées:

1. Sécurisation des opérations de calcul dans les cadres de programmation répartie
2. Application de bonnes pratiques de sécurité pour les mémoires de données non relationnelles
3. Sécurisation des mémoires de données et des journaux de transaction
4. Validation/filtrage à l'entrée des points d'extrémité
5. Suivi de la sécurité en temps réel
6. Exploration et analyse des données préservant la confidentialité, redimensionnable et composable
7. Sécurité centrée sur les données mise en oeuvre par des moyens cryptographiques
8. Contrôle d'accès granulaire
9. Provenance des données.
10. Data provenance

Mettre en place une infrastructure des mégadonnées sécurisée

Pour surmonter les problèmes que posent la sécurité et la confidentialité, il faut généralement se pencher sur trois questions distinctes:

1. Modélisation: établir officiellement un modèle de menace qui couvre la plupart des scénarios de cyberattaque ou de fuite des données.
2. Analyse: trouver des solutions faciles à utiliser fondée sur le modèle de menace.
3. .Mise en oeuvre: mettre en oeuvre la solution dans les infrastructures existantes.

Sécuriser les opérations de calcul dans les cadres de programmation répartie

Cas d'utilisation: Modélisation

Le modèle de menace pour les mappeurs comprend trois grands scénarios:

1. Dysfonctionnement des noeuds d'agents de calcul – Les agents de calcul affectés aux mappeurs dans une opération de calcul répartie pourraient dysfonctionner en raison d'une configuration erronée ou d'un noeud défectueux.
2. Attaques contre l'infrastructure – Des noeuds d'agents compromis peuvent "mettre sur écoute" la communication entre les autres agents et le noeud maître en vue de lancer une attaque par répétition, une attaque de l'homme du milieu ou une attaque par déni de service sur les opérations de calcul effectuées selon le cadre MapReduce.
3. Noeuds de données malveillants – Des noeuds de données malveillants peuvent être ajoutés à un groupe et, par la suite, recevoir des données répliquées ou fournir un code MapReduce altéré.

Analyse

Conformément au modèle de menace décrit ci-dessus, il y a deux dimensions d'analyse: garantir la fiabilité des mappeurs et sécuriser les données malgré les mappeurs non fiables. Deux techniques peuvent permettre de garantir la fiabilité des mappeurs: l'établissement de la confiance ou le contrôle d'accès obligatoire (MAC).

Mise en oeuvre

On met en oeuvre le contrôle MAC en modifiant le cadre MapReduce, le système de fichiers réparti et la machine virtuelle Java qui utilise SELinux comme système d'exploitation sous-jacent.

Conclusion

Les mégadonnées se sont implantées durablement. Il est dans la pratique impensable que la prochaine génération d'applications ne consomme pas de données, ne produise pas de nouvelles formes de données et ne contienne pas d'algorithmes reposant sur des données.

Avec la discrimination du coût des environnements informatiques, la mise en réseau des environnements d'applications et la mise en commun des environnements de systèmes et analytiques dans le nuage, la sécurité, le contrôle d'accès, la compression, le cryptage et la conformité font apparaître des risques qui doivent être traités de manière systématique. Les défis correspondants figurent dans la liste des dix principaux problèmes de sécurité et de confidentialité donnés ci-après, qui doivent être résolus pour que l'infrastructure de traitement des mégadonnées et de calcul soit plus sûre et plus résiliente.

Des éléments communs propres aux mégadonnées font leur apparition pour les raisons suivantes: utilisation de multiples catégories d'infrastructure (à la fois de stockage et de calcul) pour traiter les mégadonnées; utilisation de nouvelles infrastructures de calcul, comme les bases de données NoSQL (pour les débits élevés qu'exigent les énormes volumes de données), qui n'ont pas fait l'objet d'un examen de sécurité suffisamment approfondi; impossibilité de moduler le cryptage des gros volumes de données; impossibilité de moduler les techniques de contrôle en temps réel qui pourraient être appliquées pour des volumes de données moins importants; hétérogénéité des dispositifs qui produisent les données; et flou concernant les différentes restrictions juridiques et politiques, d'où l'application de stratégies ad hoc pour assurer la sécurité et la confidentialité.

2.3 Mettre en place des systèmes de cybercontrôle résilients

Par Stefan Lüders

La vie dans notre monde actuel "occidentalisé" est régie par des systèmes de contrôle qui régulent presque tous les aspects de notre quotidien. Notre vie est en symbiose[104] avec ces systèmes de contrôle, dont elle dépend étroitement. Sans eux, nous retrouverons rapidement des conditions de vie correspondant à celles du Moyen Age[105]. Vu notre dépendance vis-à-vis de ces systèmes de contrôle, il est essentiel de garantir leur stabilité et leur résilience.

---

104 Voir également l'article de Stefan Lüders "Notre vie en symbiose," Bulletin du CERN, 2014.

105 Tout cela est bien décrit dans le roman de Marc Elsberg "Blackout: Morgen ist es zu spät" Blanvalet, mars 2012.

Toutefois, ces systèmes de contrôle sont aujourd'hui vulnérables aux défauts des systèmes informatiques standard qui les commandent. Ils utilisent les mêmes techniques que celles utilisées dans les centres informatiques modernes: le protocole Ethernet, le protocole TCP/IP, le World Wide Web et la messagerie électronique ont remplacé les communications par bus de terrain propriétaires; grâce aux ordinateurs, il n'est plus nécessaire de disposer d'écrans, de jauges et de tableaux d'affichage manuels; le système d'exploitation Microsoft Windows remplace les terminaux à lignes de commande personnalisées.

Par ailleurs, les logiciels sont rarement de grande qualité et contiennent des défauts, des failles, des erreurs et des bugs. Pour répondre à la demande du marché, les logiciels sont commercialisés dans leur version bêta, c'est-à-dire en état de fonctionnement, mais avec des failles et des vulnérabilités qui sont détectées (et éliminées) à un stade ultérieur. Les utilisateurs et les entreprises de services collectifs ne demandent pas nécessairement d'amélioration en raison des coûts que cela supposerait.

Comme si cela ne suffisait pas, les technologies de l'information standard ont ouvert la voie à un véritable nouveau marché de la délinquance – un "réseau obscur" où des attaquants s'associent pour infiltrer et exploiter les systèmes de technologies de l'information, et compromettent ainsi la confiance des utilisateurs. Aujourd'hui, des acteurs mal intentionnés cherchent en permanence les vulnérabilités et les failles de chaque application Internet, de chaque site web, de chaque système d'exploitation et de chaque application logicielle grand public pour les exploiter à leur propre avantage ou pour vendre ce qu'ils ont trouvé sur ce marché "obscur". Et dans la mesure où la prévention et le renforcement de la résilience face à ces attaques sont des opérations infiniment plus complexes que l'exploitation de ces vulnérabilités, les attaquants bénéficient d'un avantage certain.

Néanmoins, les technologies de l'information en général se sont jusqu'à présent avérées suffisamment résilientes pour que ces attaques n'aient pas de répercussions à grande échelle sur notre quotidien, et, bien que l'économie " obscure" continue de prospérer et que le système juridique international peine à suivre le rythme, il est rare que les conséquences soient sérieuses pour le grand public[106].

Le développement exponentiel des systèmes de contrôle et leur intégration dans les technologies de l'information standard ont changé la donne. Certes, ces systèmes tirent parti des technologies de l'information, mais ils ont également hérité de leurs vulnérabilités et de leurs failles. Cette situation fragilise et expose des processus de contrôle solides, propriétaires et personnalisés, lesquels sont en outre de plus en plus

---

106 Sauf peut-être dans le cas d'attaques portant sur les serveurs mondiaux de noms de domaine, sur les principales voies Internet et, plus généralement, dans le cas d'attaques concernant la vie privée de citoyens menées par des organismes gouvernementaux.

souvent la cible d'acteurs mal intentionnés, comme le montrent les articles suivants parus dans de grands médias: "La Russie prise pour cible par des hackers" (The Register, 2000), "Des hackers s'attaquent au système de gestion de l'eau de Pennsylvanie" (InTech, 2006), "Les usines électriques de la TVA vulnérables face aux cyberattaques, selon la GAO" (The Washington Post, 2008), "Un employé poursuivi pour avoir piraté le système de contrôle du canal de Californie" (Computerworld, 2009), "Le trafic aérien aux Etats-Unis exposé à un " risque sérieux" de cyberattaques" (Flightglobal, 2009), "Le réseau électrique américain infiltré par des espions" (The Wall Street Journal, 2009), "Rapport: Des hacker se sont introduits dans les systèmes de contrôle du trafic aérien de la FAA" (CNET, 2009), "Rapport: Des cyberattaques à l'origine de pannes d'électricité au Brésil" (Wired, 2009), "DHS: Les fournisseurs d'eau et d'électricité américains victimes de cyberattaques quotidiennes" (Computerworld, 2012), "Protection insuffisante des écluses, des stations de pompage et des ponts" (Radio Netherlands Worldwide, 2012), "Le réseau électrique américain vulnérable à presque tout" (OilPrice.com, 2012). Le sabotage des installations d'enrichissement d'uranium de Nantaz en Iran, qui serait l'oeuvre des services secrets israéliens et américains, est une autre affaire qui a fait les gros titres il y a peu: "Le virus Stuxnet marque le début d'une nouvelle ère dans la cyberguerre" (Spiegel Online, 2010). Des ordinateurs fonctionnant sous Windows infectés par le virus "Stuxnet" ont falsifié les écrans que voyaient les opérateurs des installations, se sont téléchargés eux-mêmes dans le système de contrôle, puis ont modifié la vitesse de rotation de centaines de centrifugeuses, empêchant ainsi l'enrichissement de l'uranium.

Alors que "Stuxnet" est considéré comme le tout premier cybersabotage démontré, il met aussi en évidence le dilemme que représentent les cyberattaques lancées avec l'aide d'un Etat. Richard A. Clarke, ancien Coordonnateur national pour la sécurité et le contre-terrorisme à la Maison-Blanche, a déclaré que les Etats-Unis pourraient être en mesure de faire sauter une centrale nucléaire ou un camp d'entraînement terroriste n'importe où dans le monde, mais qu'un certain nombre de pays pourraient riposter par une cyberattaque et que "les représailles pourraient entraîner l'effondrement de tout le système économique du pays (...) parce que nous ne pouvons pas le défendre aujourd'hui."

Il est en effet actuellement impossible de protéger les systèmes de contrôle avec des techniques analogues à celles utilisées pour protéger des installations comme les centres informatiques, par exemple avec des "correctifs" (c'est-à-dire, en éliminant les vulnérabilités en mettant à jour le système d'exploitation).

Les centres informatiques modernes sont gérés par des systèmes de gestion de la configuration. La mise à jour ou même la réinstallation d'un grand nombre de serveurs est généralement possible dans un temps très court. Les redondances et la virtualisation facilitent ce processus, étant donné que l'on effectue la maintenance de sous-groupes de fermes de serveurs pendant que le serveur principal continue de fonctionner. En

revanche, il est actuellement impossible d'utiliser des correctifs flexibles pour les systèmes de contrôle car les fenêtres de maintenance sont rares et les exigences en matière de conformité strictes, en particulier en ce qui concerne les processus de sécurité pertinents. On considère que seuls les systèmes pleinement conformes et certifiés (par exemple, recertification vis-à-vis d'un niveau de sécurité intégrée, SIL) sont sûrs, mais effectuer des tests approfondis prend du temps et entraîne des coûts supplémentaires. Par ailleurs, il n'est pas toujours garanti que les nouveaux correctifs pour systèmes d'exploitation soient compatibles avec les logiciels utilisés par le système de contrôle, et les fabricants tardent souvent à faire la déclaration de conformité, s'ils en font une. Les systèmes intégrés, qui sont difficiles à mettre à jour, compliquent encore la situation. Enfin, même si souvent, le parc informatique est recyclé tous les trois à cinq ans, on conserve le vieux matériel pour le processus de contrôle aussi longtemps que possible, voire bien au-delà de la durée de vie officielle de son système d'exploitation[107].

Les différentes méthodes utilisées pour le contrôle d'accès constituent un autre exemple. Les services des centres informatiques privilégient généralement la confidentialité, l'intégrité et la disponibilité. Le contrôle d'accès est par conséquent capital et les techniques d'authentification et d'autorisation sont bien intégrées et centralisées grâce à une signature unique avec ou sans déploiement multifacteurs, à la gestion de certificats X.509 et à des annuaires LDAP/AD à gestion centralisée. Les systèmes de contrôle privilégient la disponibilité par rapport à la confidentialité et à l'intégrité. Ainsi, l'homme doit toujours pouvoir accéder au processus.

Afin de faciliter le transfert des opérations, les mots de passe sont partagés entre opérateurs. En outre, souvent parce qu'ils sont propriétaires ou anciens, le matériel et les logiciels ont des portes dérobées non signalées, fonctionnent avec des mots de passe par défaut qui n'ont pas été modifiés, ne permettent pas de bloquer des connexions non autorisées à l'aide de pare-feu internes ou de listes de contrôle d'accès et sont difficiles à intégrer dans les solutions de gestion d'identité centralisée. On considère que le cryptage consomme trop de ressources. Généralement, les systèmes de contrôle exigent ou utilisent des dispositifs de protection supplémentaires qui assurent leur sécurité et contrôlent l'accès. Une bonne protection du réseau devient alors d'autant plus importante, mais elle est impossible à assurer, étant donné qu'un modèle efficace de "défense en profondeur" suppose des moyens de protection pour chaque couche de matériel du système d'exploitation et des applications du réseau.

Enfin, la robustesse est de la plus haute importance. Comme nous l'avons déjà dit, des attaquants tentent en permanence de trouver des failles dans les systèmes de technologies de l'information standard installés dans les centres informatiques, en

---

107 L'arrêt progressif de l'utilisation du système d'exploitation Microsoft Windows XP constitue donc un autre problème pour les fournisseurs de services collectifs.

particulier lorsqu'ils sont directement accessibles depuis l'Internet. Il est possible de contrer ces tentatives d'intrusion ou d'exploitation de vulnérabilités en gérant correctement les centres en les tenant à jour pour tout ce qui concerne ce phénomène, en mettant en place des systèmes adaptés de détection des intrusions et en les contrôlant. Grâce à l'expérience et aux connaissances accumulées pendant plusieurs décennies concernant les différents scénarios d'attaques et les failles potentielles, ainsi qu'aux moyens acceptés de partage d'informations entre parties prenantes, il est plus facile de se protéger contre les incidents, de les détecter et d'y faire face. A l'inverse, on ne peut pas considérer que les systèmes de contrôle soient cyberrobustes. Certes, les équipements physiques sur lesquels ils sont installés peuvent l'être, mais on a été constaté à plusieurs reprises que leur mise en oeuvre logicielle ne respectait pas les normes communes en matière de technologies de l'information, échouait aux tests de sécurité de base et ne disposait pas de moyens essentiels pour repousser les attaques[108]. Les systèmes de contrôle répondent à des cas d'utilisation sont bien définis, mais ne sont plus efficaces lorsque ces cas sont moins bien définis. Contrairement à ce qui se pratique pour le matériel standard de technologies de l'information, la "sécurité" ne fait pas partie intégrante des dispositifs utilisés par les systèmes de contrôle. Même si c'était le cas, étant donné que la mise en oeuvre de la sécurité est propre à chaque entreprise et opaque, les fournisseurs de services collectifs ont du mal à déterminer si la sécurité est réellement adaptée ou s'il s'agit juste d'une illusion.

Enfin et surtout, la communauté s'occupant des systèmes de contrôle s'efforce actuellement de trouver un consensus sur la manière de mener à bien une "communication responsable", c'est-à-dire sur la manière d'annoncer et de présenter au distributeur concerné, puis aux fournisseurs de services collectifs, des vulnérabilités qui viennent d'être découvertes. Dans le monde des technologies de l'information standard, on accepte qu'un délai de trois à neuf mois s'écoule entre le moment où le fournisseur de logiciel est informé et le moment où toutes les informations sont communiquées au public, mais d'aucuns considèrent que ce délai est trop court, étant donné que la phase de contrôle dans le cycle de développement d'un logiciel est beaucoup plus longue et que la mise en oeuvre de correctifs par un fournisseur de services collectifs doit être bien coordonnée et programmée. En réalité, l'ensemble du processus correspondant prend normalement un an.

Ce problème doit être résolu pour que les systèmes de contrôle deviennent cyberrésilients. Les systèmes de contrôle doivent faire en sorte que la sécurité devienne partie intégrante de l'ensemble des fonctions, de la disponibilité, des possibilités d'utilisation et de mise à jour et de la sécurité. Les experts en systèmes de contrôle

---

108 "CERN tests reveal security flaws within industrial networked devices", *The Industrial Ethernet Book*, 2006.

doivent suivre des formations adaptées dans le domaine des technologies de l'information et, en particulier, de la sécurité de ces technologies. Cette formation doit commencer dès le lycée et l'université, la sécurité devant être intégrée dans les programmes et non considérée comme une "option". Mieux encore, tous les aspects se rapportant aux technologies de l'information devraient être confiés à des spécialistes de ces technologies compétents, capables de faire la différence entre les différents besoins liés à l'exploitation des systèmes de contrôle et des centres informatiques. Il faudra peut-être trouver de nouveaux compromis pour concilier la nécessité d'assurer en permanence la disponibilité et la mise en oeuvre, sans délai, des correctifs, de disposer d'un accès facile et d'appliquer un contrôle d'accès rigoureux. En parallèle, les techniques de virtualisation des technologies de l'information pourraient offrir la solution idéale pour surmonter ces problèmes et servir de nouvelles bases pour la mise en oeuvre de correctifs entre les phases de tests, de préproduction et d'exploitation des systèmes. La gestion complète des logiciels, les systèmes de gestion de versions, des cycles de développement des logiciels comprenant également leur mise à jour, des tests de régression approfondis et les compilations automatiques de nuit doivent devenir la norme pour les systèmes de contrôle également. L'intégration dans des inventaires très complets et mis à jour en permanence est également indispensable. Il faut obligatoirement disposer d'une documentation très complète sur la base de l'installation, tous les dispositifs, les comptes et les applications, ainsi que sur leurs interdépendances, pour comprendre les risques et déployer des mesures de protection. Des tests d'intrusion doivent être effectués par défaut. Dans l'idéal, on devrait avoir automatiquement recours à des recettes et à des procédures convenues et pleinement ouvertes pour évaluer les vulnérabilités afin que les fournisseurs et les fabricants, les fournisseurs de service et les responsables de l'intégration, mais aussi les gouvernements, les établissements universitaires et les autorités de certification puissent évaluer de manière indépendante la sécurité de tel ou tel dispositif, équipement ou logiciel de contrôle. De telles procédures devront obligatoirement accroître la robustesse des systèmes de contrôle aujourd'hui pour, à terme, améliorer leur résilience en cas d'activités malveillantes et, il faut l'espérer, ouvriront la voie à un mécanisme de certification de type ISO 9001.

Aucune de ces étapes n'est anodine ou facile à franchir. Pour la génération actuelle de systèmes de contrôle et d'experts de ces systèmes, il est même peut-être trop tard. Par conséquent, nous devons nous concentrer sur l'avenir et avoir pour objectif de lier encore plus étroitement les technologies de l'information utilisées pour les systèmes de contrôle et celles utilisées pour les centres informatiques. Notre degré de réussite déterminera ce que sera notre avenir.

2.4 La cyberrésilience vue par le secteur privé

Par Danil Kerimi

Le monde dans lequel nous vivons aujourd'hui est extrêmement complexe et hyperconnecté. Il nous offre des possibilités sans précédent, mais nous confronte aussi à des risques qui étaient inimaginables il y a seulement quelques années. Nous commençons seulement maintenant à comprendre les changements sociaux, politiques et économiques qu'il entraîne en ajustant les normes, les politiques et les modèles de fonctionnement à la métaphysique du réseau.

Tous ces changements redéfinissent en profondeur la manière dont les personnes, les entreprises et les gouvernements se connectent les uns aux autres. Les modèles traditionnels de création de richesses économiques et de consommation sont remis en question par de nouveaux modèles commerciaux et de nouvelles interactions sociales découlant de l'hyperconnectivité. Aujourd'hui déjà, les industries s'appuient de plus en plus sur les moyens numériques pour leur fonctionnement en interne, ainsi que pour les interactions avec leurs partenaires. Des entités que l'on n'a jamais considérées comme de grands acteurs technologiques sont aujourd'hui confrontées à des questions qui ne font pas partie de leur domaine de compétence ou de leur zone de confort.

Le comportement des consommateurs a lui aussi évolué, avec une plus grande autonomisation, des flux d'informations plus efficaces et une offre très vaste. Les entreprises connaissent mieux que jamais le comportement des consommateurs, ce qui permet un niveau de personnalisation sans précédent. Elles doivent par ailleurs parvenir à s'adapter à l'environnement qui évolue rapidement, afin de réussir à répondre aux nouvelles attentes des consommateurs, comme la création conjointe de produits et la mise au point rapide de prototypes.

L'hyperconnectivité devient un moteur qui permet souvent de réduire les obstacles à l'entrée des marchés, de développer les échanges commerciaux et de renforcer la concurrence au sein des secteurs mais aussi entre eux, en redéfinissant constamment l'environnement dans lequel les secteurs évoluent et en remettant en question le cloisonnement des politiques. L'automatisation ininterrompue des différentes tâches et des différents processus, qui s'inscrit dans une évolution plus large vers des économies du savoir, crée une pression considérable sur les marchés du travail traditionnels.

Le rythme de l'innovation est tel que non seulement des emplois manuels sont détruits, mais on entre également dans une phase de déclin structurel à long terme pour des emplois davantage fondés sur les connaissances. En outre, notre système éducatif actuel ne permet pas de répondre à la demande de personnel doté de nouvelles compétences (par exemple, des spécialistes des données) qui remplace le personnel occupant des emplois plus traditionnels.

Ces transformations découlent des technologies de l'information et de la communication. L'hyperconnectivité est l'oeuvre d'entreprises technologiques du monde entier et remet en question la définition même de l'entreprise technologique. Ecoutez les dirigeants de l'industrie automobile parler des voitures d'aujourd'hui et vous aurez peut-être l'impression que ces voitures ne sont que des terminaux équipés de roues. Les entreprises de soins de santé parlent de données et les banques de cybersécurité. Du secteur bancaire aux consommateurs en passant par les entreprises du secteur de l'énergie, le monde entier mise sur le numérique.

Alors que par le passé, les entreprises technologiques venaient bousculer les différents modèles d'entreprises et transformer d'autres secteurs, nous sommes aujourd'hui arrivés à un stade où d'autres secteurs viennent bousculer des modèles d'entreprises numériques plus aboutis.

Cette évolution se retrouve dans notre esprit de consommateur. Selon le rapport le plus récent du cabinet Interbrand[109], huit des dix plus grandes marques sont des entreprises TIC. La moitié des marques entre la 10ème et la 20ème place de ce classement sont des entreprises connues qui nous ont aidés à façonner le paysage technologique d'aujourd'hui. La valeur totale de ces marques technologiques figurant dans le top 20 dépasse les 1 000 milliards de dollars. Si elles correspondaient à un pays, celui-ci aurait largement sa place à la table du G20.

En 2014, trois sociétés cotées en bourse parmi les plus importantes en termes de capitalisation boursière sont également des grands noms des TIC. Selon la dernière liste établie par le magazine Fortune, six des vingt personnes les plus influentes au monde viennent du secteur des technologies, onze sont des responsables politiques ou religieux et les trois autres sont des directeurs du secteur de la finance, du commerce ou de l'énergie[110]. Il sera intéressant de voir quel sera le classement pour 2015.

Notre dépendance totale vis-à-vis du cyberespace pour nos activités quotidiennes est maintenant un fait acquis. C'est pourquoi nous nous inquiétons des risques associés à ce cyberespace et nous craignons qu'il devienne inaccessible. La cyberrésilience, ce concept qui nous était étranger il y a quelques années, est maintenant un thème

---

109 www.interbrand.com/en/best-global-brands/2013/Best-Global-Brands-2013.aspx

110 www.forbes.com/powerful-people/list/

récurrent dans les réunions des conseils d'administration, dans les débats politiques et dans les discussions dans la sphère privée partout dans le monde. Le monde est en train d'apprendre que tout objet connecté peut être piraté et que l'enjeu n'est pas que ces objets soient sécurisés en permanence, mais plutôt qu'ils soient suffisamment souples et résilients pour pouvoir fonctionner dans des conditions défavorables.

La vitesse, la mobilité et la collaboration sont des caractéristiques essentielles pour une entreprise qui veut réussir à l'ère du numérique. Pour continuer de mettre à profit les avantages qu'offre l'hyperconnectivité, il faut d'urgence mettre en place un écosystème international cyberrésilient. Ces deux dernières années, le Forum économique mondial a réuni un groupe de responsables et de décideurs afin d'étudier comment faire pour rendre l'environnement numérique plus résilient. Les différents représentants des gouvernements et des secteurs avaient tous en commun de s'inquiéter de l'augmentation considérable du nombre de cyberincidents dans le monde. Pour reprendre un concept tiré du droit de l'environnement, il est admis que les parties prenantes ont des responsabilités communes mais différenciées en ce qui concerne le cyberespace, alors que la cyberrésilience exige un niveau élevé de collaboration multi-parties prenantes. Comme c'est le cas dans d'autres domaines de la gouvernance mondiale, les pays en développement, qui souvent connaissent mal les cybermenaces et n'ont pas les moyens d'y faire face de manière adaptée, sont aussi concernés par les nouveaux risques que les pays développés. Il s'avère qu'à mesure que la dépendance de nos économies vis-à-vis de la connectivité numérique augmente, la cyberrésilience devient peu à peu une capacité clé pour les dirigeants dans tous les secteurs et dans tous les domaines stratégiques.

Face à ces inquiétudes, le Forum économique mondial s'est penché sur la question de la cyberrésilience en demandant aux chefs d'entreprise (et non aux responsables de la sécurité de l'information, des technologies, etc.) et aux hauts responsables publics de reconnaître l'interdépendance de toutes les parties qui ont un rôle à jouer dans la promotion d'un espace numérique commun résilient. Ce faisant, nous avons mis l'accent sur le rôle des dirigeants en encourageant la sensibilisation des hauts responsables et une gestion intégrée des risques. Nous avons en outre encouragé l'adoption d'une approche systémique globale de la cyberrésilience car les activités d'une entreprise vont au-delà du seul environnement de cette entreprise et s'inscrivent dans la chaîne de valeurs dans son ensemble, des fournisseurs aux clients.

L'opinion publique mais aussi un grand nombre de personnes attachent une très grande importance à la cyberrésilience. Au cours des prochaines années, les dépenses annuelles dans la cyberrésilience devraient augmenter, pour passer de 69 milliards USD en 2013 à 123 milliards USD en 2020[111]. Ces estimations dépendent évidemment des analyses de marché, qui tiendront compte à leur tour des cybermenaces existantes et

111 www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

anticipées. Ainsi, un scénario prévoit une augmentation de 13% des investissements dans la cyberrésilience, lesquels atteindraient 139 milliards USD par an, avec un renforcement de la coopération entre les secteurs publics et privés compte tenu de leurs moyens de défense. Selon un autre scénario, nous pourrions attendre une hausse de 28% des dépenses, qui atteindraient alors 157 milliards USD par an, si les capacités d'attaque dépassent les capacités de défense et que les réactions sont "au coup par coup" plutôt que fondées sur la coopération.

Les discussions concernant les cyberrisques portent souvent sur des scénarios catastrophes ou sur une "cyberapocalypse" redoutée et entraînent de nombreuses affirmations éculées comme "il n'y a plus de vie privée" ou "le maillon le plus faible". Toutefois, on devrait peut-être s'inquiéter tout autant des occasions qui ne pourraient être concrétisées en cas de rejet massif ou de segmentation de l'écosystème numérique actuel. Une seule grande "cybercatastrophe" ou une dégradation progressive ("mort à petit feu") pourrait entraîner un rejet.

La segmentation pourrait avoir lieu au niveau des régions, des pays et des entreprises et de nombreuses raisons pourraient amener un grand nombre d'acteurs à y être favorables. Ainsi, ce phénomène de segmentation pourrait s'amorcer s'il est demandé aux gouvernements s'inquiétant du manque de fiabilité de l'environnement d'assurer eux-mêmes la sécurité dans le cyberespace. Il pourrait également concerner les politiques industrielles ou les réglementations appliquées dans les différentes juridictions.

Le cabinet Mckinsey estime que le préjudice pour la croissance économique mondiale potentielle pourrait être de 3 000 milliards USD si la sophistication croissante des moyens d'attaque aboutit à une diminution des investissements[112]. Un environnement politique complexe risque en outre de compliquer la prise de décisions économiques.

On peut donc se demander à quoi ressemble la cyberrésilience du point de vue de l'entreprise. Cela signifie tout d'abord adopter une démarche interdépendante et fondée sur les risques reposant sur le principe que l'atténuation partielle des risques est une caractéristique essentielle de tout système complexe et que la résilience d'une organisation contribue à la résilience du système en général.

---

112 Ibid.

Les entreprises, comme d'autres organisations, attachent une grande importance aux priorités fixées par leurs dirigeants. Il est par conséquent important, pour définir un programme efficace de gestion des cyberrisques et encadrer sa mise en oeuvre, d'y associer la haute direction et de mettre en place des structures d'encadrement, par exemple des comités.

L'équipe de direction devrait définir un ensemble de responsabilités différenciées et des objectifs communs et prévoir les ressources, les outils de gouvernance et les crédits nécessaires pour les atteindre et faire connaître les mesures prises en la matière. En ce qui concerne la continuité des activités, des tests de résistance des systèmes ainsi que des simulations de situations de crise de type "jeu de guerre", qui exigent une coordination entre les différents départements, des technologies de l'information aux affaires publiques, pourraient s'avérer très utiles si l'on se trouvait confronté, dans les faits, à une situation dans laquelle les acteurs n'auraient pas le temps d'étudier en détail les responsabilités de chacun et les possibilités de riposte.

Il pourrait en outre être utile d'intégrer pleinement par défaut la cyberrésilience dans la gestion au sens large de la continuité de l'activité et des risques pour l'entreprise. Il pourrait être judicieux de commencer par identifier les actifs d'information qui sont essentiels à la mission de l'organisation. La défense du périmètre était peut-être une stratégie efficace dans le passé, mais vu le niveau actuel des attaques, des tentatives d'intrusion et des menaces internes, l'environnement moderne en matière de risques suppose que l'on établisse un ordre de priorité clair entre les actifs, afin de pouvoir affecter des ressources suffisantes pour les protéger.

Pour ce faire, tous les aspects de l'exploitation ainsi que le risque sur le plan de la réputation devraient faire l'objet d'évaluations d'impact régulières. Il conviendrait en outre de mettre en place des processus pour réduire le temps nécessaire à un rétablissement complet ou partiel en cas de défaillance majeure. Il est fondamental que l'ensemble de l'entreprise soit concerné et qu'il ne soit pas considéré que cette question concerne uniquement le département des technologies de l'information.

Tous les départements, y compris ceux s'occupant du marketing, des questions gouvernementales et publiques et des relations avec les consommateurs, placés sous la direction d'une équipe de gestion de haut niveau, devront être préparés à agir simultanément en rétablissant les activités touchées, en atténuant les possibles répercussions négatives pour la marque et en gérant une éventuelle réaction de rejet des clients, ainsi que les possibles conséquences réglementaires.

De nombreuses grandes entreprises ont un directeur de la sécurité de l'information. Certaines ont clairement séparé cette fonction de celle de directeur technique/directeur informatique. En outre, certaines entreprises ont fait en sorte que, même si les emplois ne sont pas de même niveau, ils sont rattachés à des entités hiérarchiques différenciées, étant donné que les objectifs stratégiques des différentes

fonctions peuvent nécessiter des priorités différentes en termes, notamment, d'architecture technique et d'acquisition.

Ce n'est qu'avec un aperçu détaillé des différents actifs d'information et de l'importance d'une réaction adaptée et immédiate en cas d'atteinte à sa sécurité qu'une entreprise peut véritablement contribuer à sa propre cyberrésilience systémique. Les entreprises qui mettent en place des structures de cyberrésilience/de gestion des risques doivent tenir compte de l'élément important que constitue la conformité, dans la mesure où les gouvernements commencent à instaurer différents mécanismes réglementaires (codes de conduite et des bonnes pratiques d'application volontaire, signalement obligatoire des incidents, élaboration de normes), pour faire face à l'insécurité grandissante.

Le rôle que jouent les fournisseurs, les sous-traitants et les clients dans l'ensemble de la cyberchaîne d'approvisionnement est également un point important dont il faut tenir compte. Une entreprise devrait s'efforcer d'améliorer ses performances au sein de l'écosystème au sens large, élargissant ainsi le périmètre de sécurité et s'assurant qu'une coalition se met en place.

La défense en amont est l'un des domaines les plus sensibles pour les activités internationales. Etant donné qu'il est de plus en plus difficile de définir le périmètre de sécurité, l'entreprise devra s'appuyer sur des sources de données internes et externes existantes pour suivre l'évolution des menaces qui pourraient aboutir à une attaque. Toutefois, il est très difficile de comprendre à quel moment le niveau des menaces internes et celui des menaces extérieures se rejoignent, sans parler de la possibilité d'appliquer des mesures préventives et de la question de leur légitimité même lorsque le danger est avéré et imminent.

Les difficultés en ce qui concerne l'attribution sont souvent citées comme l'un des plus grands obstacles, de même que la légalité et la légitimité d'une action potentielle. Cette zone floue devient un peu plus transparente lorsqu'il existe une cyberstratégie complète au niveau du pays et de l'entreprise, qui n'est pas toujours facilement accessible. Cette stratégie devrait comprendre des éléments nationaux mais aussi internationaux clairs et transparents.

La manière d'appréhender ce problème a radicalement changé et les chefs d'entreprise ont aujourd'hui une vision plus nuancée des éléments et des techniques d'atténuation possibles. Un dialogue multi-parties prenantes est engagé aux niveaux national et international, alors que les menaces continuent d'évoluer rapidement.

L'hyperconnectivité a déjà modifié notre manière de nous connecter les uns aux autres: elle a des incidences sur notre manière de prendre des décisions et d'organiser nos vies. L'effet perturbateur des technologies de l'information entraîne de plus en plus souvent des transformations sociales et économiques. Nous avons tendance à surestimer l'impact des technologies à court terme et à sous-estimer leurs incidences à long terme

sur tous les aspects de nos vies. La réflexion sur la cyberrésilience peut être le point de départ pour comprendre et élaborer des solutions qui nous aideront à prendre des décisions en vue d'obtenir les résultats positifs que nous souhaitons tous.

2.5 Assurer la cybersécurité sur tous les plans pour accroître la cyberrésilience

Par Solange Ghernaouti

Les différentes dimensions de la cyberrésilience

Les cyberrisques sont une réalité pour chacun d'entre nous. Quiconque suit un tant soit peu l'actualité en sera convaincu. La cybercriminalité est un fléau mondial et les cyberattaques sont désormais couvertes par les doctrines militaires. Lors de son sommet de septembre 2014[113], l'OTAN a défini les cyberattaques massives comme étant des actes de guerre qui pourraient entraîner une riposte militaire et, si un membre de l'OTAN en était victime, il serait considéré que c'est l'OTAN tout entière qui est attaquée. Il est nécessaire d'admettre que les conflits se déroulent également dans le cyberespace, le plus souvent dans le cadre de cyberattaques visant les infrastructures de l'information civiles et militaires par la manipulation de l'information. Sur l'Internet, la promotion de la guerre et du terrorisme côtoie la promotion des activités légitimes et illégales, tandis que le marché noir de la cybercriminalité prospère. L'Internet devient en outre un support de communication courant pour les activités criminelles et la propagande. Les attaques visant les systèmes d'information peuvent interrompre le fonctionnement des infrastructures vitales d'un pays, permettre la mise en oeuvre de stratégies criminelles, entraîner des pertes de productivité et de compétitivité ou contribuer à la prise de pouvoir dans un pays. En outre, il est plus facile avec l'Internet de mener des activités visant à ralentir ou empêcher le développement économique d'un pays, à nuire au bon fonctionnement d'un Etat ou à le déstabiliser. Un grand nombre de systèmes d'information sont la cible de cyberactivités dont l'objectif est de déstabiliser un pays en portant atteinte à son économie, à ses institutions ou à sa réputation. Ces activités sont menées dans un contexte plus large d'hypercompétitivité économique mondiale.

113 http://www.nato.int/cps/en/natohq/news_112107.htm?selectedLocale=en (Guide du sommet de l'OTAN au Pays de Galles- Newport, 4-5 septembre 2014)

Les cybermenaces, qui ont de multiples facettes, évoluent constamment et il est important de les appréhender de manière interdisciplinaire et globale afin de les combattre en permanence, de renforcer la sécurité et la résilience des infrastructures civiles et militaires et de protéger chaque agent économique, y compris les petites et moyennes entreprises et les particuliers. Le processus de tous les instants visant à assurer la cybersécurité des personnes et des biens, mais aussi la sécurité du public, doit s'inscrire dans un projet politique venant à l'appui d'une stratégie de développement durable pour la société, qui tient elle-même compte de la culture et des spécificités du pays. Cela suppose la participation de tous les acteurs, privés et publics, aux niveaux national et international[114].

Nous créons un monde de connectivité permanente grâce aux communications mobiles, hertziennes et sans contact[115], un monde où les objets deviennent intelligents et capables de communiquer: c'est ce que l'on appelle l'Internet des objets et de presque tout ce qui contribue à créer des maisons et des villes intelligentes. Des objets aussi répandus que les voitures et les feux de circulation renfermeront des composants informatiques et des technologies Internet. Ils seront ainsi capables, dans une certaine mesure, d'agir de manière autonome et de prendre des décisions, grâce à l'intelligence qui sera contenue dans leur système de programmation. Ces objets commencent déjà à envahir les lieux publics et deviennent automatiquement la cible potentielle de cyberactivités malveillantes, car chaque entité connectée à l'Internet peut être piratée et intégrée dans un botnet qui attaquera d'autres systèmes. Les failles de sécurité de ces objets pourraient avoir de graves conséquences sur notre sécurité physique. Toujours pour faciliter la vie des gens et les activités du quotidien, des robots plus ou moins sophistiqués commencent à partager notre vie de tous les jours. Etant donné que ces robots sont capables d'influencer nos comportements et notre environnement, leur contrôle par des entités malveillantes ou indésirables pourrait également avoir de graves répercussions sur notre société. Le XXIème siècle est celui des puces électroniques RFID et des nanotechnologies – l'idée de la poussière intelligente. La convergence des mondes de l'électronique et de la biologie est de plus en plus réelle, notamment en ce qui concerne le corps humain et les différents capteurs, prothèses et autres éléments d'électronique biomédicale qui peuvent être implantés dans le corps humain pour pallier certaines de ses défaillances (par exemple, pompes à insuline et stimulateurs cardiaques). Il existe déjà des interfaces neuronales qui permettent d'interagir avec des ordinateurs par la pensée. Bien sûr, tout cela peut contribuer au bien-être à mesure que l'utilisation de ces technologies et la convergence entre l'électronique et la biologie progressent et se resserrent, mais leur utilisation à d'autres fins que celles pour lesquelles elle ont été créées pourrait aboutir à des cas de piratage,

---

114 "Cyberpower: crime, conflict and security in cyberspace"; S. Ghernaouti, EPFL Press 2013.

115 Les technologies sans contact renvoient aux technologies de communication en champ proche.

y compris de la pensée humaine. Ces nouveaux risques nous obligent à réinventer la sécurité afin de mieux gérer ces risques et de protéger nos valeurs menacées par les incidences accrues des technologies sur la société.

Le cyberespace devient un élément de civilisation sur lequel nous nous appuyons considérablement. Il est ainsi important que ses infrastructures soient solides et résilientes face à tous les types d'incidents. Le concept de cyberrésilience englobe plusieurs dimensions qui peuvent nécessiter l'adoption de mesures opérationnelles, comme, par exemple, la lutte contre la cybercriminalité, les activités complémentaires liées à la cybersécurité et à la cyberdéfense, la gestion efficace des risques énergétiques et écologiques et l'éducation et l'actualisation des compétences humaines nécessaires pour la société de l'information de demain.

Lutter contre la cybercriminalité

La communauté internationale doit s'attacher de toute urgence à être mieux préparée pour lutter contre la cybercriminalité. Aucun Etat, aucune organisation, aucun internaute n'est protégé contre les cybernuisances, qu'elles soient criminelles ou simplement énervantes.

Etre mieux préparé pour lutter contre la cybercriminalité suppose que l'on soit déjà préparé, mais à un niveau faible et insuffisant. Pour les institutions, cela peut signifier:

- Disposer des moyens (stratégies, mesures, ressources, compétences) nécessaires pour faire face à ce problème, mais à des niveaux quantitatifs et qualitatifs insuffisants.
- Disposer des moyens de protection, mais qui ne sont pas suffisamment efficaces ou adaptés.

Même si ces deux cas de figure sont courants, il ne faut pas oublier que, pour de nombreux acteurs comme les petites et moyennes entreprises et les particuliers, et pour un grand nombre d'infrastructures et d'objets connectés à l'Internet, il n'existe aucune structure de contrôle ou mesure de sécurité.

Dans le cas d'un Etat, lutter contre la cybercriminalité suppose plusieurs choses:

- Disposer d'un cadre juridique applicable au niveau national compatible avec les structures internationales.
- Disposer de structures judiciaires et de forces de police dotées des ressources et des compétences leur permettant de fonctionner au niveau national et de coopérer avec un réseau international pour lutter contre la cybercriminalité transnationale.

Au niveau international, cela suppose que la communauté internationale travaille de concert pour défendre cette cause commune que constitue la lutte contre la

cybercriminalité et qu'il n'existe pas de "paradis numériques" où les personnes malhonnêtes peuvent agir en toute impunité.

L'existence de tels paradis profiterait aux criminels qui:

- verraient dans l'Internet un moyen de commettre des délits économiques et un outil pour perpétrer des actes criminels (trafic d'êtres humains, trafic de drogue, blanchiment d'argent, …);
- considéreraient le cyberespace comme un bouclier de protection et un terrain de jeu mondial.

La lutte contre la criminalité est depuis toujours une question complexe. La cybercriminalité a accentué cette complexité et rendu la lutte encore plus difficile, que ce soit au niveau national ou international.

Dans le même temps, les exploits des cybercriminels sont régulièrement relatés dans les médias, mais il ne semble pas qu'ils entraînent l'adoption de mesures suffisamment efficaces pour limiter la progression de la force de frappe des cybercriminels ou pour réduire le nombre de victimes. Le nombre d'arrestations et de procès reste faible par rapport à la multiplication des activités malveillantes, ce qui entraîne un certain sentiment d'injustice chez les victimes.

Malgré cela, l'action que mènent les Etats pour lutter contre la cybercriminalité a donné lieu à deux avancées majeures: l'une au niveau européen avec la création, en 2013, du Centre européen de lutte contre la cybercriminalité d'Europol (EC3) installé à La Haye[116], l'autre au niveau international avec l'ouverture, en 2014, du Complexe mondial Interpol pour l'innovation installé à Singapour[117].

Pour lutter efficacement contre la cybercriminalité, il faut adopter une démarche de prévention qui rend le cyberespace en tant que moyen de commettre des délits moins attractif et réduise les possibilités de mener des activités criminelles. Par conséquent, il est nécessaire de rendre les cyberattaques plus difficiles à perpétrer, ce qui en accroîtra les coûts en termes de compétences et de ressources, et ainsi réduira le "butin" escompté et augmentera les risques d'identification, d'interpellation et de poursuites pénales pour les criminels. D'une manière générale, la mise en oeuvre de la résilience peut être assurée grâce aux mesures suivantes:

- Réduire le nombre de vulnérabilités techniques, organisationnels, juridiques et humaines.

116 https://www.europol.europa.eu/ec3

117 http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation

- Renforcer la robustesse et la résilience des infrastructures de l'information en appliquant des mesures sur les plans de la technologie, des procédures et de la gestion qui soient cohérentes et complémentaires.
- Instaurer une véritable capacité permettant d'adapter les moyens de cybersécurité et de cyberdéfense à une situation en évolution constante.
- Se doter des moyens de gérer les cybercrises.
- Lutter contre les circuits de monétisation de la cybercriminalité.

Ce nouveau monde que constitue le cyberespace regorge de tous types d'activités. C'est un instrument au service de la rentabilité économique et un lieu d'exercice du pouvoir: c'est en fait un territoire stratégique. A ce titre, il doit être protégé et défendu, tant du point de vue économique que de celui de la sécurité nationale.

Garantir la défense et la sécurité sur tous les plans pour assurer un certain niveau de stabilité

La surveillance des cyberrisque s'inscrit dans un contexte de concurrence économique féroce et constante (de quasi guerre économique), de recherche du profit immédiat, de crise monétaire internationale, d'instabilité généralisée, d'injustice sociale, de risques écologiques et d'une certaine déficience en matière de gouvernance mondiale. La cybersécurité ne devrait pas être envisagée uniquement dans un contexte de réaction au coup par coup visant à "survivre" à un cyberincident, que ce cyberincident ait été prémédité ou qu'il soit accidentel. Bien que cette capacité de résistance soit fondamentale et indispensable, elle ne peut se substituer à une approche globale faisant intervenir de multiples acteurs aux niveaux national et international ou à une véritable compréhension de l'ensemble du phénomène que constituent la cybercriminalité et les cyberconflits. Une approche globale, interdisciplinaire et intégrée de la cybersécurité et de la cyberdéfense permettrait de prendre des mesures adaptées sur le plan à la fois de la prévention et de l'action à mener sur l'instant, mesures dont l'efficacité dépendrait de leur exhaustivité et de leur cohérence d'un point de vue civile autant que militaire. Il serait utopique de penser que nous pouvons résoudre les problèmes liés au cyberespace sans plusieurs niveaux de coopération entre de nombreux acteurs, à la fois à l'intérieur et l'extérieur des frontières nationales, avec pour objectif d'appuyer les stratégies en faveur de la paix dans le cyberespace et dans le monde réel.

Dans certains cas, il sera peut-être nécessaire de repenser la coopération et le dialogue entre forces civiles et militaires, afin d'assurer un ensemble cohérent de protection de la sécurité pour la société au sens large. La cybersécurité ne peut être appréhendée que d'une manière transdisciplinaire et globale. Au niveau national, cela signifie une vision commune et transversale du problème, une coopération renforcée entre les ministères et l'aptitude à travailler ensemble.

Quel que soit le principal objectif d'une cyberattaque, quelle que soit sa cible (une personne, une organisation, un Etat), les outils utilisés sont les mêmes. La nature et l'ampleur des conséquences varient en fonction de la cible et des motivations des attaquants, mais les méthodes et les outils utilisés ne changent pas. Pour un pays, le maintien de la sécurité du public, de la sécurité économique et de la sécurité nationale se situe quelque part entre la sécurité civile et la sécurité militaire, c'est pourquoi il est si important que les stratégies nationales de cybersécurité et de cyberdéfense en tiennent compte, afin d'optimiser l'efficacité et l'efficience des mesures prises et de répondre de la meilleure manière possible aux besoins de la population, en temps de paix comme en temps de guerre. Par ailleurs, à aucun moment la protection des infrastructures essentielles ne pourra être confiée uniquement au secteur privé ou uniquement au secteur public, ce qui justifie également la nécessité de prévoir un ensemble de mesures pour protéger la sécurité.

Il est important de protéger et de défendre à la fois les actifs et le patrimoine numériques des personnes, des organisations et des Etats, ainsi que les infrastructures qui prennent en charge ces actifs et ces fonctions essentielles. Ce point exige des mesures de protection complémentaires, notamment des activités de protection, aux sens civil et militaire du terme, visant à sauvegarder les infrastructures et les actifs qui sont vulnérables face aux cybermenaces.

La mise en place d'une culture de la cybersécurité et d'une cyberdéfense, tout en encourageant le dialogue international sur ces questions devraient contribuer, dans le monde complexe et incertain, dans lequel nous vivons à un certain degré de confiance et de stabilité, à condition que chaque partie prenante se comporte en faisant preuve de bonne foi et d'un sens de la responsabilité collective, sans oublier qu'il est nécessaire de gérer les risques dans les domaines de l'énergie et de l'écologie.

Parmi les risques indirects que créent les sociétés numériques et l'utilisation intensive des systèmes d'information qui ont des répercussions considérables sur notre planète, nous ne devrions pas oublier, en envisageant la cyberrésilience à long terme, de définir des mesures qui garantiront notre durabilité en termes de disponibilité de l'énergie et de préservation des ressources naturelles et de l'environnement écologique pour les générations futures.

Par conséquent, nous devrions nous concentrer en particulier sur les risques liés aux domaines suivants:

- Elimination et recyclage des déchets d'équipements électriques et électroniques.
- Consommation d'énergie (besoins électriques croissants et constants).
- Réchauffement climatique (échappement de chaleur et nécessité de refroidir les ordinateurs et les fermes de serveurs).
- Exploitation des terres et des métaux rares nécessaires pour la fabrication d'équipements électroniques.
- Conséquences environnementales des cyberattaques visant les systèmes de contrôle des sites d'assainissement, la production et la distribution de produits toxiques, les alarmes incendie, etc.

Les activités menées pour assurer la cyberrésilience devraient également répondre aux exigences de protection de l'infrastructure essentielle, surtout en ce qui concerne les éléments vitaux se rapportant à l'énergie et à l'environnement.

D'un point de vue écologique, il nous incombe à tous d'adopter une démarche de prévention pour mieux anticiper les menaces, gérer les cyberrisques, repérer les anomalies pour limiter leurs conséquences et mettre en place la cyberrésilience. Il faut garantir l'éducation et le renforcement des capacités humaines.

Ce sont les personnes formées aux questions de cybersécurité dans plusieurs disciplines des sciences sociales ou techniques qui déterminent les principes théoriques et l'attitude adoptée en matière de cybersécurité, ce qui suppose que les filières de formation correspondantes existent. Sans compétence et sans qualification dans le domaine de la cybersécurité partout dans le monde, sans transfert de connaissances et sans coopération pour renforcer les capacités humaines, il sera difficile de faire adopter des comportements compatibles avec la cyberconfiance. Il est important d'adopter des bonnes pratiques dans le domaine des technologies de l'information et de mener des formations pour sensibiliser au cyberrisques, mais tout cela est insuffisant si le concept de cybersécurité n'est pas intégré dans les produits et les services dès le début phase de conception, si l'appareil judiciaire (police et justice) n'est pas en mesure de remplir sa fonction faute de compétences ou si les acteurs politiques et économiques, de même que tous les internautes, des plus jeunes ou plus âgés, n'ont pas les compétences, les connaissances et l'expérience nécessaires. Il ne suffit pas de sensibiliser la population aux dangers inhérents à l'Internet et aux précautions élémentaires à prendre ou de les rendre seuls responsables d'une situation qui, dans la grande majorité des cas, les dépassent complètement. Dans la pratique, il serait injuste de demander à l'utilisateur final et au citoyen de supporter le coût des risques que ceux qui les ont créés n'ont pas été capables d'éliminer et, partant, de rejeter un problème de société sur des personnes qui n'ont pas le savoir-faire ou les moyens nécessaires pour trouver une solution.

La cyberrésilience, un nouveau défi dans le cadre de la cybersécurité

La résilience face à la criminalité fait partie intégrante d'une vision globale de la cybersécurité et contribue à instaurer la cyberconfiance. Il est aujourd'hui urgent d'accroître la robustesse et la résilience de nos infrastructures en prenant les mesures technologiques, judiciaires, organisationnels et de procédure appropriées. Comme pour toutes les activités liées à la sécurité, la lutte contre la cybercriminalité, les cyberabus et les cyberutilisations abusives est une tâche compliquée. Ce combat doit s'inscrire dans une perspective de protection des personnes et des actifs tangibles et intangibles, et de défense de valeurs démocratiques communes largement acceptées. Il est par conséquent utile d'être en mesure d'adopter une approche efficace et concrète en matière de cybersécurité et de cyberrésilience.

Pour éviter que la société de l'information devienne synonyme de méfiance et de surveillance, il est nécessaire d'apporter des réponses crédibles à la nécessité d'instaurer la confiance et la résilience dans le cyberespace et de proposer des solutions pratiques pour protéger les actifs et les infrastructures numériques. Toute tentative d'aller à l'encontre de cela dans le cyberespace exigera des politiques volontaristes aux niveaux national et international, des ressources et des compétences, des structures et des procédures organisationnelles et une coordination adaptée. Tant en ce qui concerne les acteurs légitimes que les acteurs douteux, le nouveau facteur de stabilité des sociétés fait partie de la sécurité de ces sociétés et dépend de leur aptitude à contrôler les cyberrisques et à maintenir les cybernuisances à des niveaux acceptables. La cybersécurité ne devrait pas être un instrument de domination et d'exercice du pouvoir pour les Etats, mais un instrument de stabilité et de promotion de la paix[118].

Chapitre III: Cyberliberté

Introduction

Alors que le chapitre précédent souligne l'importance cruciale de la cyberrésilience en vue d'instaurer la confiance dans le cyberespace, ce dernier chapitre présente une vue d'ensemble des défis liés à la cyberliberté et des nouvelles menaces qui en découlent, menaces qui proviennent à la fois des secteurs public et privé et qui remettent en cause l'espoir d'un Internet libre.

La liberté d'opinion et de discours, le libre accès à l'information et le droit à la confidentialité ont toujours joué un rôle central dans la société civile, car ils constituent des droits humains et des libertés civiles essentiels à l'appui des principes et des valeurs démocratiques. Le développement de l'Internet et des technologies de l'information et de la communication a offert la possibilité à des milliards de personnes partout dans le monde d'accéder à des quantités d'informations et à des moyens de communication jusque-là inimaginables. Toutefois, ces outils essentiels de l'ère du numérique, s'il est vrai qu'ils représentent de vastes plates-formes pour l'échange de vues, de données et d'idées innovantes, sont aussi exploités pour porter atteinte au progrès, aux droits politiques et à la confidentialité, ce qui nuit à la confiance dans leur utilisation.

Comme la Cour européenne des droits de l'homme l'a souligné à plusieurs reprises, "la liberté d'expression s'applique non seulement aux "informations" ou aux "idées"

---

118 Assurer la cyberconfiance à l'échelle mondiale contribuera à résoudre les principaux problèmes qui empêchent de parvenir à la cybersanté, comme ceux présentés dans "En quête de la cybersanté", UIT 2011 (http://www.itu.int/pub/S-GEN-WFS.01-1-2011)

accueillies favorablement ou considérées comme inoffensives ou indifférentes, mais aussi à celles qui heurtent, choquent et troublent l'Etat ou une partie de la population"[119].

Si les blogs et les médias sociaux ont ouvert de nouvelles voies pour l'échange d'idées, certains Etats ont recours depuis quelques années au blocage de l'Internet pour étendre leur censure qui vise à contrôler l'opinion publique et à entraver la liberté d'information et d'expression.

Cette censure remet en cause les avantages de l'Internet, à savoir sa capacité de propagation illimitée et son accessibilité partout dans le monde, et s'inscrit dans le cadre du débat actuel sur la neutralité des réseaux, principe visant à garantir l'égalité des droits en ce qui concerne l'accès à ce média essentiel de notre époque.

Les quantités massives de données hautement disponibles caractérisent la société de l'information actuelle et renforcent les menaces d'espionnage provenant à la fois des secteurs public et privé, ce qui met en péril le droit à la confidentialité et la sûreté d'utilisation des outils numériques. Le fait est que la surveillance mise en place à juste titre par les gouvernements pour garantir la sécurité nationale peut rapidement conduire à la collecte de données et au stockage d'informations personnelles en masse, si bien qu'il est difficile de faire une distinction entre les pratiques acceptables et les pratiques inacceptables qui donnent l'impression de franchir une ligne rouge.

Parallèlement, pour bénéficier du régime de protection des données le plus commode possible, dans le souci de se procurer un avantage financier et concurrentiel, le secteur privé collecte et transfère de grandes quantités de données personnelles par-delà les frontières, ce qui crée des risques supplémentaires pour les données personnelles.

Etant donné que l'Internet est par essence sans frontières, les législations nationales ne peuvent garantir à elles seules la liberté de l'Internet. C'est pourquoi il est essentiel d'élaborer et d'adopter un cadre pour l'instauration de la cyberconfiance.

Le présent chapitre est divisé en cinq sections. Pour commencer, il met en évidence l'absence d'un cadre juridique approprié concernant la protection des libertés civiles dans le cyberespace et de la liberté de l'Internet, comme le montre la situation actuelle dans de nombreuses parties du monde arabe. Ensuite, il met l'accent sur le débat relatif aux mégadonnées et sur le problème de la protection des données, afin de souligner la nécessité d'un cadre réglementaire international pour préserver la liberté de l'Internet et le droit à la confidentialité. La troisième section traite de la surveillance étatique et de la collecte de renseignements dans le cyberespace et de leurs incidences sur l'instauration de la cyberconfiance.

---

119 Cour européenne des droits de l'homme; affaire Handyside c. Royaume-Uni http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["695376"],"itemid":["001-57499"]} (dernière consultation le 17/10/2014).

La quatrième session aborde le problème de la violation de l'intimité numérique et de la protection des données par les gouvernements dans une perspective européenne, et s'intéresse à l'importance de la mise en place d'une politique harmonisée en la matière à l'échelle de l'Union européenne, non seulement pour faciliter la coopération entre ses Etats membres, mais aussi pour servir de modèle au-delà de ses frontières. Enfin, la dernière section vise à établir des critères de gestion de la cyberliberté en tant que droit humain fondamental et que puissant moteur de la cyberconfiance.

3.1 Cyberliberté: Progrès et défis

Par Mona Al-Achkar

Introduction

La puissance des nouvelles technologies a marqué l'entrée dans une ère où l'on s'affranchit de plus en plus des contraintes techniques limitant le champ des possibles à de nombreux niveaux, une ère du numérique dans lequel individus et Etats nations sont dotés d'un pouvoir sans précédent non seulement de se développer, mais aussi de planifier des actes d'abus et de violence majeurs.

Ce paradoxe se reflète dans l'opposition entre les avantages incontestables de l'ère du numérique et les nombreux dangers auxquels sont confrontés les personnes, le monde des affaires et les Etats nations, dangers qui résultent de l'utilisation grandissante des TIC et du développement des activités criminelles, toujours plus sophistiquées, dans le cyberespace. Les menaces à l'encontre de la sécurité nationale se sont aggravées, et les infrastructures critiques sont de plus en plus exposées à des risques multiples, notamment aux attaques à partir de l'Internet.

Avec la cybercriminalité, l'incompatibilité et l'absence ou l'insuffisance d'un cadre juridique restent les principaux facteurs qui nuisent à la confiance dans l'utilisation des plates-formes du cyberespace, car elles permettent l'installation d'une insécurité juridique et entravent le plein exercice des libertés civiles. Inversement, la surveillance de l'Internet représente une réelle menace pour de nombreuses libertés civiles, telles que le respect de la vie privée, la liberté d'expression, la protection contre l'auto-incrimination, les perquisitions et saisies injustifiées, et le droit à l'application régulière de la loi. Le niveau de protection de ces libertés civiles dépend largement de la législation, des pratiques juridiques et du système politique en vigueur dans un pays ou une région donnée.

Pour garantir un cyberenvironnement économique digne de confiance, il est indispensable de protéger ces libertés civiles et d'instaurer ainsi la confiance dans le cyberespace. C'est ce qu'illustre clairement l'affaire PRISM, qui a révélé que l'Agence de la sécurité nationale des Etats-Unis (NSA) avait collecté des données personnelles et mené des opérations d'espionnage de façon clandestine. À la suite de ces révélations, Cisco avait annoncé une baisse de 8% à 10% de ses recettes, et avait prévu une

diminution supplémentaire de ses activités et de ses revenus pour 2013-2014, en raison de la situation économique mondiale mais aussi des conséquences du scandale de l'affaire PRISM.

Cette surveillance de masse, qui donne lieu à l'apparition de concepts tels que ceux de "cyberrépression" et d'"Etat policier électronique", tend à signaler le déclin de bon nombre des libertés civiles citées précédemment, aussi bien dans les régimes dictatoriaux que dans les pays démocratiques.

Libertés civiles

Le terme "libertés civiles" vient du latin *ius civis* qui signifie "droit des citoyens" et tire sa source de la *Magna Carta* destinée à limiter les abus de pouvoir des autorités. C'est pourquoi les libertés civiles sont tenues pour une protection contre les pratiques et les actions illégales des gouvernements et la violation par ces derniers des droits juridiques fondamentaux.

Alors que les droits humains sont universels et s'appliquent dans une mesure égale à tous les pays, les libertés civiles relèvent de la législation nationale de chaque pays. Par conséquent, chaque pays octroie à ses citoyens les libertés fondamentales qui leur reviennent en vertu de son système juridique national. La caractéristique la plus importante des libertés civiles réside dans le fait qu'elles limitent les intrusions de l'Etat dans la vie des citoyens, ainsi que toutes les formes d'abus de pouvoir, et qu'elles garantissent par conséquent la capacité des citoyens à participer à la vie civile et politique de leur pays sans subir de discrimination ou de répression.

Les libertés civiles comprennent des droits personnels, politiques et économiques, tels que: le droit à un procès équitable, le droit à l'application régulière de la loi, la liberté d'association, le droit à la pétition, le droit d'auto-défense, le droit de vote, la protection contre l'esclavage et le travail forcé, la protection contre la torture et la mort, le droit à la liberté et à la sécurité, la liberté de conscience, la liberté de religion, la liberté d'expression, la liberté de parole, le droit à la vie privée, le droit de propriété, le droit au mariage, le droit de se défendre, le droit à l'intégrité physique, le droit d'utiliser des équipements, le droit à une éducation égalitaire et le droit d'exercer une fonction publique.

Les libertés civiles inscrites dans la législation nationale peuvent avoir une base juridique commune, telle que le délit d'infraction aux libertés civiles, qui permet aux particuliers de demander réparation – non seulement vis-à-vis d'autres particuliers, mais aussi vis-à-vis de l'Etat – lorsqu'ils ont subi des torts ou des dommages corporels du fait d'une violation de leurs droits fondamentaux. Ces infractions peuvent concerner, par exemple, l'intrusion injustifiée dans le domicile ou la vie privée d'une personne, la diffamation ou l'appropriation illicite.

Liberté de l'information: le droit d'accès à l'information

La liberté de l'information ou le droit d'accès à l'information a fait son apparition en tant que nouveau droit, distinct mais indissociable de la liberté d'expression. On peut le définir comme le droit d'accès aux informations détenues par les organismes publics[120].

D'après le document final établi par une réunion d'experts organisée par le Secrétariat du Commonwealth, dans lequel il est tenu compte de l'Article 19 de la Déclaration universelle des droits de l'homme: "La liberté de l'information doit être garantie en tant que droit légal susceptible d'exécution permettant à tout individu d'obtenir des documents et des informations détenues par les branches exécutive, législative et juridique de l'Etat, ainsi que par toute entreprise publique et tout autre organisme remplissant des fonctions publiques."

Le principe fondamental qui sous-tend cette liberté réside dans le droit des citoyens de savoir, l'obligation des gouvernements d'informer leurs citoyens et le fait que la charge de la preuve incombe à la partie qui reçoit la demande d'informations. C'est pourquoi la plupart des gouvernements ont tendance à classer secrètes les informations qu'ils ne souhaitent pas divulguer ou à ne pas les publier pour raisons d'Etat.

Le droit d'accès à l'information inclut le droit de chercher, de recevoir et de transmettre des informations et des idées, et vaut autant pour les personnes qui cherchent activement des informations que pour celles qui attendent d'en recevoir par l'intermédiaire des médias ou des voies officielles. Ce droit concerne principalement l'accès aux informations publiques. Il met l'accent sur le principe de la publicité des actes, ainsi que la transparence de l'administration publique, ce qui établit un lien direct entre son application et la participation active des citoyens à la vie politique et aux mécanismes de lutte contre la corruption.

Conformément à la Résolution 59 (1) de l'Assemblée générale des Nations Unies: "La liberté de l'information est un droit fondamental de l'homme […], la pierre de touche de toutes les libertés à la défense desquelles se consacrent les Nations Unies"[121]. De manière analogue, comme il est dit dans le préambule des Principes de Lima ou dans la Déclaration de Chapultepec: "[…] Les droits individuels à la liberté d'expression et à l'accès à l'information sont indispensables à l'existence même de toute société démocratique et essentiels au progrès, au bien-être et à la jouissance de tous les autres droits humains"[122].

---

120 http://www.unesco.org/new/fr/communication-and-information/freedom-of-expression/freedom-of-information/.

121 Assemblée générale des Nations Unies (1946) Résolution 59 (1), 65eme séance plénière: http://foishehri.wordpress.com.

122 http://www.rjionline.org/MAS-Codes-Peru-Lima-Principles.

Par ailleurs, dans l'Engagement de Tunis, le Sommet mondial sur la société de l'information a réaffirmé la nécessité pour les Etats nations de respecter les droits humains et les libertés fondamentales, et a reconnu "[…] l'importance de la liberté d'expression et de la libre circulation des informations, des idées et du savoir pour la société de l'information"[123].

Par conséquent, le droit d'accès à l'information est considéré comme essentiel, entre autres, à l'exercice de la liberté d'expression et de la liberté d'opinion. Il suppose l'obligation pour les gouvernements de garantir la libre circulation des informations et des idées. En 1995, Abid Hussain, alors Rapporteur spécial des Nations Unies sur la liberté d'expression et d'opinion, a affirmé dans son rapport à la Commission des droits de l'homme des Nations Unies: "La liberté perdra toute réalité si la population ne peut pas accéder à l'information. L'accès à celle-ci fait partie de la vie démocratique. La tendance à dissimuler des informations au grand public doit donc être fermement réprimée".

Le niveau de la liberté d'accès à l'information varie d'un pays à l'autre. Certains faits récents en ce domaine méritent particulièrement d'être relevés. Par exemple, l'une des conséquences du récent printemps arabe a été l'inclusion dans la constitution[124] de certains pays arabes d'une disposition garantissant le droit à l'information[125]. A l'inverse, les citoyens des Etats-Unis ont plus de difficultés à accéder aux informations détenues par leur gouvernement depuis l'adoption du *Patriot Act*.

S'il est demandé aux Etats nations de reconnaître et de respecter le droit à l'information, il convient de signaler que celui-ci fait souvent l'objet de restrictions de la part des autorités, dès lors que celles-ci estiment qu'il entrave ou compromet la sécurité nationale, l'intégrité territoriale, la sécurité publique, la prévention de la criminalité, la protection de la santé et des moeurs, et le respect de la vie privée, de la réputation ou des droits d'autrui. Toutefois, ces restrictions doivent être conformes à la loi et répondre aux critères d'impartialité juridique et de bon fonctionnement démocratique.

Dans le cyberespace, le droit à l'information offre aux particuliers et aux organisations la possibilité d'atteindre un plus haut degré de liberté d'expression et d'échange social. Parallèlement, il pose un ensemble de nouveaux défis qui peuvent restreindre l'utilisation des médias sociaux. Le printemps arabe et les documents dérobés par WikiLeaks en sont les exemples les plus récents. Ces cas, outre les problèmes qu'ils posent pour les intérêts nationaux et le secret des données classifiées, mettent en

---

123 https://www.itu.int/wsis/docs2/tunis/off/7-fr.pdf.

124 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f.

125 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f.

évidence les restrictions et les pratiques policières auxquelles gouvernements et entités du secteur privé ont recours sur l'Internet.

Comme suite à l'engagement pris par le G8 en 2004 de promouvoir un environnement propice à un dialogue informel, souple, ouvert et inclusif, les pays du Moyen-Orient et de l'Afrique du Nord ont lancé la même année une initiative appelée *Forum for the future*. Par la suite, en juillet 2008, des organisations arabes de la société civile issues de Bahreïn, d'Egypte, de Jordanie et du Maroc ont créé le Réseau arabe pour la liberté de l'information. Toutefois, en dépit des activités de sensibilisation concertées menées dans la région, la législation relative à la liberté de l'information n'a pas évolué dans la plupart des pays arabes. La Jordanie et la Tunisie demeurent les seuls Etats arabes à avoir adopté une loi sur la liberté de l'information, bien que des projets de loi sur ce sujet aient été débattus à Bahreïn, en Egypte, au Koweït, au Liban, au Maroc, en Palestine et au Yémen. En 2004, au Liban, un groupe de juristes libanais a élaboré un projet de loi sur la protection des dénonciateurs d'irrégularités, avec l'aide de l'*American Bar Association*. Ce projet a été soumis au parlement libanais en 2010 par le Réseau national pour le droit d'accès à l'information au Liban.

Vie privée: protection contre la communauté mondiale du renseignement

La vie privée est une liberté civile relative aux libertés personnelles, à la dignité et à l'intégrité. Elle consiste dans le droit des citoyens à une protection contre toute intrusion injustifiée de l'Etat dans leur vie, comme des fouilles non autorisées de leur domicile et l'espionnage de leurs communications ou de leur correspondance. A l'ère du numérique, la vie privée est envisagée dans un nouveau contexte. Elle ne se limite plus désormais à la protection de l'environnement physique et matériel, comme le domicile, le courrier ou les documents, mais s'applique également à l'énorme volume de données personnelles présentes dans le cyberespace, ainsi qu'au haut niveau de connectivité qui fait de chaque personne un "capteur de la communauté mondiale du renseignement"[126].

Il n'existe pas de consensus mondial concernant ce qui peut être considéré comme une protection suffisante de la vie privée. Néanmoins, il existe un cadre juridique international fondamental pour le droit à la vie privée, qu'il est possible d'étendre au cyberespace, et qui reflète les dispositions des législations, déclarations, conventions et traités internationaux, régionaux et nationaux.

En vertu de l'Article 12 de la Déclaration universelle des droits de l'homme, la vie privée est reconnue comme un droit humain fondamental. Aux termes de cette déclaration,

---

126 Philippe Langlois, fondateur de la société Priority One Security, basée à Paris, à propos de la capacité des agences à collecter les données personnelles des utilisateurs de smartphones. http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0.

nul ne doit être l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, et toute personne a droit à la protection de la loi à cet égard.

L'Article 17 du Pacte international relatif aux droits civils et politiques dispose que: "Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation et que, en conséquence, toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes."

Parmi les lignes directrices, conventions et directives pertinentes, on peut citer:

- Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, publiées en 1980 par l'Organisation de coopération et de développement économique.
- La *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, publiée en 1981 par le Conseil de l'Europe.
- Les *Lignes directrices sur l'utilisation des flux de données personnelles informatisées*, publiées en 1989 par le Conseil de l'Europe.
- Les *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel*, publiés en 1999 par les Nations Unies.

Ces instruments établissent des principes garantissant une protection minimale de la confidentialité des informations personnelles à toutes les étapes de leur traitement (collecte, stockage, diffusion, utilisation, transfert, etc.). Ils reconnaissent également le droit des personnes à accéder à leurs données personnelles, à les mettre à jour et à être informées des méthodes et des objectifs des opérations de collecte de données. En outre, ils établissent le droit des personnes à faire détruire leurs données une fois que le but de leur collecte et de leur traitement a été atteint, ce qui va dans le sens du droit à l'oubli sur l'Internet. Au niveau régional, certains pays ont déjà fixé des mesures et des niveaux minimaux de protection en ce qui concerne les questions de confidentialité.

La directive de 1995 de l'Union européenne (UE) sur la protection des données autorise la collecte de données personnelles à des fins précises, explicites et légitimes, et interdit la détention de données qui ne seraient pas à jour, pertinentes et exactes. Par ailleurs, les Etats membres de l'UE sont tenus d'empêcher le transfert de ces données à

l'étranger[127] en l'absence de mesures équivalentes garantissant la protection des données et le droit des citoyens à accéder à leurs données, à les protéger et à les modifier, et à refuser à une tierce partie le droit d'utiliser leurs données.

Par exemple, pour autoriser les flux transfrontières de données vers les Etats-Unis, où cette obligation de respecter un certain niveau de protection n'existe pas, l'UE a conclu avec ce pays l'accord "Sphère de sécurité" (*Safe Harbor*), qui autorise certaines entreprises américaines à collecter des données concernant des citoyens de l'UE, à condition qu'elles prouvent leur engagement à garantir la protection de ces données conformément aux normes de l'UE. De plus, ces entreprises sont tenues d'informer les citoyens de l'UE concernés des modalités de traitement et d'utilisation de leurs données, et de reconnaître le droit de ces derniers à accéder à leurs données, à ne pas les divulguer et à les modifier.

Au niveau régional, la Directive de l'UE sur la protection des données réglemente la libre circulation des données personnelles entre ses Etats membres, et impose l'adoption de dispositions dans les législations nationales, tout en autorisant chaque pays de l'UE à fixer lui-même les modalités de mise en oeuvre. Les personnes doivent bénéficier du droit de connaître l'origine des données, de faire corriger des données inexactes, de faire appel en cas de traitement illicite des données, et de refuser la permission d'utiliser leurs données dans certaines circonstances.

Au niveau national, presque tous les pays reconnaissent un droit constitutionnel à la vie privée. Quelques nouvelles constitutions (Afrique du Sud) et de nombreux pays européens ont adopté des lois visant à réglementer la surveillance des données personnelles et à protéger la vie privée des citoyens[128]. Les Nations Unies se sont exprimées en faveur de la protection de la vie privée en approuvant un projet de

---

127 Directive 95/46/EC du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *Journal officiel L 281, 23/11/1995 P. 0031 – 0050* - (57) en revanche, lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit;

128 FISA Amendments Act (2008), Communications Assistance for Law Enforcement Act, au Etats-Unis - Data Protection Act (1998) et Regulation of Investigatory Powers Act (RIPA) au Royaume-Uni- Loi informatique et libertés (1978) en France - Convention de l'UE pour la protection des données à caractère personnel, Directive de l'UE sur la conservation des données.

Résolution[129] élaboré par le Brésil et l'Allemagne, intitulé "Le droit à la vie privée à l'ère du numérique[130]".

Liberté d'expression: la marque distinctive des sociétés démocratiques

Dans les sociétés démocratiques, la législation, la liberté de parole et l'indépendance de la société civile sont les garants de la liberté et des libertés civiles, à l'opposé des traits caractéristiques des régimes tyranniques, tels que l'impunité de la police, les procès inéquitables et les détentions arbitraires.

En vertu de l'Article 19 de la Déclaration universelle des droits de l'homme, ainsi que de l'Article 19 du Pacte international relatifs aux droits civils et politiques: "Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit." La liberté d'expression désigne la capacité d'exprimer librement des idées et des opinions sur des sujets économiques, politiques, sociaux et autres, à l'aide de tous les moyens de communication existants – par exemple l'écriture, la peinture, la radiodiffusion ou les blogs. En conséquence, la liberté de la presse et la liberté d'utiliser les médias sociaux relèvent de la liberté d'expression.

De manière analogue, l'Article 11 de la Charte des droits fondamentaux de l'Union européenne, correspondant à l'Article 10 de la Convention européenne des droits de l'homme, dispose que: "Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière." Il stipule en outre que: "L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire." Par ailleurs, comme pour toutes les restrictions de droits et de libertés, il reconnaît les principes de nécessité et de proportionnalité, ainsi que la nécessité d'empêcher les pratiques arbitraires et discriminatoires.

---

129 L'Assemblée générale s'exprime en faveur du droit à la vie privée à l'ère du numérique. http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

130 Soixante-neuvième session – Troisième Commission – Point 69 b) de l'ordre du jour: Questions relatives aux droits de l'homme, y compris les divers moyens de mieux assurer l'exercice effectif des droits de l'homme et des libertés fondamentales.

Par conséquent, la liberté d'expression est considérée comme essentielle à la confiance des citoyens dans leur gouvernement et dans le système politique, car elle permet l'application d'autres droits humains, une meilleure compréhension des politiques publiques, la création d'une opinion publique éclairée, et la liberté de faire part de ses préoccupations au moyen des médias. Au niveau national, la liberté d'expression est reconnue dans de nombreuses constitutions comme une marque distinctive des régimes démocratiques. Dans ce contexte, l'Assemblée générale des Nations Unies considère que la surveillance des réseaux de télécommunication menace les droits humains et les libertés civiles, de la liberté d'opinion et d'expression au droit à la vie privée et à l'activisme politique, et qu'elle remet en cause les fondements de la société démocratique[131].

La liberté d'expression en ligne doit donc être respectée et les gouvernements doivent éviter de l'étouffer et supprimer tous les obstacles qui s'y opposent. En particulier, s'agissant du propos de notre exposé, ils sont tenus de ne pas recourir à la cyberrépression pour faire taire les voix d'opposition, et d'éviter d'intercepter des communications, de censurer des contenus et de bloquer des sites web.

Cependant, dans les faits, de nombreux pays ne respectent pas la liberté d'expression. Certains d'entre eux évoquent la protection des valeurs religieuses et de la décence, outre la sécurité nationale et la lutte contre le terrorisme, pour justifier les restrictions de la liberté d'expression en ligne. Ils censurent des contenus qu'ils considèrent comme sexuellement explicites ou qui incitent à la haine sur la base de considérations raciales, religieuses ou d'autres facteurs culturels, ou qui encouragent les activités terroristes. Le danger réside dans la terminologie juridique utilisée pour réprimer ces contenus, qui est généralement extensible et qui peut donc manquer d'objectivité et nuire à la stabilité de la justice, et par conséquent conduire à des abus d'autorités.

Médias sociaux

Les discussions, les échanges de vues et de but communs, ainsi que les groupes de pression, sont traditionnellement les étapes préliminaires à l'organisation de protestations pouvant conduire à une révolution. L'abondance d'échanges sur les médias sociaux concernant la liberté de l'Internet et la démocratie, associée à la capacité grandissante des citoyens à influer sur la vie politique nationale, a joué un rôle essentiel dans le développement du débat politique lors du printemps arabe. Les

131 Assemblée générale des Nations Unies- 16 mai 2011 A/HRC/17/27- Conseil des droits de l'homme – Dix-septième session – Point 3 de l'ordre du jour - Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement. "L'utilisation de plus en plus courante et évoluée de la surveillance numérique a privé les sociétés de l'aptitude à décider de leur propre usage dans un cadre législatif, ce qui conduit à "des pratiques au coup par coup échappant à la supervision de toute autorité indépendante" et menace de réprimer la liberté d'expression."

citoyens ont pu ainsi disposer d'un nouvel espace d'expression, à l'aide des publications sur les blogs, des tweets et des téléchargements sur YouTube. Selon un activiste égyptien: "L'Internet mérite la plus haute protection contre les intrusions de l'Etat. Si vous voulez libérer les peuples, donnez-leur l'Internet".

Les médias sociaux créent une capacité sans précédent de mobilisation des personnes et d'échange d'informations clandestines. Ils offrent de grandes possibilités en matière d'organisation et de diffusion des informations, et peuvent aider à créer et structurer des groupes d'opposition, recruter des militants, attirer des partisans, diffuser des idéologies et constituer des réseaux de soutien internes et externes. Pendant le printemps arabe, les militants ont utilisé les médias sociaux pour obtenir un soutien régional et international et pour organiser des campagnes de propagande.

Même si les médias sociaux ne peuvent pas remplacer les actions concrètes nécessaires pour organiser avec succès une révolution, ils ont fourni aux citoyens arabes un moyen d'utiliser l'information comme une arme contre la répression. Les participants aux mouvements du printemps arabe se sont servis des médias sociaux pour rester en contact, partager des informations, diffuser des nouvelles concernant les événements récents, organiser leurs activités, diffuser des informations et des nouvelles, envoyer des messages au monde et influencer l'opinion publique. Les images et les vidéos envoyés à l'aide des téléphones mobiles ont permis de recueillir des informations concernant les forces gouvernementales et leur position. Les actions politiques ont été organisées essentiellement sur les réseaux sociaux. Avant et pendant les changements de régime survenus dans plusieurs pays arabes à la faveur du printemps arabe, des tweets des groupes d'opposition se sont propagés de manière virale et ont atteint des millions d'utilisateurs. Le nombre de pages Facebook et de blogs a très fortement augmenté, ce qui a engendré dans toute la région des discussions sur la démocratie, la liberté et la transparence. Des millions de citoyens étaient sur les médias sociaux, et de nombreuses pages et sites ont été créés pour étendre la portée de l'opposition à l'aide de messages en ligne et de blogs. Des activistes ont filmé et publié sur Facebook des séquences en temps réel des événements au moyen de leur téléphone mobile. Aujourd'hui, nombre des slogans de cette période sont fréquemment repris dans différents pays lors de diverses protestations sociales, politiques ou économiques.

Au cours des douze derniers mois, des attaques inquiétantes contre la liberté d'expression ont eu lieu au Liban. La réputation du pays comme étant un bastion de la liberté de parole a été ternie par une série d'arrestations, de détentions et d'intimidations de citoyens libanais en raison de leurs activités en ligne, en particulier sur les médias sociaux.

Les personnalités politiques libanaises semblent adopter une attitude de plus en plus défensive, ouvertement mis en cause dans des tweets de 140 caractères ou d'autres contenus diffusés sur les médias sociaux. Par exemple, quatre utilisateurs de Facebook ont été arrêtés et un utilisateur de Twitter condamné à deux mois d'emprisonnement

pour avoir insulté le Président de la République. Dans une autre affaire, un blogueur placé en détention pendant plus de huit heures a été menacé de poursuites s'il persistait à signer des écrits politiques au lieu de se limiter à la poésie. Les autorités responsables de la cybercriminalité ont interrogé plusieurs blogueurs et bloqué certains blogs, notamment en raison d'une publication concernant le traitement inéquitable des employés d'une grande chaîne de supermarchés.

Ces décisions, qui s'apparentent aux sanctions prises dans les pays autocratiques, sont inhabituelles pour le Liban, où l'expression des opinions a été relativement peu régulée dans le passé.

Dangers: Faits et acteurs

Le cyberespace constitue une nouvelle dimension de la sécurité nationale et représente une précieuse mine d'informations pour la collecte de renseignements. Cependant, les moyens traditionnellement utilisés par les entités s'occupant de sécurité pour surveiller et collecter les informations ne sont plus suffisants.

De nos jours, il est nécessaire de repérer et de cibler les auteurs de complot et d'anticiper les actions des réseaux susceptibles d'être malveillants ou criminels. Cet objectif donne lieu au déploiement de technologies sophistiquées afin d'assurer une surveillance de masse des réseaux informatiques et des utilisateurs, de façon à détecter, identifier et suivre les intrus, et à préserver les données liées à des faits concrets.

La collecte de données personnelles et les violations des libertés civiles qu'elle entraîne font les gros titres des médias dans le monde entier; les affaires Snowden, WikiLeaks et Tempora[132], entre autres, ont conduit à un resserrement de l'étau autour de l'Internet, notamment par l'intermédiaire des lois SORM-2 et SORM-3[133], du "registre unique[134]"

---

132 Tempora est un système de surveillance électronique clandestin testé à partir de 2008[2] et mis en service en 2011, administré par le Government Communications Headquarters du Royaume-Uni (GCHQ). Tempora effectue des interceptions sur les câbles à fibre optique, qui constituent l'épine dorsale de l'Internet, afin d'accéder à de grandes quantités de données personnelles d'utilisateurs. http://fr.wikipedia.org/wiki/Tempora.

133 Ces lois semblent être en conflit avec l'article 23 de la Constitution de Russie, qui dispose que:[32]

1) Chacun a droit à l'inviolabilité de la vie privée, au secret personnel et familial, à la défense de son honneur et de sa réputation.
2) Chacun a droit au secret de la correspondance, des entretiens téléphoniques, des communications postales, télégraphiques et autres. La limitation de ce droit n'est permise que sur la base d'une décision judiciaire.

134 In Ex-Soviet States, Russian Spy Tech Still Watches You- Andrei Soldatov and Irina Borogan- 12.21.12 6:30 AM. http://www.wired.com/dangerroom/2012/12/russias-hand/all/

et de la censure des réseaux sociaux[135]. Récemment, certains pays ont renforcé les contrôles sur l'Internet par le biais de mesures visant à garantir l'identification des utilisateurs en ligne[136].

Les agences de sécurité peuvent intercepter des données personnelles et les comparer avec des listes de cibles des services de renseignement. Les technologies de surveillance leur permettent de localiser les cibles avec précision au moyen de Google Maps ou de systèmes GPS de suivi des déplacements, ou d'éléments intégrés dans les photos publiés sur les réseaux sociaux. Par le biais de ces technologies, elles peuvent aussi obtenir les adresses et relevés téléphoniques de parents et d'amis en enregistrant et en stockant des courriels. D'après des documents émanant des services de renseignements britanniques, les espions se tiennent même à l'affut sur les applications de jeux populaires pour obtenir des données concernant la position géographique, l'âge, le sexe et d'autres informations personnelles des joueurs.

Ce phénomène fragilise considérablement la vie privée ainsi que de nombreuses libertés civiles. Cependant, les gouvernements ne sont pas les seuls à se rendre responsables de violations de la vie privée et d'autres libertés civiles. En effet, la surveillance illégale de particuliers est le fait tant d'entités privées que d'entités publiques, étant donné qu'elle peut être utile à des fins de marketing et de collecte de renseignements. Les grandes comme les petites entreprises suivent nos achats, compilent nos données personnelles pour nous envoyer des publicités sur nos téléphones mobiles, collectent et analysent nos données et les utilisent à des fins commerciales. Parfois, elles collectent des données particulièrement délicates, qu'ils qualifient d'optionnelles, et qui ont trait, entre autres, à l'origine ethnique et à l'orientation sexuelle.

La censure étatique s'exerce par le biais de mesures telles que le filtrage de l'Internet, le déploiement d'outils malveillants comme les chevaux de Troie[137], et la restriction de l'anonymat en ligne. Ces mesures visent à faciliter la surveillance des communications par l'Etat, en simplifiant l'identification des personnes qui consultent ou diffusent des contenus interdits, ainsi qu'à collecter des renseignements.

---

135 King, Gary, Jennifer Pan et Margaret Roberts. 2014. Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation. Disponible à l'adresse suivante:

http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

136 En Chine, les utilisateurs sont tenus de fournir leur véritable identité pour télécharger des vidéos en amont. http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121

137 L'application QQ, en Chine, est considérée comme un cheval de Troie.

L'ampleur des données collectées et des communications enregistrées est tout à fait considérable – et déconcertante – et met sérieusement en péril la vie privée et les libertés civiles.

Toutefois, cette surveillance présente certains aspects positifs évidents. Elle a permis, par exemple, de déjouer un attentat à la bombe d'Al-Qaïda en Allemagne en 2007, et d'arrêter les responsables de réseaux de drogues[138] et de pornographie infantile[139]. Dans ce contexte, nous pouvons également mentionner le projet européen INDECT – système d'information intelligent soutenant l'observation, la recherche et la détection pour la sécurité des citoyens en milieu urbain – qui vise à garantir la sécurité des citoyens, principalement contre la violence.

Gros plan sur le monde arabe[140]

La plupart des pays arabes sont membres des Nations Unies, et tous font partie de la Ligue des Etats arabes, qui se compose d'Etats arabes indépendants d'Afrique du Nord et du Nord-Est et d'Asie du Sud-Ouest. L'objet de la Ligue arabe est de renforcer les relations entre ses Etats membres, d'encourager la coopération entre eux, et de préserver leur indépendance et leur souveraineté. Plus précisément, elle vise à garantir une coopération étroite sur les plans économique et financier, en matière de communications et de santé, dans les domaines social et culturel, ainsi que pour ce qui est des questions relatives à la nationalité, aux passeports, aux visas, à l'exécution des décisions judiciaires et à l'extradition des criminels.

Les pays arabes s'engagent à respecter la liberté d'expression, en vertu de l'Article 19 de la Déclaration universelle des droits de l'homme, ainsi que de l'Article 32 de la Charte arabe des droits de l'homme, inspiré dudit Article 19.

Les moeurs et traditions sociales, ainsi que la religion, sont généralement les raisons avancées pour justifier les restrictions et la répression. Certains pays ont adopté des lois d'urgence, qui ont toujours pour but de mettre sous l'éteignoir les opinions dissidentes, en poursuivant ceux qui osent dire librement ce qu'ils pensent. Ces derniers peuvent être victimes d'arrestations brutales et de tortures, et mis en prison pour avoir commis le crime d'appartenir à une "organisation illégale", pour trahison, ou pour avoir

---

138 Drug lord Guzman arrested. http://news.yahoo.com/internet-crucial-venezuela-battleground-075124059.html

139 How the NSA's High-Tech Surveillance Helped Europe Catch Terrorists.

http://www.civilbeat.com/articles/2013/06/21/19341-how-the-nsas-high-tech-surveillance-helped-europe-catch-terrorists/

140 Le monde arabe est ici défini comme l'ensemble des pays de la Ligue arabe: Algérie, Arabie saoudite, Bahreïn, Comores, Djibouti, Egypte, Emirats arabes unis, Irak, Jordanie, Koweït, Liban, Libye, Mauritanie, Oman, Qatar, Somalie, Soudan, Syrie (suspendue), Territoires palestiniens, Tunisie et Yémen.

comploté contre la sécurité et les intérêts nationaux. Certains pays créent ou utilisent leurs capacités à restreindre les libertés civiles par le biais de proxys Blue Coat et de technologies étrangères dont ils se servent pour suivre et bloquer les communications dissidentes.

La censure en ligne est de grande ampleur, bien que les gouvernements prétendent censurer uniquement les sites pornographiques. Les utilisateurs peuvent se voir diriger vers un serveur proxy qui les empêche d'accéder à une liste de sites interdits et bloque des contenus jugés non conformes aux valeurs religieuses, culturelles, politiques et morales locales. La plupart des journalistes et des blogueurs pratiquent l'autocensure, notamment en ce qui concerne les questions politiques, culturelles, religieuses, ou tout autre sujet que les autorités peuvent considérer comme délicat du point de vue politique ou culturel. En général, ils évitent de critiquer les chefs d'Etat ou d'autres personnalités officielles, ou de publier des informations qui pourraient nuire à la réputation du pays, aux relations avec l'étranger ou à l'économie nationale. La diffamation est un crime.

Dans le cadre d'une affaire très médiatisée survenue aux Emirats arabes unis en 2009, le journaliste indépendant Mark Townsend, ancien chroniqueur économique du journal anglophone Khaleej Times, basé à Dubaï, a été accusé de diffamation criminelle et interdit de quitter le pays pendant près de deux ans pendant le déroulement de l'enquête. Il a été inculpé en vertu de l'article 373 du code pénal, parce qu'il aurait publié des articles dans lesquels il critiquait le Khaleej Times, détenu à 30% par l'Etat, et encourait une peine maximale de deux ans d'emprisonnement et une amende pouvant aller jusqu'à 20 000 dirhams (5 400 USD). Il a finalement été acquitté en mai 2011. Dans une autre affaire, cinq activistes et blogueurs émiratis ont été arrêtés et inculpés pour avoir insulté les dirigeants des Emirats arabes unis dans des publications sur le forum Internet UAE Hewar. Ils ont été condamnés à des peines de prison.

Sur une note plus positive, l'Internet est devenu un espace à partir duquel les activistes peuvent s'organiser et exercer des pressions. Un optimisme à nuancer, toutefois, étant donné que les gouvernements arabes coupent l'Internet dès que des manifestations civiles éclatent contre les autorités.

Dans le monde arabe, la vie privée est perçue essentiellement en termes physiques et matérielles. Elle concerne avant tout des droits tels que l'inviolabilité du domicile, de la correspondance et des communications. Cependant, les systèmes juridiques arabes ne protègent pas suffisamment le droit à la vie privée, hormis dans les rares cas où ce droit est protégé par la constitution ou par des codes.

Au Liban, la vie privée n'a pas de statut juridique bien défini, bien que le sujet ait fait l'objet de nombreux débats entre les dirigeants politiques. Elle est protégée par un ensemble de dispositions constitutionnelles et législatives. La constitution libanaise,

très proche en cela de la constitution des Etats-Unis, ne définit pas le droit à la vie privée. Néanmoins, elle protège les personnes ainsi que leur domicile et leurs effets personnels.

Certaines dispositions protègent la vie privée des personnes contre la divulgation d'informations dans certaines circonstances précises. L'Article 17 dispose que le domicile est inviolable et que nul ne peut y pénétrer que dans les cas prévus par la loi et selon les formes prescrites par elle. En outre, une loi sur la confidentialité des conversations stipule que les citoyens ont droit à la confidentialité de leurs communications locales ou internationales, filaires ou hertziennes.

La constitution libanaise reconnaît le droit des citoyens à être garantis dans leurs personnes, domiciles, papiers et effets, contre des perquisitions et saisies déraisonnables, lesquelles sont possibles uniquement lorsqu'elles sont autorisées dans des conditions prescrites par la loi. Au Liban, comme dans de nombreux pays du monde, les intrusions dans la vie privée, qui enfreignent de nombreuses libertés civiles, se fondent juridiquement sur des motifs tels que la sécurité nationale, la lutte contre le terrorisme et la protection de l'intérêt général.

Des motifs similaires sont invoqués pour justifier le blocage par le gouvernement de médias sociaux utilisant l'Internet qui servent parfois à promouvoir et organiser des mouvements de protestation dans le monde arabe.

En mars 2013, Reporters sans frontières a qualifié plusieurs pays arabes d'"ennemis de l'Internet"[141] en raison de leurs pratiques, par exemple leurs mesures de répression contre les blogueurs, qui entraînent de graves violations de la liberté de l'information et des droits humains.

La ligue des Etats arabes et les libertés civiles

La Ligue des Etats arabes a été créée sept mois avant les Nations Unies par six pays (Arabie saoudite, Egypte, Irak, Liban, Syrie et Transjordanie) et compte aujourd'hui vingt-deux Etats membres.

La Charte portant création de la Ligue en 1945 ne contient aucune référence aux droits humains. Par ailleurs, les documents juridiques de la Ligue arabe ne comportent aucune disposition relative à la protection des défenseurs des droits humains.

Toutefois, la Ligue a créé une commission chargée d'oeuvrer à l'intégration et à l'harmonisation du système juridique, en unifiant la terminologie, les structures et les procédures juridiques et judiciaires. Pour mettre en oeuvre les recommandations de cette commission, la Ligue a créé un Centre arabe d'études juridiques et judiciaires à Beyrouth. Ce centre a élaboré diverses conventions ayant trait à la coopération entre

141 Reporters sans frontières. Mars 2013 – Rapport spécial sur la surveillance de l'Internet intitulé "Ennemis de l'Internet" s'intéressant à cinq pays et cinq entreprises. http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html.

les pays arabes sur de nombreuses questions juridiques d'intérêt commun, notamment le modèle législatif sur la cybercriminalité. Il collabore avec de nombreuses organisations régionales et internationales ainsi qu'avec des organismes de la société civile sur les questions relatives à la gouvernance de l'Internet. Par exemple, il a collaboré avec la Commission économique et sociale des Nations Unies pour l'Asie occidentale pour créer et inaugurer le Forum arabe sur la gouvernance de l'Internet. En outre, il fait partie depuis 2009 des membres fondateurs de l'Observatoire panarabe pour la cybersécurité, et est à l'origine d'un projet de convention arabe sur la cybersécurité, qui doit être soumis au Conseil des ministres arabes de la justice. Ce projet présente clairement la protection des libertés civiles sur l'Internet comme un élément essentiel dans l'optique d'instaurer la confiance dans l'utilisation du cyberespace. Parallèlement, le Centre a inauguré de nombreux forums et de nombreuses rencontres annuelles à l'intention des décideurs du secteur des TIC sur des questions relatives aux droits de l'homme et aux libertés civiles, en particulier le droit à la vie privée, le droit d'accès à l'information et la liberté d'expression.

Conclusion

Des efforts concertés en matière de législation sont nécessaires pour trouver un juste équilibre entre, d'un côté, la nécessité de protéger les libertés civiles, la vie privée des internautes et, d'abord et surtout, la liberté d'expression, et, de l'autre, la nécessité de lutter contre les cybermenaces à l'encontre de la sécurité nationale. Y parvenir permettrait d'éviter que le cyberespace ne devienne un nouveau domaine placé sous surveillance.

Les Etats doivent traiter les infractions dans le cyberespace comme des infractions pénales au titre du droit national, et les combattre à l'aide à la fois de mesures proactives et réactives. Un traité ou accord international spécial prévoyant un niveau minimal de protection acceptable pour toutes les parties intéressées contribuerait à la protection de la vie privée lors des échanges d'informations. En complément, il conviendrait d'instaurer un cadre de coopération internationale efficace pour lutter contre la cybercriminalité transfrontière. A cet égard, le Centre d'études juridiques et judiciaires de la Ligue des Etats arabes m'a demandé d'élaborer un projet de convention arabe sur la coopération en matière de lutte contre la cybercriminalité transfrontière.

Dans le cadre de cette coopération, il conviendrait de mener les enquêtes, la surveillance, les poursuites, l'assistance juridique mutuelle et les procédures judiciaires conformément aux droits nationaux. De la même façon, la mise en oeuvre des procédures internationales d'application de la loi autorisées devrait être conforme aux législations nationales et aux traités d'assistance juridique mutuelle. Les Etats devraient introduire des procédures et mesures spéciales afin de protéger les échanges internationaux d'informations confidentielles, et surveiller les réseaux informatiques ainsi que la collecte et le traitement des données. Cela est particulièrement nécessaire dans les pays où le niveau de protection de la vie privée est insuffisant.

Il convient d'accorder une attention particulière à la protection contre les perquisitions et saisies illégales. La nature technique du cyberespace, associée à la hausse de la cybercriminalité et à l'absence d'un cadre pénal international en la matière, rend plus difficile la défense du respect des libertés civiles.

Dans la plupart des systèmes juridiques nationaux, le comportement des instances policières est réglementé par la constitution et la législation, ainsi que par des procédures qui protègent les citoyens contre les pouvoirs et mesures d'application de la loi abusifs, tels que les perquisitions et saisies non justifiées et la violation des libertés civiles lors du déroulement de ces opérations.

Pour les nombreux pays qui ne sont pas encore dotés de lois et de procédures concernant le cyberespace, et qui continuent de se référer au droit pénal général pour traiter les questions relevant de la cybercriminalité, une solution consisterait pour leurs gouvernements respectifs à adopter des directives visant à empêcher les violations des libertés civiles dans ce domaine. Ces directives devraient notamment définir de manière claire quelles sont les circonstances qui justifient les perquisitions et saisies, dans les limites des exceptions légitimes au respect des libertés civiles. Les rédacteurs de ces directives pourraient s'inspirer d'exceptions légales traditionnelles – par exemple, dans le cas du common law, le principe de l'objet bien en vue (*plain view doctrine*) ou les circonstances exceptionnelles (*exigent circumstances*).

Pour compenser ces exceptions, diverses mesures de protection pourraient être mises en place: chiffrement, serveurs de courriel anonymes, communications anonymes sécurisées, pare-feu et serveurs proxys. Bon nombre de ces technologies offrent une protection contre la cybercriminalité tout en renforçant le respect de la vie privée.

3.2 Cadres juridique, politique et réglementaire pour la liberté de l'Internet et les mégadonnées

Par Pavan Duggal

Introduction

Le monde dynamique actuel a subi une transformation radicale sous l'effet de la croissance exponentielle du cyberespace. Si l'Internet a aboli les repères géographiques, ce média transfrontière créé par le cyberespace est toutefois devenu l'objet d'immenses préoccupations pour tous les gouvernements de la planète. C'est pourquoi il est de la plus haute urgence de mettre en place des cadres politique et réglementaires appropriés pour le cyberespace.

L'Internet est fondé entièrement sur les données et les informations au format électronique. En réalité, les termes "données" et "informations" s'utilisent de manière interchangeable pour désigner les blocs élémentaires essentiels à la création de l'architecture de contenu servant de fondation aux voies de communication qui parcourent l'Internet.

Le développement de l'Internet, depuis l'Advanced Research Projects Agency Network (ARPANET) à la fin des années 60 au World Wide Web puis à l'époque actuelle des médias sociaux et du SMAC (Social, Mobile, Analytics et Cloud) a été un long parcours. L'Internet a été un grand facteur d'égalité, étant donné qu'il permet à tous ses utilisateurs d'accéder librement à l'information et qu'il les aide à résoudre leurs problèmes quotidiens et à gérer les différents aspects des activités humaines d'une multitude de façons.

L'Internet crée de gigantesques volumes de données. Comme l'a déclaré Eric Schmidt, ancien P.-D.G. de Google, "nous créons à présent autant de données en deux jours que nous en avons produit de l'aube de la civilisation jusqu'à 2003, soit environ cinq exaoctets". En écho à cette croissance stupéfiante, IBM affirme que nous créons chaque jour 2,5 quintillions de données – "[…] si bien que 90% des données existant dans le monde ont été créées au cours des deux dernières années"[142]. Ce phénomène est encore mis en évidence par une statistique figurant dans un rapport conjoint IDC-EMC, selon laquelle la taille de l'univers numérique fait plus que doubler tous les deux ans, et atteindra 40 000 exaoctets (40 milliards de gigaoctets) d'ici à 2020[143]. Dans ses perspectives pour 2012, *The Economist* a indiqué que la quantité de données numériques dans le monde était passée de 130 exaoctets en 2005 à 1 227 exaoctets en

142 http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

143 http://www.baselinemag.com/analytics-big-data/slideshows/surprising-statistics-about-big data.html#sthash.COE9uzq6.dpuf (dernière consultation le 4 août 2014).

2010, et qu'elle devrait atteindre 7 910 exaoctets en 2015[144]. Les préoccupations liées à ces gigantesques quantités de données ont pris une nouvelle ampleur avec l'arrivée des mégadonnées dans l'écosystème numérique.

Le présent article étudie les cadres juridique, politique et réglementaire relatifs aux libertés sur l'Internet et aux mégadonnées.

Définition

Avant de procéder à l'examen des questions juridiques et réglementaires ayant trait à la liberté de l'Internet, il convient de s'intéresser aux différentes définitions que les chercheurs et les juristes donnent de ce terme.

La définition de la liberté de l'Internet est une question large et controversée; il n'existe pas de définition universellement acceptée. Le Président des Etats-Unis, Barack Obama, a un jour déclaré: "L'Internet a libéré l'innovation, stimulé la croissance et favorisé la liberté plus rapidement et plus largement qu'aucun autre progrès technique dans l'histoire de l'humanité. Son indépendance est sa force.

144 Welcome to the yotta world', The Outlook for 2012, Economist, décembre 2011; http://www.economist.com/node/21537922.

L'Internet offre un système de communication unique en raison de la liberté qu'il possède vis-à-vis des interventions étatiques"[145]. Il a notamment ajouté: "La liberté de l'Internet est incompatible avec la réglementation relative à la liberté des réseaux et […] l'Internet devrait conserver sa liberté unique vis-à-vis de toute intervention étatique."

Dereck Bambauer, professeur de droit à l'université d'Arizona, a déclaré: "Peut-être qu'au bout du compte, la liberté de l'Internet est un terme qu'il conviendrait d'abandonner, parce qu'il est trop général pour être utile. Au lieu de se référer à ce concept, les pays, les cultures et les utilisateurs devraient faire face aux compromis délicats que supposent les communications sur l'Internet"[146].

Voici comment l'agence *Media Marxist outfit Free Press* définit la liberté de l'Internet sur son site web: "La liberté de l'Internet signifie que les fournisseurs de services Internet ne doivent pas faire de différence entre les différents types de contenus et d'applications en ligne"[147]. Le site web *Dictionnary.com* définit la neutralité des réseaux comme le principe selon lequel les protocoles Internet de base devraient être "non discriminatoires", ce qui suppose en particulier que les fournisseurs de contenus devraient être traités sur un pied d'égalité par les opérateurs de services Internet.

La liberté de l'Internet passe par la libre utilisation des fréquences

Alors que les radiodiffuseurs et les opérateurs de téléphonie mobile se voient octroyer des licences par les pouvoirs publics pour exploiter certaines bandes de fréquences, d'autres régions du spectre radioélectrique sont librement accessibles, ce qui signifie que toute entreprise peut lancer un produit – par exemple un téléphone sans cordon, un casque Bluetooth, un interphone de surveillance des bébés ou une télécommande, en utilisant cet espace librement accessible, sans avoir besoin d'une licence octroyée par les pouvoirs publics[148].

La liberté de l'Internet comporte non seulement la liberté d'accès à ce média, mais aussi la liberté d'expression. Plus important encore, elle signifie la liberté de simplifier la vie des personnes grâce aux nombreuses fonctionnalités offertes par l'Internet.

---

145 http://freestatefoundation.blogspot.in/2012/08/the-true-meaning-of-internet-freedom.html.

146 Bambauer, D., The Enigma of Internet Freedom, eJournal USA, Vol. 15, No. 6, 2010, pp. 4-6., voir également: http://www.wseas.us/e-library/conferences/2013/Dubrovnik/ECC/ECC-38.pdf (dernière consultation le 8 août 2014).

147 http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/.

148 http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/.

Caractéristiques essentielles

Des chercheurs sont parvenus à la conclusion que la liberté de l'Internet englobe un ensemble de libertés fondamentales, telles que la liberté de parole, le droit à la vie privée, la liberté d'innover et d'être récompensé et reconnu, et la liberté de l'architecture de l'Internet dans son ensemble[149].

Cadres politiques et réglementaires existants

Bien que l'Internet soit devenu un média mondial transfrontière, force est de constater que le monde ne s'est pas encore attelé à la tâche consistant à définir des normes acceptées au niveau international spécialement applicables au cyberespace. Par conséquent, lorsqu'on s'intéresse aux cadres juridique, politique et réglementaire, il est important de tenir compte du fait qu'il n'existe pas de traités internationaux sur la liberté de l'Internet. Des progrès ont toutefois été accomplis dans cette direction.

Comme cela a déjà été dit dans le présent rapport, la Convention sur la cybercriminalité adoptée par le Conseil de l'Europe en 2001, constitue un exemple remarquable en la matière. Les principales caractéristiques de cette Convention sont les suivantes:

- Premier traité international visant à aborder la cybercriminalité à l'aide d'une harmonisation des législations nationales pertinentes, de la formulation de définitions communes pour certaines infractions pénales, de l'amélioration des techniques d'enquête, et du renforcement "dans mesure la plus large possible" de la coopération entre les nations pour lutter contre ce phénomène150.
- Exige l'incrimination de pratiques telles que le piratage et les infractions se rapportant à la pornographie enfantine, et étend la responsabilité pénale à la violation des droits de propriété intellectuelle.
- Fournit une politique criminelle commune destinée à protéger la société contre la cybercriminalité par l'adoption d'une législation appropriée et la promotion de la coopération internationale[151].

La Déclaration sur la liberté de la communication sur l'Internet, adoptée par le Conseil de l'Europe en 2003, est une autre illustration remarquable de ces efforts. Les caractéristiques fondamentales de cette déclaration sont les suivantes:

- Affirme la nécessité d'assurer un équilibre entre la liberté d'expression et d'information et d'autres droits et intérêts légitimes, conformément à

---

149 Neelie Kroes, *Internet Freedom,* http://europa.eu/rapid/press-release_SPEECH-12-326_en.pdf, (dernière consultation le 8 août 2014).

150 http://en.wikipedia.org/wiki/Convention_on_Cybercrime (dernière consultation le 8 août 2014).

151 http://epic.org/privacy/intl/ccc.html.

l'Article 10 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales.

- Exprime des préoccupations concernant les tentatives visant à limiter l'accès du public aux communications sur l'Internet pour des raisons politiques ou d'autres motifs contraires aux principes démocratiques.
- Affirme que le contrôle a priori des communications sur l'Internet, sans considération de frontières, devrait rester une exception.
- Considère qu'il est nécessaire de supprimer les obstacles à l'accès individuel à l'Internet et de compléter ainsi les mesures déjà prises pour mettre en place des points d'accès publics.
- Exprime la conviction que la liberté de fournir des services via l'Internet contribuera à garantir le droit des usagers d'accéder à des contenus pluralistes provenant de multiples sources nationales et étrangères.
- Souligne que la liberté de communication sur l'Internet ne devrait pas porter atteinte à la dignité humaine, aux droits de l'homme ni aux libertés fondamentales d'autrui, tout particulièrement des mineurs.
- Salue les efforts entrepris par les fournisseurs de services pour coopérer avec les autorités chargées de l'application de la loi lorsqu'ils sont confrontés à des contenus illicites sur l'Internet.

SMSI

Le Sommet mondial sur la société de l'information a formulé les suggestions suivantes à l'intention du Partenariat sur la mesure des TIC au service du développement concernant les orientations à donner à ses activités:

- qu'il poursuive, étende et approfondisse ses travaux sur la mesure de la société de l'information, notamment en faisant appel à la participation des instituts nationaux de statistique à un stade aussi précoce que possible de l'élaboration des statistiques;
- qu'il continue ses activités de sensibilisation et de renforcement des capacités, en accordant une attention particulière aux pays à faible revenu;
- qu'il réfléchisse à de nouvelles sources de données et à de nouvelles méthodes;
- qu'il crée un groupe d'experts sur les cibles du SMSI.

Un fort consensus s'est dégagé en faveur du maintien du processus du SMSI et du suivi de la société de l'information après 2015. En outre, il convient d'approfondir la nature de ce suivi et de maintenir la coopération internationale ainsi que la coordination nationale sur la base du modèle multi-parties prenantes[152].

La Déclaration des libertés sur l'Internet constitue un plaidoyer éloquent en faveur des libertés en ligne[153]. Il est affirmé dans son préambule qu'un Internet libre et ouvert peut contribuer à un monde meilleur[154]. La Déclaration vise à obtenir des millions de signataires parmi les internautes[155]. Elle prône le respect de cinq principes fondamentaux en matière de politique de l'Internet:

- Ne pas censurer l'Internet.
- Accès universel à des réseaux rapides à un prix abordable.
- Liberté de se connecter, de communiquer, de créer et d'innover sur l'Internet.
- Protection des nouvelles technologies et des innovateurs contre les actes répréhensibles des utilisateurs
- Droit à la vie privée et capacité des internautes à protéger leur vie privée et à contrôler la confidentialité des données les concernant[156].

Lacunes en matière de cadres

Cependant, il est clair qu'il manque un régime international sur la liberté de l'Internet qui soit accepté par toutes les parties prenantes. En outre, la liberté de l'Internet en tant que phénomène soulève de nombreuses questions juridiques, politiques et réglementaires, dont certaines sont examinées ci-après.

De nos jours, de nombreux pays veillent au respect des droits fondamentaux et sont dotés de législations nationales qui garantissent la liberté de parole et d'expression dans le monde réel. Les mêmes droits ont également été interprétés dans l'optique de la liberté de parole et d'expression sur l'Internet ou appliqués dans ce contexte. Toutefois, les révélations survenues dans le cadre de l'affaire Snowden ont montré que la liberté

---

152 Manifestation de haut niveau SMSI+10 (2014) – Document final de la partie "Forum" http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/OutcomeDocument2014.pdf (dernière consultation le 06/11/2014).

153 http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom (dernière consultation le 08/08/2014).

154 http://www.internetdeclaration.org/ (dernière consultation le 08/08/2014).

155 Déclaration des libertés sur l'Internet, http://www.savetheinternet.com/internet-declaration

156 http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom (dernière consultation le 08/08/2014).

de parole et d'expression sur l'Internet faisaient l'objet d'intrusions non autorisées. A l'insu des utilisateurs concernés, les communications aux formats audio, vidéo, image et texte sont surveillées par des sources diverses. Concrètement, l'Internet et ses diverses fonctionnalités et plates-formes sont devenus des moyens de mettre en place une société fondée sur la surveillance. Partant de ce constat, il est clair qu'il y a deux sortes de personnes dans ce monde: ceux qui savent, et ceux qui ne savent pas qu'ils sont ou qu'ils ont été surveillés.

Le renforcement de la surveillance et du contrôle en ligne sont en train de devenir la norme, ce qui a des incidences directes sur la liberté de parole et d'expression sur l'Internet. En bref, si l'Internet n'est pas tout à fait le Far West, il apparaît clairement, au vu des indices qui se font jour, que la liberté de parole dans le cyberespace n'est pas une liberté absolue.

Les règles de comportement civilisé s'appliquent également à l'Internet. Par conséquent, les contenus en ligne destinés à causer des désagréments ou à susciter des ressentiments, de la haine ou de l'hostilité, ou qui visent une personne ou un groupe de personne particuliers, devraient être interdits par les législations nationales.

Toutefois, le voile d'anonymat que procure l'Internet peut donner aux utilisateurs mal intentionnés ou injurieux le sentiment de pouvoir dire et faire tout ce qu'ils veulent en toute impunité.

Néanmoins, dans ce contexte, des pays du monde entier mettent en place des mesures juridiques par lesquelles les tribunaux commencent à lever ce voile d'anonymat en demandant aux fournisseurs de services de divulguer la véritable identité des personnes se livrant à des activités illégales. Reste cependant que, comme cela a déjà été indiqué, il n'existe pas de définition admise à l'échelle internationale de ce qui constitue la liberté de parole et d'expression sur l'Internet.

La Déclaration universelle des droits de l'homme de 1948 énonce des principes fondamentaux que l'on pourrait interpréter comme étant entièrement compatibles avec la liberté de l'Internet.

Nouveaux défis

Les réseaux de médias sociaux ont fait apparaître de nouvelles formes de discours en ligne révélateurs de la mentalité des personnes. Cependant, les lois et les législations en vigueur dans le monde n'ont pas évolué de manière suffisamment rapide pour relever les nouveaux défis inhérents aux médias sociaux.

Les smartphones et autres dispositifs de communication ont annoncé l'entrée dans l'ère du web mobile. L'association des téléphones mobiles et de l'Internet ouvre la voie à des manifestations de la liberté de parole en ligne jusque-là inédites. Le problème survient lorsque des pays différents ne traitent pas les contenus inappropriés en ligne de la même façon, et que les limites de la liberté de discours en ligne ne sont pas les mêmes

d'un pays à l'autre. Malgré ces différences, il existe un consensus universel sur un point en ce qui concerne l'apparition du web mobile. L'association des téléphones mobiles et de l'Internet ouvre la voie à des manifestations de la liberté de parole en ligne jusque-là inédites.

Une autre question examinée précédemment concerne la capacité de communiquer librement et de façon anonyme sur l'Internet. Comme cela a déjà été dit, certaines personnes pensent que l'anonymat de l'Internet leur permet de dire tout ce qu'ils veulent en ligne, sans avoir à se soucier des éventuelles incidences de leurs propos sur les autres[157]. Souvent, la victime d'une diffamation présumée en ligne porte plainte contre un accusé anonyme.

Les différents pays ont des législations différentes en matière de diffamation, traitant de diverses formes de discours et de contenus diffamatoires. Ces législations s'appliquent également dans le cyberespace. Dans cette perspective, il apparaît de plus en plus clairement au vu des récentes décisions de justice que personne n'a le droit de diffamer une autre personne ou d'essayer de nuire à la réputation d'autrui.

Les dispositions législatives nationales en la matière varient d'un pays à l'autre. Certains pays restreignent l'accès à l'Internet uniquement lorsqu'ils estiment que cette mesure est justifiée lorsqu'il s'agit de protéger les valeurs morales, les droits juridiques personnels, la défense nationale ou la sécurité de l'Etat. D'autres ont officiellement reconnu que la liberté d'expression s'étendait au cyberespace, ou envisagent de le faire.

Nous vivons une époque charnière de l'histoire de l'humanité, dans laquelle la liberté de l'Internet est menacée non seulement par des entités étatiques, mais aussi par des acteurs privés qui, de fait, gèrent et contrôlent les données sur l'Internet.

Autres défis liés à la liberté de l'Internet

La juridiction en ce qui concerne l'Internet est une question importante rendue complexe par le fait que la liberté d'expression d'une personne peut être restreinte à l'intérieur des frontières territoriales d'un pays, alors que cette personne se trouve physiquement sur le territoire d'un autre pays. Par ailleurs, le fait d'être invariablement la cible des cybercriminels peut aussi être un facteur contribuant à empêcher les utilisateurs de jouir concrètement de leurs libertés sur l'Internet. Par conséquent, la cybercriminalité est devenue un problème important sur les plans juridique, politique et réglementaire, qui peut avoir des incidences sur la liberté de l'Internet quel que soit l'endroit où se trouvent les utilisateurs.

Un autre problème ayant des répercussions sur la liberté de l'Internet est celui de la cybersécurité. Un utilisateur ne peut jouir de sa liberté juridique sur l'Internet qu'à

---

157 Eric Sinrod, *"Freedom of anonymous online speech has potential limits"* http://www.lexology.com/library/detail.aspx?g=7a8eb382-b007-49c6-8ca1-4a9197062d9d, (dernière consultation le 08/08/2014).

condition que celui-ci soit sûr, sécurisé et fiable. Cependant, les atteintes à la cybersécurité ont une nouvelle fois mis au premier plan les différents défis auxquels nous sommes confrontés pour ce qui de la protection et de la préservation des ressources et de l'infrastructure du cyberespace.

Il sera nécessaire d'envisager les libertés sur l'Internet selon une approche entièrement différente, compte tenu du caractère mondial et des vulnérabilités de ce cybermédia. Vu la hausse rapide des cyberattaques visant des systèmes et réseaux informatiques dans de nombreux pays, un équilibre devra être trouvé entre la liberté de l'Internet et la nécessité d'assurer et de maintenir la cybersécurité.

Il n'existe toujours pas de consensus international concernant la question de la responsabilité des intermédiaires. Certains pays, à l'instar des Etats-Unis, n'attribue pas ce type de responsabilité aux fournisseurs de services. D'autres exigent parfois que les intermédiaires fassent preuve de la diligence voulue dans les cas où ils veulent éviter une éventuelle responsabilité civile concernant les données en ligne, tout en se déchargeant de leurs obligations au titre de certaines dispositions de base de la législation nationale.

L'apparition du "darknet" représente un autre défi considérable pour la liberté de l'Internet. Les cybercriminels n'hésitent pas à utiliser cet environnement pour mener leurs activités et plans malveillants visant à nuire aux libertés des personnes sur l'Internet.

Le développement de la cyberguerre, phénomène dont le secret est aujourd'hui éventé, vient s'ajouter à liste des défis qui font obstacle à la confiance dans l'utilisation du cyberespace et à l'exercice des libertés sur l'Internet. L'entrée dans l'ère du cyberterrorisme vient encore entraver de façon chaotique le plein exercice des libertés sur l'Internet.

Il est clairement nécessaire d'adopter une interprétation de la liberté de l'Internet valable au niveau international et d'établir des principes de base communs dans ce domaine. Un travail considérable a été accompli sur les importantes questions juridiques et politiques évoquées ci-avant, qui ont des incidences sur la liberté de l'Internet. C'est dans ce contexte que des organisations telles que la World Federation of Scientists et l'Union internationale des télécommunications peuvent continuer de jouer un rôle important en favorisant l'apparition d'un consensus concernant la marche à suivre.

Mégadonnées

A ce stade, l'incidence des mégadonnées sur la liberté de l'Internet ne saurait être ignorée, car, en définitive, il faut envisager cette liberté dans le contexte des données et des informations électroniques. Aujourd'hui, l'Internet est un gigantesque réseau de réseaux, un colossal dragon de données doté d'une mémoire infinie. Par conséquent, il

faut aussi considérer que la liberté de l'Internet sous toutes ses formes est en connexion, en association et en relation directe avec les mégadonnées.

Les mégadonnées sont la grande réalité de notre temps. La quantité de données générée par les différents systèmes et réseaux informatiques est telle qu'il n'y a rien d'étonnant à ce que des entreprises souhaitent se consacrer à l'analytique des mégadonnées. Les mégadonnées sont définies de diverses manières par les différentes parties prenantes, et constituent une question importante sur les plans juridique, politique et réglementaire.

Définition des mégadonnées

Wikipédia définit les mégadonnées de la manière suivante: "[...] terme générique désignant tout ensemble de données si volumineux et complexe qu'il devient difficile à traiter à l'aide des outils de gestion des données disponibles ou des applications de traitement des données classiques. Cependant, les mégadonnées incluent généralement les ensembles de données dont le volume dépasse la capacité des outils logiciels habituellement utilisés pour ce qui est de la saisie, de la curation, de la gestion et du traitement des données dans un délai raisonnable"[158]. Le **Oxford Dictionary** définit les mégadonnées comme suit: Ensembles de données trop volumineux et trop complexes pour être manipulés ou interrogés au moyen des méthodes ou des outils habituels[159]. Le **rapport de la Maison-Blanche sur les mégadonnées**, publié le 1er mai 2014, énonce la définition désormais largement admise selon laquelle les mégadonnées "[...] ont un volume si élevé, une variété si grande ou évoluent à une vitesse telle que les modes classiques de saisie des données sont insuffisants[160]". Selon la **Tech America Foundation**, "le terme "mégadonnées" désigne de larges volumes de données à vitesse élevée, complexes et variables qui nécessitent des techniques et des technologies évoluées pour assurer la saisie, le stockage, la diffusion, la gestion et l'analyse des informations[161]".

Les diverses caractéristiques des mégadonnées sont les suivantes:

- Elles doivent être de nature élastique[162].

---

158 http://en.wikipedia.org/wiki/Big_data.

159 http://www.oxforddictionaries.com/definition/english/big-data

160 http://www.lexology.com/library/detail.aspx?g=e7161021-7570-476c-bf8a-b4637d10a355

161 Tech America Foundation, Demystifying Big Data: A Practical Guide to Transforming the Business of Government (2012), https://www-304.ibm.com/industries/publicsector/fileserve?contentid=239170 (dernière consultation le 4 août 2014).

162 http://hadoopblog.blogspot.in/2012/02/salient-features-for-bigdata-benchmark.html

- De nombreux systèmes de mégadonnées prennent en charge des données qui n'ont pas subi de curation, de sorte qu'il y a toujours des points de données représentant des valeurs aberrantes extrêmes, ce qui crée des "points sensibles" dans le système.
- Les mégadonnées peuvent rapidement obtenir les cycles de calcul requis en utilisant une infrastructure dans le nuage en tant que service[163].
- La quantité de données créée dans ce contexte est très grande. C'est la taille des données qui détermine leur valeur et leur potentiel, et si elles peuvent effectivement être considérées comme des mégadonnées.
- La variété est liée au fait de gérer la complexité de multiples types de données, y compris des données structurées, semi-structurées et non structurées.
- La vitesse à laquelle les données sont créées, traitées et analysées continue d'augmenter. La création des données en temps réel est l'un des facteurs qui contribuent à cette augmentation de la vitesse, de même que le besoin d'incorporer les flux de données dans les processus opérationnels et la prise de décisions.
- L'incertitude des données: La véracité a trait au niveau de fiabilité associé à certains types de données[164].

Les mégadonnées soulèvent de nombreuses préoccupations d'ordre juridique, politique et réglementaire. Tout d'abord, il convient de noter qu'il n'existe pas de cadre international – ou de traités internationaux – concernant les mégadonnées. Par conséquent, la réglementation des mégadonnées relève encore des législations nationales. Or la plupart des pays ne disposent pas d'une législation ou de dispositions juridiques relatives à ce domaine. En vue de la mise en place de cadres politique et réglementaire, il est cependant indispensable de tenir compte des paramètres importants exposés ci-dessous.

La protection des données est l'un des plus grands défis liés aux mégadonnées. Les différentes juridictions nationales ont des exigences réglementaires différentes pour ce qui est de la protection des données. L'Union européenne dispose de directives relatives à la protection des données, alors que les pays d'autres régions ont intégré diverses dispositions relatives à la protection des données dans leur législation nationale. Il importe de prêter attention aux méthodes de collecte, de protection et de préservation des données. La protection des mégadonnées nécessite une nouvelle approche

---

163 http://www.dummies.com/how-to/content/characteristics-of-big-data-analysis.html

164 IBM, Analytics: The real-world use of big data- How innovative enterprises extract value from uncertain data, http://www.ibm.com/smarterplanet/global/files/se__sv_se__intelligence__Analytics_-_The_real-world_use_of_big_data.pdf (dernière consultation le 8 août 2014).

distincte, étant donné que la législation en matière de protection des données a toujours été conçue dans l'optique de volumes de données relativement faibles produits par des particuliers, qui sont minuscules comparés aux volumes des mégadonnées.

La protection des mégadonnées pose d'immenses défis, tant du point de vue du traitement des données que de la réglementation. Leur volume considérable et leur architecture de référencement et d'approvisionnement utilisant des sources diverses nécessitent un cadre juridique distinct, sûr et sécurisé qui permette de protéger à la fois les utilisateurs et les fournisseurs des données.

La minimisation des données soulève également des problèmes en matière de protection de la vie privée et des données. Dans cette optique, il convient d'accorder une attention particulière à la nécessité d'établir des bonnes pratiques internationales appropriées pour la collecte, la détention et la destruction des données, y compris les données à caractère personnel sous forme identifiable.

Les législations nationales divergent sur la question du consentement individuel pour la collecte, l'utilisation ou la divulgation des données par opposition au contrôle individuel des données. Comme indiqué précédemment, il n'existe pas de dispositif juridique international relatif aux mégadonnées, que ce soit pour cette question ou pour les autres questions liées au cyberespace.

Un autre problème juridique est celui de l'anonymat des données et du masquage des données pour les personnes qui mettent des informations sur l'Internet. Une importante question qui n'a pas été traitée de manière appropriée est celle des principes de base qui devraient s'appliquer dans le contexte de la collecte, du traitement, de la détention et de la diffusion des mégadonnées. Etant donné que les mégadonnées se trouvent aujourd'hui systématiquement dans le nuage, leur protection et leur préservation constituent d'autres défis sur les plans juridique, politique et réglementaire.

La confidentialité des données est un enjeu important dans le contexte des mégadonnées, en raison des énormes volumes de données consommés, et aussi parce que chaque fournisseur de données possède un droit intrinsèque à la protection et à la préservation de ses données. Par conséquent, il est de l'entière responsabilité du service de réseau de garantir une protection suffisante de ces données.

La juridiction des mégadonnées est aussi une question importante sur les plans juridique, politique et réglementaire, car ces données se situent systématiquement dans le nuage et sur divers autres serveurs se trouvant dans différents endroits du monde. En cas d'atteinte à la confidentialité des mégadonnées, la personne lésée doit entreprendre une action en justice contre les fournisseurs de services concernés. Le grand défi sera d'identifier l'emplacement physique des données en question, étant donné que la détermination de l'emplacement du serveur sur lequel l'infraction s'est

produite aurait des incidences du point de vue de la législation locale relative aux atteintes à la vie privée.

La cybercriminalité dans la perspective des mégadonnées représente également un enjeu juridique majeur, dans la mesure où l'économie de l'Internet repose entièrement sur ces données, et que les atteintes non autorisées à la confidentialité des mégadonnées peuvent grandement faciliter les desseins des cybercriminels, qui s'en prendront donc toujours plus souvent à ce type de données.

En octobre 2013, Adobe a confirmé que des cybercriminels étaient parvenus à accéder illégalement à son réseau, ce qui leur avait permis d'obtenir plus de 2,9 millions de noms d'utilisateur, de numéros de cartes de crédit et de débit encryptés, de dates d'expiration de carte, d'identifiants et de mots de passe. Les auteurs de cette cyberattaque ont également eu accès au code source d'Adobe pour plusieurs produits, dont Acrobat et Coldfusion[165].

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), organe consultatif de l'Union européenne, a déclaré en janvier 2013: "L'exploitation des mégadonnées aura des incidences sur la confidentialité des données. Par ailleurs, l'exploitation des mégadonnées par des parties hostiles pourrait ouvrir la voie à [un] nouveau type de vecteurs d'attaque"[166]. L'ENISA a ajouté que les mégadonnées sont l'agrégation d'informations produites "[...] du fait de la prolifération des technologies sociales, de l'informatique en nuage, de l'informatique mobile et de l'utilisation de l'Internet en général", et qu'elles étaient devenues un nouvel enjeu de sécurité.

Vie privée

L'analytique des mégadonnées pourrait avoir des incidences directes sur la violation de la vie privée. En 2014, la Maison-Blanche a publié son rapport longuement attendu sur les mégadonnées: *Big Data: Seizing Opportunities, Preserving Values* ("Mégadonnées: saisir les occasions, préserver les valeurs"). Elaboré à la demande du Président des Etats-Unis, Barack Obama, le rapport étudie de quelles façons l'évolution rapide des progrès technologiques rend possible la collecte, le stockage, l'analyse et l'utilisation de grandes quantités de mégadonnées, tant par les pouvoirs publics que par le secteur privé. Il décrit les menaces pour la vie privée et l'égalité qui pourraient résulter des mégadonnées, aujourd'hui et dans l'avenir, et encourage les initiatives juridiques,

---

165 http://blogs.mcafee.com/consumer/consumer-threat-notices/malicious-acrobatics-adobe-the-latest-target-in-string-of-cyberattacks

166 http://www.out-law.com/en/articles/2013/january/cloud-mobile-social-and-big-data-technology-innovations-increasing-threat-of-cyberattacks-says-eu-body/.

politiques et réglementaires visant à protéger les citoyens aux Etats-Unis et dans le monde contre d'éventuelles atteintes[167].

Les mégadonnées et la confidentialité des données prennent donc de plus en plus d'importance dans le monde juridique. Des conflits surviendront souvent concernant la propriété des contenus de mégadonnées, d'autant plus lorsque des tierces parties s'occupent du développement des systèmes conçus pour créer ces données. La protection des données, y compris des informations personnelles sensibles, à l'aide de la cryptographie et du contrôle granulaire de l'accès, est un autre motif de préoccupation majeur.

La consultation des mégadonnées et l'accès à ces dernières présentent également un lien intrinsèque avec la vie privée, et constituent des enjeux juridiques de premier plan dans le contexte de la préservation des données et de l'analytique des données. Il est particulièrement important de préserver l'authenticité, l'intégrité et la véracité des mégadonnées qui font l'objet d'un accès et d'une consultation.

Par ailleurs, l'utilisation de systèmes de sécurité centrés sur les données reposant sur la cryptographie pose elle-même des problèmes sur le plan juridique, et le contrôle granulaire de l'accès entraîne plusieurs autres problèmes complexes sur les plans juridique et politique en ce qui concerne la vie privée. De plus, il est nécessaire de préserver la vie privée lors de la diffusion des informations.

Une autre préoccupation de taille concernant les mégadonnées réside dans le fait qu'il peut être très difficile d'en préserver l'anonymat une fois qu'elles ont été collectées. Si des projets de recherche prometteurs sont en cours en vue de masquer les données personnelles à l'intérieur des grands ensembles de données, des efforts bien plus évolués sont actuellement déployés afin de réidentifier des données apparemment "anonymes". L'investissement collectif dans la capacité de fusionner les données est plusieurs fois supérieur à celui en faveur des technologies destinées à améliorer la confidentialité[168]. Il est particulièrement important de garantir l'authenticité, l'intégrité et la véracité des mégadonnées destinées à faire l'objet d'une consultation et d'un accès.

D'autres problèmes juridiques concernent la sécurisation de l'infrastructure des mégadonnées par l'intermédiaire d'un cadre juridique approprié pour protéger les calculs dans les structures de programmation distribuées. A ce sujet, il convient

---

167 Kenneth R. Florin, Ieuan Jolly et al. "White House "big data" report highlights benefits and potential for abuses from big data" http://www.lexology.com/library/detail.aspx?g=a036aed0-cffb-4ae1-a518-44b92201effb (dernière consultation le 4 août 2014).

168 Bureau administratif du Président, *Big Data: Seizing Opportunities, Preserving Values,* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (dernière consultation le 4 août 2014).

d'élaborer de bonnes pratiques appropriées pour établir et maintenir la sécurité des mémoires de données non relationnelles. La gestion des données constitue encore un autre problème juridique. A ce sujet, il est nécessaire d'établir des cadres juridiques propices appropriés afin de sécuriser le stockage des données et les journaux transactionnels, ainsi que les audits granulaires.

Les droits de propriété intellectuelle relatifs aux mégadonnées constituent un autre problème juridique majeur. Qui détient les droits de propriété intellectuelle des mégadonnées? Quels sont les droits de propriété intellectuelle associés à la collecte, au stockage, au traitement ou au partage des mégadonnées? Des préoccupations sont souvent exprimées concernant le fait que les nouveaux outils de recherche et d'analyse des mégadonnées pourraient entraîner une violation du droit d'auteur des mégadonnées. La détermination de la responsabilité des parties contractantes en cas d'informations inexactes ou incomplètes, où lorsque des accords contractuels ne sont pas honorés, sont d'autres motifs de préoccupation.

Il se peut également que les technologies rendent possible l'accès non autorisé aux informations sur des concurrents commerciaux, ce qui pose divers problèmes en matière de droit de la concurrence. Le fait que la rentabilité des mégadonnées dépende de ces secrets commerciaux et de ces données personnelles sensibles a en soi des incidences sur le respect de la confidentialité et de la sécurité – et nuit à la confiance dans l'utilisation des plates-formes en ligne et des technologies.

Certains estiment que la collecte et le traitement des mégadonnées ont une influence sur les identités individuelles et collectives des personnes, ce qui risque de nuire à la qualité de la démocratie.

Une préoccupation supplémentaire a trait au fait que parmi ceux qui censurent les mégadonnées figurent de nombreux puissants intermédiaires, ce qui augmente le risque que ces données fassent l'objet d'une utilisation abusive pour violer les droits et les libertés individuelles.

En résumé, il est nécessaire de mettre en place un cadre juridique propice approprié pour faire en sorte que les mégadonnées n'empêchent en aucune façon les citoyens de jouir de leurs droits – ou d'ailleurs de remplir leurs obligations et devoirs civiques.

Rôle de la World Federation of Scientists et de l'UIT

Compte tenu de l'absence de paramètres internationaux instituant des cadres juridique et politique pour les mégadonnées, il est indispensable que des organisations telles que la World Federation of Scientists et l'Union internationale des télécommunications poursuivent leurs efforts afin d'en faciliter l'élaboration.

Conclusion

En conclusion, on peut affirmer que la liberté de l'Internet et les mégadonnées sont deux concepts tout à fait passionnants en pleine évolution, qui occupent une place de

plus en plus grande dans nos vies quotidiennes. Il est par conséquent indispensable de d'établir et de mettre en oeuvre des cadres juridique, politique et réglementaire internationaux appropriés pour préserver les libertés sur l'Internet. L'enjeu n'est rien de moins que l'avenir même des structures de l'ère du numérique, qui nous sont si utiles et dont nous sommes devenus si dépendants à bien des égards au fil des années.

La tâche importante à accomplir est la conception et la mise en oeuvre de ces cadres juridique, politique et réglementaire internationaux fondés sur des principes universellement admis.

Ces cadres ne pourront que se développer progressivement. De nombreuses initiatives sont en cours dans le domaine juridique en ce qui concerne les libertés sur l'Internet et les mégadonnées. Toutefois, des efforts doivent impérativement être déployés pour élaborer des cadres politique et réglementaire efficaces au niveau international.

Le Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists peut jouer un rôle extrêmement important à cet égard, non seulement pour assurer une fonction de surveillance, mais aussi pour contribuer à l'élaboration de ces cadres internationaux. Aux côtés de l'Union internationale des télécommunications, la World Federation of Scientists et d'autres organisations concernées seront, espérons-le, capables d'apporter une contribution importante en vue d'atteindre ce but, à la mesure de leurs compétences et de leur expérience dans ces domaines. Il serait sans doute très bénéfique pour toutes les parties prenantes que ces organisations puissent aider à l'élaboration de principes de base communs universellement admis visant à instaurer un environnement approprié pour ce qui est du cyberespace.

Comme indiqué précédemment, l'enjeu n'est autre que la capacité des utilisateurs à continuer de profiter des avantages liés aux libertés sur l'Internet, en surmontant les difficultés relatives à la cybersécurité et à d'autres défis, qui risquent de nuire à la confiance dans cet univers en pleine expansion et toujours plus essentiel.

Il est à espérer que des dispositions juridiques pertinentes se mettront en place à un rythme aussi soutenu que la croissance du nombre d'internautes et l'accélération des progrès techniques relatifs au cyberespace. Ce n'est que par un suivi constant de l'évolution des dispositions juridiques pertinentes et par une contribution aux progrès accomplis en la matière que le monde en général, et les acteurs essentiels en particulier, seront en mesure de déterminer quelles voies emprunter.

Le processus d'élaboration de cadres juridique, politique et réglementaire pertinents pour les mégadonnées et la liberté de l'Internet évoluera au cours du temps. L'extension du respect des droits fondamentaux au cyberespace constituera une condition préalable importante pour réussir dans cette entreprise.

3.3 Etat des lieux mondial de la surveillance étatique dans le cyberespace

Par Howard Schmidt

Introduction

Pour pouvoir bien comprendre le sujet de la surveillance dans le cyberespace, et formuler une opinion avisée à cet égard, il importe en premier lieu de souligner que notre cadre de référence est en grande partie fondé sur un monde dans lequel les règles de conduite (écrites ou autres) ont évolué au fil du temps, en particulier au cours de la période située bien avant l'avènement de ce que l'on dénomme le "cyberespace".
Pour chaque personne qui considère que la surveillance est justifiée, il y en aura toujours une autre de l'avis contraire, ainsi qu'un grand nombre de parties prenantes qui se trouvent dans une zone grise en ce qui concerne ce sujet. C'est en analysant des données empiriques et en appliquant un raisonnement inscrit dans une perspective mondiale que l'on pourra en définitive aboutir à un ensemble de lignes directrices équilibrées dont toutes les parties prenantes pourront tenir compte lorsqu'elles devront déterminer si la surveillance étatique est à la fois appropriée et justifiée.

Collecte de données

L'évolution de la technologie a créé un environnement dans lequel des volumes conséquents de données sont générés, transmis et collectés à différentes fins. Tout ce qui est produit dans le cyberespace repose sur des données; aussi, il est essentiel de pouvoir non seulement saisir ces données, mais aussi collecter les données saisies. Les transactions financières constituent un exemple de données essentielles qui doivent pouvoir être saisies et collectées. Prenons l'exemple du mode de versement des salaires de nos jours. Parmi nous, nombreux sont ceux qui reçoivent leurs salaires sous la forme d'un transfert électronique de fonds déposés sur leur compte, et qui conservent et archivent ces données électroniques au moyen d'un compte épargne. Ces données archivées peuvent ensuite entre transférées vers un autre point de collecte par le biais d'une transaction (par exemple dans un supermarché) lors de laquelle des biens sont fournis en échange de ces données, qui constituent donc un instrument financier.

Les communications téléphoniques mobiles entre deux parties constituent un autre exemple de données collectées d'une manière similaire: la société de téléphonie mobile conserve la trace des communications pour ce qui est de l'endroit depuis lequel ils ont été effectués, leur date et leur durée. Cette collecte de données est effectuée, comme

les sociétés de téléphonie mobile l'expliquent à leurs clients, à des fins de facturation. Les sites web collectent des données concernant leurs utilisateurs à diverses fins, notamment pour définir et garder en mémoire leurs préférences et archiver des éléments d'information qu'ils ont créés (notamment sur les sites web des médias sociaux).

En tant que citoyens dans le cyberespace, nous comprenons et acceptons que, dans certaines circonstances, la collecte de données n'est pas seulement raisonnable et acceptable, mais bien souvent souhaitable. La collecte de données par les parties prenantes concernées est d'autant mieux acceptée que le contenu des données collectées et les raisons de cette collecte sont exposés clairement. Dans de tels cas, nous choisissons soit d'accepter les conditions relatives à la collecte de données avant de nous livrer à l'activité concernée, soit de ne pas nous livrer à cette activité si nous estimons que le coût de la collecte de données et des politiques d'utilisation est trop élevé.

Concrètement, en tant que parties prenantes, nous acceptons les termes d'un contrat avec les entités qui ont accès à nos données; ce contrat définit la façon dont les données peuvent être collectées et utilisées, les entités qui peuvent conserver nos données (par exemple la société de téléphonie mobile), et la mesure dans laquelle celles-ci peuvent transférer la responsabilité de conserver ces données ainsi que les entités auxquelles elles peuvent les transférer. Si les entités responsables de la conservation des données ont un pouvoir immense en ce qui concerne les données, elles n'ont pas pour autant le droit d'en disposer comme bon leur semble. A terme, lorsque ces entités choisissent de faire un usage des données qui sort du cadre du contrat qui les lient aux personnes ou organisations auxquelles les données sont liées, elles doivent conclure un nouvel accord autorisant cet usage. Dans le cas contraire, l'absence de nouveau contrat peut être raisonnablement considérée comme un abus de pouvoir ou de confiance.

Cadre judiciaire vs collecte de renseignements

Les motifs énoncés plus haut sont à l'origine de l'existence des cadres en vigueur à l'heure actuelle, lesquels permettent une utilisation des données au-delà de ce que peuvent souhaiter les parties prenantes concernées. Lorsqu'il existe un doute raisonnable concernant une personne qui serait impliquée dans des activités criminelles, des procédures juridiques et judiciaires permettent d'avoir accès à des données préalablement collectées et de les analyser afin qu'elles puissent constituer des éléments de preuve. Les règles et procédures associées à la surveillance effectuée dans ce cadre diffèrent en fonction des pays, mais la population a en général accès aux règles de conduite.

La situation est un peu plus floue lorsque la surveillance est effectuée par l'intermédiaire de services de renseignement étatiques. A l'échelle mondiale, les services de renseignement surveillent et collectent secrètement des données et utilisent ces

informations à différentes fins. Officiellement, la plupart de ces services déclarent que les renseignements collectés le sont pour des raisons visant à assurer la sécurité nationale (par exemple dans le cas des récentes révélations de la NSA) ou le bien commun. D'autres indiqueront simplement que leur souveraineté les y autorise, et que, au fond, ils n'ont pas besoin d'expliquer les raisons pour lesquelles ils effectuent des collectes de renseignements. Ce problème revêt une dimension particulière dans le cadre d'une économie mondiale où deux ou plusieurs pays ont des positions différentes en ce qui concerne de telles collectes de données. Dans de tels cas, les cybercitoyens peuvent penser bénéficier d'un niveau de confidentialité qui corresponde aux règles édictées par leur gouvernement, mais transmettent des informations via le cyberespace, où les voies qu'empruntent les données entre le lieu d'origine et le lieu d'arrivée peuvent traverser les frontières nationales. Lorsque les données sont reçues dans un pays où les règles sont différentes, elles sont alors soumises à ces règles. Dans la mesure où la collecte de renseignements est un processus fermé qui est rarement soumis au principe de transparence attendu des procédures juridiques et judiciaires, il devient extrêmement difficile de déterminer si une limite a été franchie.

Règles et méthodes en matière de collecte de renseignements

Si la collecte de renseignements est autorisée en dehors d'un cadre juridique ou judiciaire (et c'est bien souvent le cas), il importe alors d'examiner la question de l'utilisation, par les entités qui s'occupent de collecter des renseignements, de logiciels malveillants et d'applications installées secrètement. Dans un grand nombre d'Etats souverains, la création de logiciels et d'applications malveillants destinés à infiltrer des systèmes informatiques par l'intermédiaire de diverses méthodes de propagation est considérée comme tout à fait illégale en soi. Toute action effectuée par le logiciel malveillant à compter de la propagation est également considérée comme un acte criminel imputable au créateur du logiciel; de même, tout utilisateur ou entité propageant et utilisant consciemment le logiciel aux mêmes fins est considéré comme ayant commis un acte criminel. Les cadres juridiques et judiciaires en place à l'heure actuelle régissent ces actes, et les peines peuvent être assez lourdes en cas de violation de la loi à cet endroit.

Une fois de plus, lorsque l'on analyse le fonctionnement des entités qui s'occupent de collecter des données avec l'appui de l'Etat, il apparaît que les règles qui encadrent les activités impliquant la création et la propagation de logiciels malveillants et d'applications installées de manière officieuse ainsi que la collecte de données en lien avec l'utilisation de tels "outils" sont très floues. Selon l'Etat souverain considéré, le fait de mener de telles activités peut être jugé acceptable de la part de services de renseignements d'Etat à différentes fins, le plus souvent pour des motifs liés à la sécurité nationale. Il est toutefois important de noter que, dès lors que le logiciel malveillant est déployé, il peut se propager bien au-delà des frontières prévues, comme c'est souvent le cas, et avoir des incidences négatives sur des systèmes qui seraient clairement

considérés comme hors du champ d'action des services de renseignement à tous égards. Il pourrait notamment s'agir de systèmes essentiels tels que les réseaux des hôpitaux et les réseaux électriques, et de systèmes de sécurité utilisés pour surveiller des processus dangereux (comme la fabrication de produits chimiques). En outre, les systèmes financiers, de production d'aliments et de production peuvent en subir les conséquences, ce qui peut créer des troubles considérables au sein de la société.

A cyberarmes égales

L'on peut considérer que l'utilisation d'un logiciel malveillant telle qu'elle est définie dans le présent ouvrage est l'équivalent de l'utilisation d'une cyberarme, étant entendu que la portée de cette arme peut être bien plus grande que ce qui était prévu initialement. En outre, la capacité de créer et de déployer une cyberarme n'est limitée par aucune des contraintes économique ou naturelle rencontrées habituellement lors de conflits traditionnels. La présence de métaux, d'installations chimiques ou d'outils de haute technologie n'a que peu d'impact sur les capacités des créateurs de logiciels malveillants. Il leur suffit amplement de disposer d'un ordinateur et d'une connexion au réseau ou d'un support de stockage et de transport de données externe (par exemple une clé USB), et du savoir-faire nécessaire pour créer le logiciel malveillant.

Dès lors qu'un logiciel malveillant a été créé et s'est propagé, il peut ensuite être utilisé comme une arme par toute personne ou entité qui peut le trouver et s'en saisir. Cela signifie que la cyberarme peut être retournée contre l'entité qui en est à l'origine, notamment par la propagation d'une version ayant subi une mutation augmentant la fonctionnalité du logiciel malveillant initial. Dans de tels cas, l'entité qui est à l'origine du logiciel malveillant tient lieu de fournisseur mondial de cette cyberarme. Cela signifie concrètement que, au-delà des bénéfices qui découlent de la première attaque, toutes les parties "jouent à armes égales" peu de temps après le lancement du logiciel malveillant; dans ce cas, la situation peut devenir très destructrice et aucun individu ou entité ne peut se protéger. Par ailleurs, une fois les cyberarmes déployées, elles existent pour ainsi dire à jamais puisqu'il n'y a aucun arsenal à détruire.

Comment aller de l'avant

Il va sans dire que, indépendamment des intentions des entités qui se livrent subrepticement à une surveillance appuyée par l'Etat, des problèmes considérables voient le jour et leurs retombées négatives peuvent être incontrôlables et imprévisibles. Cette situation peut créer une onde de choc susceptible de déstabiliser les relations internationales et les conditions économiques mondiales. Si l'Internet peut constituer un moyen efficace d'effectuer une surveillance avec des intentions que certains peuvent juger bonnes, il est important de savoir que l'Internet est devenu une composante intégrale et nécessaire de l'économie mondiale et qu'il permet aux individus, aux organisations et aux pays, peu importe leur taille, de prendre part à l'économie sur un

pied d'égalité. Il permet également d'échanger des idées gratuitement et instantanément et de collaborer entre tous les maillons de la chaîne.

De ce fait, il est important que le monde des affaires dans son ensemble et à tous les niveaux exerce une pression sur les pouvoirs publics de tous les pays afin que ces derniers adoptent les lois adéquates. Ces lois devraient permettre d'éviter que les utilisateurs soient privés des avantages socio-économiques qui découlent de l'Internet. Elles devraient également rendre possible l'augmentation continue du nombre d'individus, d'organisations et de pays pouvant prendre part à une économie collaborative alimentée par un Internet stable, dans le cadre de laquelle tous sachent avec certitude que les intérêts des pouvoirs publics ne sont pas placés avant ceux des individus qu'ils servent.

3.4 L'étendue de la surveillance étatique dans le cyberespace: point de vue de l'Union européenne

Par Henning Wegener

La question de la tension inhérente et croissante entre d'une part la liberté et l'intégrité de l'Internet (et des communications numériques de manière générale) et d'autre part le besoin de plus en plus urgent d'assurer l'ordre public et de répondre aux préoccupations collectives sur le plan de la sécurité a été traitée dans de nombreuses sections de la présente publication, en particulier dans l'essai de Mme Al-Achkar sur les libertés sur l'Internet et notamment les libertés du citoyen.

Du fait de la divulgation actuelle d'intrusions massives dans les dispositifs numériques et les réseaux et de la peur des données massives, cette tension est plus que jamais au premier plan des préoccupations de la société en Europe. La très forte croissance des moyens techniques permettant de collecter et de traiter des données, qui ont fait basculer l'humanité dans une nouvelle ère marquée par la perte de la confidentialité, a fait craindre que les principes des législations nationale et internationale et les biens personnels et collectifs courent un grave danger. Le nombre croissant d'atteintes portées aux droits humains sous-jacents constituent désormais, et à juste titre, un problème mondial, et la définition de règles et de limites destinées à enrayer cette tendance, en apparence irréversible, nécessite que des mesures soient prises à l'échelle internationale.

Un premier pas important vers la mise en place des politiques nécessaires a été franchi par l'Assemblée générale des Nations Unies dans la Résolution A/RES/68/167, adoptée sans vote le 18 décembre 2013 et intitulée "Le droit à la vie privée à l'ère du numérique"; cette résolution rend compte de la volonté de la communauté internationale de prendre des mesures contre la surveillance, l'interception et la collecte de données personnelles à grande échelle. En application du paragraphe 5 du dispositif de ladite

Résolution, le Haut-Commissariat des Nations Unies aux droits de l'homme a présenté un rapport en juin 2014 (A/HRC/27/37) qui a fait l'objet d'un débat au sein du Conseil des droits de l'homme, à sa vingt-septième session, et devrait être examiné par l'Assemblée générale à sa soixante-neuvième session, les vues et recommandations proposées devant être examinées par les Etats Membres. Le rapport énonce de manière parfaitement claire les prescriptions qui doivent être respectées sur le plan des droits humains dans le cadre des mesures de surveillance étatique: ces mesures doivent être nécessaires et proportionnelles, transparentes et conformes aux droits au respect de la vie privée des personnes se trouvant à l'étranger. Les auteurs du rapport indiquent clairement qu'ils n'estiment pas que ces prescriptions soient respectées à l'heure actuelle.

Dans l'attente de résultats concrets de ces procédures mondiales et en dépit des besoins et de perspectives communs à l'humanité tout entière, on observe des différences régionales révélatrices de la façon dont les pays et leurs habitants réagissent face aux révélations et aux cas d'intrusion dans les domaines de la vie privée numérique, de la souveraineté nationale et de la protection des données (dans le cadre d'un large débat public initié par l'affaire Snowden).

Dans certaines régions du monde, on observe davantage de résignation que de révolte, voire de l'indifférence; dans un grand nombre des pays les plus puissants, les systèmes politiques au pouvoir font taire les voix au sein de la société qui rejettent cet état de fait; aux Etats-Unis, la conscience des besoins présumés ou réels en matière de sécurité publique est nettement plus grande, et le système juridique est plus clément. En revanche, en Europe et principalement au sein de l'Union européenne, les révélations et l'ampleur considérable des vols de données obtenues illégalement ont suscité une vive indignation et un profond rejet. Un véritable mouvement de fond politique a vu le jour et il serait malavisé de le sous-estimer, ne serait-ce qu'en raison de la perte collective de confiance des deux côtés de l'Atlantique, une cyberconfiance qui prévalait jusqu'alors. Les relations étroites et pérennes entre les démocraties européennes et les Etats-Unis, sous-tendues par un lien affectif très fort, en sont incontestablement affectées.

Ce sentiment collectif en Europe témoigne d'un profond attachement à la liberté et au respect de la vie privée, un attachement sans aucun doute fortement amplifié par l'histoire récente marquée par des dictatures et par la négation de la confidentialité (des souvenirs toujours très présents dans les mémoires) mais aussi par l'état très avancé de protection des données et de libertés du citoyen, et par la nature même de l'Union européenne en tant qu'entité juridique. La peur d'un "Big Brother" tout puissant, d'un Léviathan qui ne serait limité par aucune loi, est bien plus présente en Europe que partout ailleurs, bien qu'il serait erroné de sous-estimer l'indignation collective qu'éprouvent également les Américains à l'égard de la surveillance étatique à grande

échelle. Cette polémique jouera certainement un rôle central lors des prochaines élections présidentielles.

Néanmoins, si nous entendons définir des critères à l'échelle mondiale pour préserver la cyberconfiance à une époque où les moyens techniques d'intrusion ne connaissent aucune limite, il serait utile de se pencher sur la situation de l'Union européenne et sur son cadre juridique; en effet, cela pourrait contribuer à l'établissement d'un pilier important d'un cadre réglementaire universel.

Cette situation tient notamment à ce que l'UE constitue une communauté de droit regroupant 28 pays hautement industrialisés qui jouent un rôle majeur dans l'économie numérique mondiale, et dans lesquels les technologies numériques constituent désormais et plus que nulle part ailleurs le modèle de l'économie et de la société; aujourd'hui encore, l'UE est le bloc économique le plus important. De ce fait, les pays de l'UE sont proportionnellement plus exposés aux cyberattaques qu'un grand nombre de pays; McAfee a indiqué qu'en Allemagne par exemple, les dommages résultant de cyberattaques représentaient 1,65% de son PNB, soit le taux le plus haut parmi tous les pays industrialisés. A une époque où les groupes de cybercriminels sont l'un des principaux responsables de dommages dans les économies fortement tributaires de l'Internet et ouvertes, et où les services d'espionnage étrangers s'en donnent à coeur joie, la cybercriminalité est désormais une triste réalité en Europe. Cette situation a poussé l'Union européenne à mettre en place un système de cybersécurité collectif et uniformisé hautement perfectionné.

Par ailleurs, l'UE est à la fois une union constituée de 28 pays indépendants et une organisation dotée d'institutions communes et d'organes chargés de la définition de normes. La majeure partie des textes normatifs sont issus d'un travail mené conjointement par le Conseil européen – à l'initiative de la Commission européenne – et le Parlement européen. Les résolutions et décisions sont immédiatement exécutoires pour tous les Etats membres et pour toutes leurs régions, conformément aux directives relatives à la mise en oeuvre des objectifs adoptés. Ces résolutions et décisions doivent être transposées dans la législation nationale de chaque Etat membre, un processus unique dans le système international. Le socle institutionnel commun de la législation européenne a une force juridique immédiate pour les Etats membres et a également des incidences dans le monde entier. Aussi, l'UE peut constituer un exemple dont de nombreuses entités peuvent juger bon de s'inspirer, en tant que laboratoire institutionnel dans lequel un grand groupe de pays mettent à l'épreuve des décisions susceptibles d'être également mises en œuvre dans d'autres pays du monde. La législation européenne est un instrument interne de coordination et d'harmonisation contraignant, mais aussi un chemin vers une réglementation internationale.

En Europe, la cybersécurité et les politiques destinées à garantir la protection des données personnelles relèvent de la compétence des organes de l'Union européenne. S'agissant de la cybersécurité, la Commission européenne travaille à l'élaboration d'un

cadre réglementaire à l'intention de ses membres depuis plus d'une décennie. Toute une série de documents importants, pour une part analytiques et pour une autre part prescriptifs, ont donné lieu à un corpus complet de règles; ces règles sont obligatoires pour les Etats membres et n'ont aucun équivalent, tant en ce qui concerne leur portée que leur précision, dans la législation relative au domaine numérique des autres pays du monde, à l'exception des Etats-Unis. En outre, en 2004, les 28 Etats membres ont créé l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), qui fait office de groupe de réflexion commun et de coordonnateur chargé d'activités conjointes importantes de l'UE, et encourage la mise en place de plus amples mesures réglementaires. Il convient également de mentionner le Centre européen de lutte contre la cybercriminalité, rattaché à Europol, et l'équipe CERT européenne qui fait office de point central de contact et d'action en cas de cyberattaque. Il nous est impossible ici de passer en revue tout l'éventail d'activités que mène l'UE dans le domaine de la cybersécurité, tant sur le plan juridique qu'institutionnel, mais le site web de l'ENISA présente une vue d'ensemble de ces activités et donne accès à d'autres analyses[169]. L'UE accorde une très grande importance à sa Stratégie numérique et à l'optimisation de la cybersécurité. La Stratégie de cybersécurité de l'Union européenne[170] et le Projet de directive concernant la sécurité des réseaux et de l'information (Directive SRI)[171] sont deux documents complets adoptés récemment et qui contiennent des normes plus anciennes qu'il serait bon d'étudier. Ces deux documents, et plus particulièrement la Directive SRI, énoncent des prescriptions, des normes et des obligations très complètes à l'intention du secteur privé et des CERT ainsi que des opérateurs d'infrastructures, de réseaux et de systèmes d'information essentiels.

Dans notre contexte, l'élément pertinent est le fait que l'UE constitue un territoire sur lequel la législation en matière de cybersécurité est harmonisée. Sur les 28 pays que compte l'UE, 23 ont transposé la Convention de Budapest sur la cybercriminalité dans leur législation nationale (les autres pays en feront certainement de même prochainement) et tous ont incorporé la Décision-cadre (analogue) de 2002[172] dans leur législation. La cybercriminalité ainsi que toute intrusion dans des dispositifs numériques et des réseaux sont donc sanctionnées de la même manière dans tous les pays de l'UE,

---

169 www.enisa.europa.eu. Voir aussi Henning Wegener, *La ciberseguridad en la Unión Europea,* http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf. Une version en allemand est également disponible à l'adresse www.unibw.de/infosecur.

170 JOIN/2013/01 final.

171 COM/2013/048 final.

172 COM/2002/173 final.

et les procédures visant à faire appliquer la loi peuvent suivre leur cours dans l'un quelconque des pays de l'Union.

La protection des données constitue un autre volet important de la politique de l'UE dans le domaine du numérique. La protection des informations personnelles et de la vie privée des individus ont véritablement pris tout leur sens avec le développement du stockage numérique de données. La législation européenne applicable a une portée très vaste. Le fondement juridique est toujours la Directive 95/46/CE du Parlement européen et du Conseil, qui énonce des normes de protection minimum et que tous les membres de l'UE ont depuis transposé dans leur législation nationale respective. Cette directive s'applique aux données personnelles des individus. L'utilisation des données est considérée comme légitime si la personne concernée a donné son consentement exprès, ou dans d'autres circonstances définies très précisément. Les restrictions s'appliquent également dans une certaine mesure aux utilisateurs de données situés en dehors de l'Union[173].

En 2010, la Commission européenne a engagé un projet législatif plus ambitieux afin d'adapter les normes existantes en matière de protection des données à la situation actuelle[174]. Le projet de Règlement général sur la protection des données (GDPR) vise à rendre compte des besoins d'une société de l'information avancée caractérisée par des flux de données, des moyens de stockage en nuage et des réseaux sociaux qui se sont considérablement accrus et une connectivité qui connaît une croissance exponentielle. En cas d'adoption, ce nouveau règlement aura immédiatement force obligatoire dans tous les Etats membres et constituera un corpus de règles européennes harmonisées, contenant notamment un ensemble unique de règles précises pour les 28 Etats membres. Ce règlement est plus strict et plus précis que la directive de 1995 et prévoit de lourdes amendes en cas d'infraction. Le projet de texte a été adopté par le Parlement européen en mars 2014 et est actuellement examiné par les gouvernements en vue de le soumettre au Conseil de l'Europe. La version définitive de ce règlement est attendue ces prochains mois et elle entrera en vigueur en 2016. Néanmoins, ce règlement produit déjà des effets par anticipation puisqu'il révèle que l'UE s'oriente vers un régime très strict dans le domaine des données.

Après ce bref passage en revue de la législation européenne existante et en cours d'élaboration, qui forme un tissu législatif cohérent, nous pouvons à présent revenir au problème de la surveillance dans le cyberespace. Toute intrusion dans des supports de données numériques – ordinateurs, téléphones, réseaux ou autres dispositifs

---

173 Pour la plupart des Etats membres de l'UE, deux autres instruments internationaux sont également applicables: les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, et la convention du Conseil de l'Europe sur la protection des données qui a force obligatoire dans les 46 pays signataires.

174 COM/2012/011 final.

numériques – de même que la copie, le vol, la modification ou le transfert de données stockées constituent une cyberinfraction, en l'absence de justification précise. En cas d'intrusion dans des dispositifs numériques et des réseaux, et si des données personnelles sont concernées, cet acte constitue également une violation de la législation en matière de protection des données. La cybercriminalité et la manipulation de données personnelles sont donc étroitement liées, et il doit être fait appel aux deux corpus de prescriptions juridiques. La liberté sur l'Internet est en jeu dans les deux types de cyberdélinquance.

L'espionnage industriel ou politique sur l'Internet (ou sur le nuage ou d'autres supports de stockage), c'est-à-dire le vol ou la manipulation de faits politiques ou de données professionnelles ne contenant pas de données personnelles, n'est pas sanctionné dans le cadre du droit international. Il peut toutefois faire l'objet de sanctions dans les pays disposant d'une législation appropriée en vertu du droit pénal ou civil traditionnel, indépendamment de l'identité de l'auteur de l'infraction, qu'il s'agisse d'un individu, d'une entreprise, d'une institution ou d'un gouvernement étranger. Dans les pays de l'UE, la Convention de Budapest et/ou la législation nationale fournissent les outils nécessaires. Lorsque l'acte commis a des effets ou cause des dégâts à l'intérieur du territoire, le droit pénal s'applique même si l'acte a été perpétré en dehors des frontières nationales. En vertu de cette convention, les Etats membres sont tenus de sanctionner les actes de cybercriminalité commis sur leur territoire même si l'auteur de l'acte n'est pas résident du pays concerné[175]. Puisque les cyberinfractions peuvent avoir des répercussions à très vaste échelle, le droit en matière de cybercriminalité pourrait s'inscrire dans le cadre du droit pénal international, bien qu'il ne soit encore ni adopté ni appliqué dans tous les pays, en particulier dans les cas où l'Etat d'origine ne coopère pas ou est lui-même l'auteur de l'infraction. Si la surveillance et l'interception de données portent sur des données personnelles, les interdictions et sanctions prévues au titre de la législation en matière de protection des données s'appliquent en sus.

Un constat s'impose: l'intrusion actuelle à grande échelle dans l'espace numérique par des gouvernements, nationaux ou étrangers, et des entités privées soumis à la législation européenne, et dans tous les pays où une législation analogue existe, constitue une violation grave de la loi, à moins que cette intrusion soit justifiée par des motifs de sécurité publique ou des préoccupations d'ordre public et ait été autorisée en application de la législation nationale et des procédures juridiques en la matière, auquel cas l'intrusion devient donc légale. Par souci de précision, il convient de souligner que, en dépit de la pratique répandue à laquelle se livrent des pouvoirs publics, les cyberattaques commises à l'étranger ne peuvent aucunement être justifiées par des convictions nationales, des besoins subjectifs en matière de sécurité ou les procédures juridiques en vigueur au sein d'un gouvernement étranger si le gouvernement du pays

175 Voir le paragraphe 233 du Rapport explicatif sur la Convention sur la cybercriminalité.

dans lequel l'intrusion se produit ou qui en subit les conséquences n'a pas donné son consentement exprès. Dans l'UE, les actions menées conjointement par des membres de gouvernements sont fréquentes, et dont légales. Ces principes portent sur la surveillance à grande échelle de connexions Internet, de nœuds et de connexions hertziennes internationaux, etc. Ce point devient encore plus pertinent lorsque l'on prend en considération l'ampleur des collectes de données, qui serait illimitée, auxquelles procèdent des services de sécurité étrangers – dans une véritable course effrénée. Ces collectes de données bénéficient de prouesses et de moyens techniques sans précédent, mais sortent apparemment du cadre d'une évaluation pragmatique des risques et de justifications acceptables pour ce qui est de la sécurité, bien souvent sans égard pour les gouvernements des pays amis, de la protection des données, des droits humains, et des dégâts occasionnés[176].

Bien évidemment, il convient d'émettre plusieurs réserves concernant cette interprétation de la situation juridique, qui s'appliquent bien au-delà de l'UE. Premièrement, les cyberattaques, qui tirent avantage de l'anonymat de base sur l'Internet, sont difficiles à détecter. Du fait de la difficulté de déterminer la responsabilité de la cyberattaque, de remonter à sa source et d'identifier ses auteurs, l'application de la loi est dans de nombreux cas inutile ou tout du moins complexe. Dans les cas d'attaques visant des données qui sont commises depuis l'étranger, une autre difficulté s'ajoute pour intercepter l'auteur lorsque l'Etat d'origine ne coopère pas. Cette situation ne devrait bien évidemment pas empêcher de rétablir les faits sur le plan juridique. Deuxièmement, les gouvernements étrangers opèrent principalement sous le couvert de la souveraineté et de l'immunité diplomatique individuelle des auteurs des infractions; de nombreuses opérations de surveillance sont toutefois menées par des prestataires privés auxquels cette logique ne s'appliquerait pas. Néanmoins, l'impossibilité de poursuivre les auteurs en justice – il est possible en principe d'avoir recours uniquement aux procédures diplomatiques – ne change en rien la situation juridique sous-jacente. Dans les pays où le ministère public doit engager des poursuites d'office en cas de suspicion d'acte illicite criminel, comme c'est le cas dans la plupart des pays de l'UE, il y aurait une obligation d'engager des poursuites pénales même dans le cas où un accusé pourrait revendiquer son immunité. En Allemagne, des procédures pénales contre X sont en cours afin de traduire en justice les auteurs d'écoutes illégales réalisées sur le téléphone mobile de la chef du gouvernement. Afin d'assurer le bon déroulement de la justice, il serait souhaitable que de telles procédures deviennent plus fréquentes, voire qu'elles deviennent la règle.

Troisièmement, il serait probablement bienvenu d'élaborer – et de préférence dans un cadre international – une doctrine en ce qui concerne la surveillance numérique menée par des services de sécurité étatiques, nationaux ou étrangers, sans autorisation

176 Le rapport du Haut-Commissariat des Nations Unies aux droits de l'homme dont il est question plus haut énonce cette idée avec force.

préalable en cas notamment de "danger manifeste et actuel" ou de menace terroriste majeure et imminente, lorsque les criminels sont pris en fragrant délit ou en cas de crime majeur ou d'attaque majeurs et imminents visant des infrastructures essentielles. Il est toujours possible de délivrer une autorisation postérieure aux faits.

La révolte que l'on observe actuellement dans la plupart des pays d'Europe à l'encontre des intrusions et des opérations d'espionnage menées à grande échelle par des organismes des Etats-Unis – mais aussi par d'autres pays – semble quelque peu exagérée et volontairement amplifiée; aussi, avant de chercher à définir des critères raisonnables afin de distinguer le nécessaire du strictement inacceptable, il serait utile d'introduire un peu de réalisme dans le débat et de dédramatiser la situation[177].

Tout d'abord, il n'est pas possible de ne pas évoquer les avancées techniques sans précédent qui rendent possibles les intrusions dans les dispositifs numériques et les collectes de données à grande échelle, ainsi que le traitement de ces données grâce à de puissants outils de recherche. On ne peut pas condamner, sur le principe, l'utilisation de ces technologies dans le but de renforcer la sécurité nationale. Ces technologies ne peuvent pas disparaître du jour au lendemain, elles vont perdurer. De nouvelles technologies sont employées lorsqu'elles voient le jour et il est impossible de faire machine arrière.

Deuxièmement, les services de renseignement des pays de l'UE ont également eu recours à ces techniques, bien souvent en étroite coopération avec leurs homologues des Etats-Unis à des fins d'espionnage. La plupart d'entre eux, voire tous, emploient ces technologies dans le cadre des opérations qu'ils mènent non seulement à l'étranger, mais aussi sur leur propre territoire. Cela est particulièrement vrai dans le cas du Royaume-Uni, où les données et pratiques des Etats-Unis au titre du Programme PRISM sont utilisées sans les autorisations et le contrôle judiciaire requis. Il y est même fait recours en l'absence de suspicion concrète d'acte criminel et pour collecter un volume considérable de données aléatoires saisies par le biais d'un espionnage des communications sur les réseaux sociaux réalisé en mettant sur écoutes tous les câbles à fibres optiques déployés sur le territoire du Royaume-Uni ("Programme TEMPORA"). L'indignation vigoureuse manifestée dans de nombreux milieux européens à l'égard des pratiques des Etats-Unis est donc quelque peu teintée d'hypocrisie.

Troisièmement, les retombées positives des pratiques des Etats-Unis sur le plan de la sécurité dans le cadre de la lutte contre le terrorisme, le crime organisé et le blanchiment d'argent sont indéniables et, compte tenu de la supériorité technologique des services des Etats-Unis, nombreux sont les exemples qui indiquent que leurs alliés européens comptent parmi les principaux bénéficiaires.

---

177 Dans cette optique, voir également Nigel Inkster, *The Snowden Revelations: Myths and Misapprehensions,* SURVIVAL, février-mars 2014, p. 51; Joachim Krause, *Diskutieren statt moralisieren,* Internationale Politik, janvier-février 2014, p. 108.

De ce fait, il est légitime de remettre en question l'ampleur des mesures de surveillance, mais beaucoup moins la justification fondamentale qui les sous-tend. S'agissant de l'ampleur des mesures, seule une faible proportion des données que les services des Etats-Unis ont obtenues ou auxquelles ils ont accès est effectivement utilisée. D'après les chiffres de la NSA pour 2013, le volume du trafic quotidien de données sur l'Internet s'élève à 1 828 pétaoctets. La NSA ne peut saisir que 1,2% de ces données et ne peut en examiner qu'une faible proportion; ainsi, seul 0,0004% du trafic de données sur l'Internet serait passé au crible de certains filtres[178]. Il est important de remettre les choses en perspective.

Enfin, comme cela a été mentionné auparavant, un débat fructueux s'est engagé aux Etats-Unis. Ce pays n'a jamais été un bloc monolithique d'opinion mais est plutôt une démocratie dynamique dotée d'une capacité d'apprentissage intrinsèque. Il est tout à fait possible que les procédures menées actuellement aux Etats-Unis en vue de réexaminer les politiques et pratiques en matière de surveillance et de protection des données se traduisent en définitive par une embellie de la situation transatlantique. En janvier 2014 déjà, le Président Obama annonçait des mesures destinées à limiter les dégâts[179]. Ces mesures prévoient entre autres un contrôle administratif plus strict des opérations menées, parfois sans aucune limite, par les services de renseignement; la possibilité de collecter des données uniquement à des fins strictement de sécurité publique; le stockage de données relatives aux télécommunications principalement par le secteur privé, et la possibilité pour les services de renseignement d'avoir accès à ces données uniquement s'ils bénéficient d'une autorisation judiciaire.

Les arguments précédents, destinés à rééquilibrer le débat, ne visent aucunement à minimiser le problème de la collecte excessive et effrénée de données telle qu'elle a cours actuellement. Il ne fait aucun doute que, des deux côtés de l'Atlantique, la façon d'envisager la surveillance et la protection des données ainsi que les contraintes juridiques nécessaires est toujours très éloignée, ce qui tient en grande partie à des motifs d'ordre historique, aux traditions juridiques et au traumatisme de l'attaque terroriste de 2001. Des deux côtés de l'Atlantique, on ne considère pas de la même façon l'équilibre entre sécurité et liberté, et il est peu probable que cette différence de vues se réduise prochainement. Malgré le caractère douteux sur le plan juridique des pratiques d'espionnage et d'intrusion illégale et l'opprobre courant qu'elles suscitent, il est peu probable que ces pratiques disparaissent, bien qu'il importe que la dimension criminelle et les sanctions pénales qui leur sont associées apparaissent clairement.

---

178 Données de Joachim Krause, ibid. p. 114. Etant donné la source (la NSA) de ces chiffres, certains doutent de leur véracité; toutefois, même s'ils n'ont qu'une valeur indicative, ces chiffres montent que la NSA n'est pas en mesure de surveiller plus d'une fraction du trafic sur l'Internet, qu'elle met l'accent sur des données partielles pertinentes pour la sécurité, et qu'elle est loin de saisir la totalité des données circulant sur l'Internet.

179 "Presidential Policy Directive 28" (PPD 28), www.whitehouse.gov.

L'espionnage à l'encontre d'alliés est un sujet particulièrement sensible qui affecte les rapports de fraternité, les objectifs communs et même des liens personnels d'amitié, mais il a cours depuis très longtemps, même dans le contexte transatlantique. Cela étant, au-delà de la faute de protocole que cette pratique constitue et de la perte de confiance qu'elle entraîne, il est très peu probable que les alliés se précipitent pour conclure des accords officiels de "non-espionnage"[180]. Il serait bon que des accords informels soient signés.

Beaucoup de temps a été consacré à la recherche de solutions au dilemme de la surveillance, en particulier en ce qui concerne la relation entre l'UE et les Etats-Unis. Des débats sont en cours, au sein de la société et des pouvoirs publics, et il serait donc malavisé de prétendre donner des leçons en distillant des recommandations fermes et générales à l'intention de toutes les parties prenantes. Cette contribution s'achèvera plutôt sur quelques conseils très modestes.

S'agissant de l'UE, il importe d'établir prochainement sous leur forme définitive les instruments juridiques destinés à compléter les volets de la Stratégie numérique relatifs à la cybersécurité, le Projet de directive concernant la sécurité des réseaux et de l'information (Directive SRI) ainsi que le Règlement général sur la protection des données (GDPR), qui pourront servir de base pour tout accord futur qui serait conclu avec les Etats-Unis et d'autres pays.

Les Etats membres de l'UE doivent également veiller à ce que leurs propres services de renseignement observent scrupuleusement les législations européenne et nationale. Il serait insensé de demander davantage aux Etats-Unis qu'aux pays européens eux-mêmes. Les pays de l'UE devraient également conclure entre eux un accord mutuel de non-espionnage à l'échelle de l'Union et envisager de mettre en place progressivement un service de renseignement européen et un système de partage complet des informations entre les membres de l'Union. Dans l'intervalle, il conviendrait de renforcer encore la coordination entre les services de sécurité européens.

Les pays de l'UE doivent faire appliquer la législation nationale en matière de protection dans le cyberespace et de protection des données afin de montrer clairement où la loi se situe pour ce qui est des opérations de renseignement peu transparentes et d'espionnage.

Comme cela est démontré dans un précédent chapitre, la meilleure cyberdéfense repose sur une résilience accrue, pour ce qui est également d'éviter la collecte illégale de données et les attaques informatiques. Il est possible d'améliorer à bien des égards la résilience technique des systèmes et des réseaux ainsi que les moyens dont les utilisateurs disposent pour se protéger (grâce à une meilleure connaissance des

---

180 Voir Leif-Eric Easley, *Spying on Allies.* SURVIVAL, août-septembre 2014, p. 141; Rodri Jeffreys Jones, *Eine Frage der Etikette,* Internationale Politik, septembre-octobre 2014, p. 74.

mesures de sécurité, de meilleures pratiques en ce qui concerne l'économie de l'information et les sauvegardes, le cryptage, etc…). En d'autres termes, comme le dit le proverbe, charité bien ordonnée commence par soi-même.

Restaurer la cyberconfiance dans le contexte transatlantique sera difficile et ne portera ses fruits que dans le temps. Mais l'heure est venue de travailler à une approche transparente et commune de la façon dont un équilibre solide pourrait être trouvé entre le principe de liberté et les besoins en matière de sécurité, et la façon dont les activités des services de renseignement étatiques étrangers et la surveillance exercée par ces derniers peuvent être mises en conformité avec les dispositions de la législation de l'UE. Les agents de pays étrangers seront inévitablement jugés en fonction des normes du pays dans lequel ils opèrent. L'écart de points de vue de part et d'autre de l'Atlantique à cet égard ne s'atténuera peut-être pas prochainement, mais il devrait être réduit. L'UE ne peut pas dévier de ses normes élevées en matière de protection des données. Il conviendrait d'engager des travaux afin de réviser l'accord relatif à la sphère de sécurité (*Safe Harbour Agreement*) qui définit les conditions à respecter en ce qui concerne les transferts transfrontières de données, et la mise en œuvre irréprochable de ces conditions devraient commencer.

A l'issue de la vague actuelle d'intrusions dans les données, intrusions qui sont de l'avis général excessives, un nouvel esprit de proportionnalité et de mesure devrait prévaloir; le potentiel technique immense de saisie de données serait alors utilisé avec modération, dans le respect des intérêts touchés, y compris des droits humains, et des principes juridiques des pays dans lesquels les recherches se déroulent. Nous devons mettre en place une culture d'évaluation plus réaliste des besoins et de retenue.

A moyen terme, la perspective mondiale devrait prévaloir. L'UE devrait prendre part aux travaux visant à établir un cadre réglementaire international, dans la droite ligne de la Résolution A/RES/68/167 de l'Assemblée générale, et contribuer ainsi au respect d'un juste équilibre entre les intérêts communs en matière de sécurité et la liberté sur l'Internet.

3.5 Les limites de la cyberliberté: recherche de critères

Par William A. Barletta

Les techniques de télécommunication numériques, qui trouvent en particulier leur illustration dans l'Internet, ont engendré des bouleversements au sein de la société qui n'ont eu d'égal que l'arrivée de l'électricité dans les villes et villages il y a plus d'un siècle. Tout comme la distribution de l'électricité, les télécommunications numériques reposent sur des réseaux très étendus et interconnectés. Mais à la différence des réseaux électriques, qui ont une étendue régionale, l'Internet a une portée mondiale; il traverse les frontières nationales et transcende les différences culturelles. Tout comme

l'électricité, à laquelle n'ont pas accès près de deux milliards de personnes en situation de pauvreté énergétique, l'Internet compte une proportion comparable de personnes ayant un accès limité à l'information. Les réseaux électriques modernes permettent aux consommateurs d'émettre et de recevoir de l'énergie; quant aux utilisateurs de l'Internet, ils envoient et reçoivent couramment des informations, bien souvent dans une proportion égale.

Aussi, à l'image de l'analyse des réseaux énergétiques sur les plans juridique et politique, l'analyse des réseaux qui alimentent la société de l'information a généré ses propres conditions de justice distributive et d'impératifs moraux. La liberté[181] est l'une de ces conditions; de nombreuses personnes s'appuient sur ce principe et considèrent que la liberté sur l'Internet est un droit humain fondamental, tels que ces droits sont définis dans la Déclaration universelle des droits de l'homme des Nations Unies[182]. En particulier, l'article 19 de la Déclaration garantit le droit à la liberté d'expression:

"Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit."

Westby indique que[183] "Bien que la Déclaration universelle des droits de l'homme ne soit pas directement contraignante pour les Etats Membres de l'ONU, des parties de cette déclaration, y compris l'article 19, ont acquis une force juridique dans le cadre du droit coutumier international. Le libellé de l'Article 19 ("[…] de ne pas être inquiété […] de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées […]") correspond bien à la classification habituelle de la liberté sur l'Internet qui couvre également la liberté d'accès. Certains souhaiteraient élaborer davantage l'expression "de ne pas être inquiété" afin de couvrir le droit au respect de la vie privée, à l'anonymat, à la sécurité des données et même le droit de supprimer définitivement des contenus ayant été publiés sur l'Internet.

En vertu de l'article 19, l'*accès* à l'Internet peut être vu comme un facteur de mérite pour évaluer la liberté sur l'Internet. En outre, cet article donne à entendre les limites

---

181 La liberté sur l'Internet est considérée par certains comme une "expression factice" utilisée par les Etats-Unis et leurs alliés européens dans la lutte pour la gouvernance future de l'Internet. Voir "World War 3.0," Vanity Fair, mai 2012.

182 Résolution 217A (III) de l'Assemblée générale des Nations Unies, 10 décembre 1948, http://www.un.org/en/documents/udhr/.

183 J.R. Westby, The Role of Science and Technology as Empowerment of Person and State, Compte rendu de la 44ème session des Séminaires internationaux sur les situations d'urgence planétaires, 19-24 août 2011, Erice, Sicile.

en ce qui concerne les contenus (ou *utilisations*) et le degré d'interférence (respect de la vie privée et intégrité du contenu), qui constituent d'autres facteurs de mérite pour évaluer la liberté sur l'Internet. Freedom House, organisme international de surveillance, fait le point chaque année[184] sur la situation de la liberté sur l'Internet. Dans son rapport de 2013[185], il conclut que sur les soixante pays examinés, trente-quatre ont connu une évolution négative et seize ont connu une évolution positive depuis la mi-2012.

De telles évaluations peuvent être qualifiées de caractérisation du droit de ne pas être soumis à une répression, en particulier lorsque l'Internet est utilisé pour exprimer des revendications sociales, organiser des forces politiques d'opposition, ou simplement diffuser des informations pouvant être embarrassantes pour des personnes occupant une position importante au sein de la société. Les membres de ce groupe ont beaucoup écrit sur les sujets du renforcement des moyens d'action des citoyens via l'Internet et de la cyber-répression à cet égard[186]. Westby s'est exprimé clairement sur ce sujet, en indiquant que "Les intérêts de l'Etat-nation qui vont à l'encontre des droits des individus

---

184 Freedom House applique une méthode fondée sur trois piliers pour évaluer le niveau de liberté sur l'Internet et dans le secteur des TIC:

- Entraves à l'accès: y compris les obstacles sur le plan des infrastructures et les obstacles économiques, le contrôle exercé sur les fournisseurs de services Internet (ISP) en ce qui concerne les questions juridiques et la participation au capital, et l'indépendance des organismes de réglementation.
- Limites imposées sur les contenus: y compris la réglementation juridique visant les contenus, le filtrage et le blocage techniques de sites web, l'autocensure, le dynamisme/la diversité des médias d'information en ligne, et l'utilisation des TIC pour la mobilisation civique.
- Violations des droits des utilisateurs: y compris la surveillance, le respect de la vie privée et les répercussions que peuvent avoir les activités en ligne, notamment l'emprisonnement, le harcèlement ou les cyberattaques.

Les rapports de Freedom House sont disponibles à l'adresse http://www.freedomhouse.org/report-types/freedom-net#.VBB2dUhA140.

185 Freedom on the Net 2013, A Summary of Findings, p. 2. Disponible à l'adresse http://www.freedomhouse.org/report/freedom-net/freedom-net-2013#.VBB6CUhA140.

186 H. Wegener, "Cyber Repression: Going Worse. What can be done?", Compte rendu de la 44ème session des Séminaires internationaux sur les situations d'urgence planétaires, Erice, Sicile (2011): "Les conséquences de la censure à grande échelle – cyber-répression – sont graves et ne sauraient être sous-estimées. Les individus sont privés des avantages importants de l'ère de l'information et ont une vision fausse des réalités mondiales, qui les condamne à une immaturité politique. La cyber-répression à grande échelle peut modifier l'état d'esprit collectif d'une nation. La gravité de la suppression d'informations à grande échelle est égale à la gravité d'autres variantes de la cybercriminalité et des cyberconflits…".

se heurtent à ces derniers, et les TIC sont l'outil de choix pour que les deux camps affirment leur pouvoir"[187].

Ce qui se résume dans nos sociétés dites "libres" à un problème – certes complexe – d'équilibre politique à assurer en permanence entre liberté et intervention de l'Etat selon des critères juridiques précis devient dans un grand nombre d'autres Etats un problème de droits de l'homme et de qualité de l'ordre mondial de l'information. La censure de l'Internet qu'exercent des gouvernements, par l'intermédiaire de techniques de filtrage échappant à toute contrainte juridique et ayant de graves conséquences sur la recherche et la diffusion d'informations par les individus constitue une violation des droits de l'homme qui prend une dimension particulièrement importante[188].

Si cette tension est plus facilement dirigée à l'encontre des actions menées par des Etats-nations, l'absence de gouvernance centrale de l'Internet conjuguée à la structure grandement dispersée de ce dernier permet aux organisations non gouvernementales et à des sociétés de limiter de manière significative la liberté sur l'Internet dont jouissent certains groupes en particulier. L'Internet a renforcé les moyens d'action d'acteurs non étatiques de manière telle que les pouvoirs publics considèrent qu'il est intéressant d'imposer à des sociétés[189] de mener des activités de censure, de surveillance de l'utilisation, etc.

Un moyen de traiter la question de la liberté d'accès à l'échelle mondiale pourrait être envisagé dans les pays qui disposent d'entreprises produisant des technologies liées à l'Internet. Les pouvoirs publics de ces pays pourraient interdire l'exportation – ou tout du moins exiger que des rapports soient soumis à cet égard - de "[…] produits et de technologies susceptibles d'aider un gouvernement étranger à acquérir la capacité d'effectuer une censure, une surveillance ou toute autre activité connexe par l'intermédiaire de moyens de télécommunication, y compris l'Internet"[190]. Si l'efficacité de telles mesures est discutable, elles mettent en évidence la nature complémentaire des mesures prises par les Etats-nations et les différents secteurs de l'industrie afin de définir les limites de la liberté sur l'Internet.

Comme la plupart des indicateurs de conduite retardés, ces mesures négatives ne représentent qu'une partie de l'équation. Les actions qui font progresser le bien-être

---

187 Westby, op.cit.

188 Wegener, UIT 2011, p. 46.

189 "D'après des documents judiciaires rendus publics ce jeudi, en 2008, le Gouvernement des Etats-Unis a menacé d'infliger à Yahoo! une amende de 250 000$ par jour si la société n'honorait pas une demande assez large de données d'utilisateurs, que la société jugeait anticonstitutionnelle.", *U.S. threatened massive fine to force Yahoo to release data*, Washington Post, 11 septembre 2014.

190 Chambre des Représentants des Etats-Unis, H.R.3605 - Global Online Freedom Act (loi sur la liberté en ligne dans le monde), 2011.

social et économique au sein de la société sont tout aussi révélatrices, bien que plus difficiles à évaluer. Une gouvernance stricte menée avec l'objectif formulé clairement d'assurer la stabilité, la sécurité et la résilience des réseaux peut mettre un terme à l'inventivité, à l'apparition de nouveaux modèles de réseaux et à l'ouverture sur le plan de la technologie.

Dès lors, il n'y a rien d'étonnant à ce que les intérêts (collectifs) légitimes des Etats puissent se heurter aux intérêts des individus dans le cyberspace. Ces intérêts comprennent notamment, mais pas exclusivement, la protection des citoyens contre des menaces connues en vue de préserver les normes (culturelles) de la société, la prévention des crimes motivés par la haine[191] et du terrorisme, la prévention des perturbations au sein des infrastructures sociales essentielles (y compris l'Internet et d'autres infrastructures informatiques), la protection des secrets d'État légitimes, les mesures visant à faire connaître la politique étrangère d'un Etat, et la promotion du bien-être économique au sein d'un pays, en particulier en exerçant une influence sur les externalités. Bien que les règles de conduite relatives à la promotion d'intérêts contradictoires d'Etats soient bien élaborées en dehors du domaine du numérique, des difficultés majeures font surface dans le cyberespace en raison, d'une part, de l'absence de cadres juridiques harmonisés régissant la conduite dans le cyberespace et, d'autre part, des différences culturelles flagrantes qui sont le fruit de l'histoire et sont légion dans un réseau mondial qui transcende de nombreuses frontières nationales.

L'exemple suivant est assez significatif. De manière générale, les pays de l'UE interdisent fermement les contenus qu'ils définissent comme "incitation à la haine" ou les représentations du même ordre[192]. Ces interdictions trouvent leur origine dans la Seconde Guerre mondiale et les morts innombrables qu'elle a engendrées. Certains pays musulmans appliquent également des prescriptions fortes à l'égard du prosélytisme[193] ou de la diffusion de représentations blasphématoires, écrites ou graphiques, du prophète Mahomet. Dans les deux cas, ces prescriptions reflètent des normes culturelles fortes et leur violation peut engendrer un mouvement de discorde

---

191 La coopération policière internationale visant à éradiquer la pédopornographie est un exemple sur lequel tous les pays sont d'accord.

192 Par exemple, un tribunal français a ordonné à Yahoo! de retirer de son site de vente aux enchères du matériel ayant appartenu à des Nazis. Est-ce pire que le fait que la Chine ait forcé Yahoo! à signer un "engagement volontaire" à ne pas "produire, publier ou diffuser des informations dangereuses qui pourraient compromettre la sécurité de l'Etat et perturber sa stabilité sociale"? Christopher Bodeen, "Web Portals Sign China Content Pact," Associated Press, 15 juillet 2002.

193 Hillary Clinton, "Internet Freedom," http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom.

voire des actes de violence au sein de la société. Lorsque les pouvoirs publics bloquent de tels sites, s'agit-il de leur part d'une violation répressive de droits humains?
Les Etats-Unis quant à eux ont une vision assez large de ce qui relève du discours autorisé, une vision qui est entérinée dans leur Constitution. Lawrence Tribe, un juriste américain renommé, et un de ses collègues ont écrit[194]:

> "La parole est très puissante. C'est l'essence de la démocratie, une condition préalable à la découverte de la vérité, essentielle pour notre développement personnel. Mais la parole est aussi dangereuse. Elle peut corrompre la démocratie, permettre de commettre un crime ou inciter à le faire, encourager des ennemis, et interférer avec les pouvoirs publics. Elle peut faire office d'arme et être déployée à l'encontre de cibles innocentes."

Toutefois, même aux Etats-Unis, les limites imposées en ce qui concerne la liberté d'expression afin de lutter contre les incitations à la haine et la cyberintimidation deviennent de plus en plus courantes. Au sein de la société américaine, qui est prompte à intenter des actions en justice, ces limites ne constituent pas des restrictions à la liberté d'expression mais plutôt des motifs de sanctions pouvant aller jusqu'au pénal.

Les pouvoirs publics peuvent, en plus de bloquer matériellement l'accès à des sites, rendre leur accès beaucoup trop coûteux dans l'optique de restreindre nettement l'accès sur la base de considérations politiques. Par exemple, la surveillance de sites contenant des contenus "dangereux", provocants ou illégaux afin d'identifier des visiteurs et de restreindre leur accès à ces sites peut être suivie de l'application de procédures secrètes visant les libertés des personnes qui visitent ces sites. De nombreuses personnes ont été inscrites sur des listes de personnes interdites de vol en raison d'une surveillance incorrecte de sites "terroristes". Bien qu'il soit facile d'admettre que de tels programmes de surveillance répondent à des impératifs pour les Etats, l'absence de procédures judiciaires ouvertes visant à établir un équilibre entre les intérêts individuels et les intérêts des Etats est troublante.

Les politiques relatives à l'anonymat et au respect de la vie privée sont la cause de nombreux désaccords entre les pays. Un grand nombre d'entre eux considèrent que l'anonymat dans les communications sur l'Internet est un droit. Du fait que l'anonymat puisse protéger la personne contre tout harcèlement et toutes représailles, ce principe est vu comme une composante essentielle de la liberté d'expression. En effet, les Etats-Unis reconnaissent[195] un droit à la conduite de campagnes politiques de manière anonyme; ils ont également affirmé le droit des personnes d'avoir des interactions

---

194 Lawrence Tribe et Joshua Matz, Uncertain Justice, (New York, 2014) p.123.

195 Cour suprême des Etats-Unis, McIntyre v. Ohio Elections Commission (93-986), 514 U.S. 334 (1995).

anonymes "pour autant que ces actes ne constituent pas une violation de la loi" [196]. Néanmoins, les Etats-Unis n'ont pas adopté de politiques générales concernant l'anonymat et le droit au respect de la vie privée sur l'Internet, préférant introduire une réglementation pour des secteurs donnés. De façon plus résolue, l'UE a choisi de réglementer directement les droits des individus au respect de la vie privée et à l'anonymat.

En revanche, l'anonymat peut être un rempart commode pour les auteurs d'actes perturbateurs et criminels. Parmi les restrictions imposées en vue de renforcer le contrôle de l'utilisation de l'Internet, la Russie a interdit l'accès anonyme aux réseaux WiFi dans les lieux publics[197] lorsque le numéro IP ne peut pas être lié de manière définitive à des individus précis. En outre, comme le montrent les révélations d'Edward Snowden, le gouvernement des Etats-Unis a mis l'accent sur une prérogative extrêmement large (et peut-être illimitée) de surveiller les communications sur l'Internet. Et les pouvoirs publics ne sont pas les seuls à surveiller l'utilisation de l'Internet, de grandes sociétés telles que Google font de même. Aussi, il n'y a rien d'étonnant à ce que différents utilisateurs aient donc une expérience sur mesure (ou ciblée) de l'Internet, qu'ils le veuillent ou non.

L'utilisation à grande échelle par les Etats-Unis des opérations de surveillance, y compris des communications de chefs d'Etats d'amis, telles qu'elles ont été révélées par Edward Snowden, donne à penser que peu de télécommunications sont véritablement privées, si ce n'est aucune. Il est à déplorer que les débats publics au sujet de l'étendue, des motifs et des composantes des activités de surveillance menées par les pouvoirs publics soient généralement à l'abri d'un contrôle juridictionnel en vertu du secret d'Etat[198]. Les arguments avancés par le gouvernement des Etats-Unis, selon lesquels "tout le monde le fait", ne sont en rien rassurants. En effet, compte tenu de l'expansion considérable des capacités des ordinateurs et de la capacité de stockage par coût unitaire, presque tous les pays industrialisés peuvent surveiller tout le trafic Internet entrant dans un pays ou sortant de celui-ci. Pour les pays les plus avancés sur le plan

---

196 Décision du Tribunal du District nord de la Californie dans l'affaire *Columbia Insurance Company contre Seescandy.com, et al.*

197 "Medvedev signs order banning anonymous Wi-Fi," http://en.itar-tass.com/russia/744055, 8 août 2014.

198 Le privilège du secret d'Etat("State Secret Privilege") est une règle juridique relative à l'usage des preuves aux Etats-Unis, créée par la règle du précédent. Elle consiste à écarter des preuves sur la base uniquement d'un affidavit soumis par les pouvoirs publics, affirmant que l'examen judiciaire de ces preuves risquerait d'entraîner la divulgation d'informations sensibles susceptibles de mettre en péril la sécurité nationale. Le cas *United States v. Reynolds*, qui impliquait des secrets militaires, est la première affaire lors de laquelle la Cour a formellement reconnu cette règle. Voir http://fr.wikipedia.org/wiki/Privil%C3%A8ge_de_secret_d%27%C3%89tat.

économique, la surveillance à grande échelle de l'ensemble du trafic est possible avec la complicité (forcée ou volontaire) des fournisseurs de services de télécommunication.

L'ampleur de la réaction publique aux Etats-Unis et en Europe face aux révélations de surveillance de la quasi-totalité du trafic mobile a poussé Apple à doter son dernier système d'exploitation mobile (iOS8) d'un système de cryptage fort sans porte dérobée. Aussi, pas même Apple n'est en mesure de décrypter un téléphone sur injonction d'un tribunal[199]. Si les détracteurs d'Apple insistent sur le fait que le système d'exploitation iOS8 "n'empêche que les enquêtes légales menées avec des mandats en bonne et due forme"[200], ses défenseurs avancent que l'entreprise "met au point des systèmes qui empêchent toute personne souhaitant obtenir des données, y compris des pirates, des initiés malveillants, et même des gouvernements étrangers hostiles, d'avoir accès aux téléphones. Cette démarche est absolument dans l'intérêt public. Ce faisant, Apple établit également un précédent selon lequel les utilisateurs, et *non* les entreprises, doivent rester maîtres de leurs propres appareils[201]." Il reste à voir quelle sera la réponse officielle du gouvernement des Etats-Unis; néanmoins, plusieurs personnalités officielles ont critiqué[202] la démarche d'Apple. Il n'aurait rien de surprenant à ce qu'une réponse officielle qui relèverait davantage de la contrainte que de la persuasion morale soit donnée.

Par le passé, les Etats-Unis ont déjà cherché à imposer des contraintes aux fabricants de matériel afin de permettre la localisation, de divulguer l'identité d'utilisateurs, et de décrypter le trafic Internet. La Secrétaire d'Etat, Madame Hillary Clinton, expliquant la

---

199 Politique d'Apple en matière de confidentialité: "Quand un gouvernement nous demande des informations, nous ne manquons pas pour autant à nos principes et à nos engagements de respect de la confidentialité de nos clients." https://www.apple.com/chfr/privacy/government-information-requests/. Voir aussi Matthew Green, "Is Apple picking a fight with the US government," Slate, 23 septembre 2014. Disponible à l'adresse http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html.

200 Oren Kerr, dans son article "Apple's dangerous game," (http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/Kerr) a quelque peu modifié les opinions qu'il avait exprimées et a reconnu qu'un système doté d'une porte dérobée en ce qui concerne le cryptage est susceptible d'être piraté, ce qui compromet donc la sécurité du système dans son ensemble.

201 Matthew Green, Ibid.

202 Lors d'un entretien réalisé dans le cadre de la nouvelle émission de CBS "60 minutes" le 12 octobre 2014, le directeur du FBI, James Carney, a accusé Apple de protéger, par ses nouveaux paramètres de confidentialité, les ravisseurs, les pédophiles et les terroristes. Voir http://money.cnn.com/2014/10/13/technology/security/fbi-apple/index.html?hpt=hp_t2.

façon dont le Département d'État des Etats-Unis procède pour "protéger et défendre un Internet libre et ouvert" dans le cadre de sa politique[203], a indiqué ce qui suit[204]:

> "Toutes les sociétés reconnaissent que la libre expression a des limites. Nous ne tolèrerons pas ceux qui incitent d'autres personnes à avoir recours à la violence, tels que les agents d'Al-Qaida qui, en ce moment-même, utilisent l'Internet pour appeler au massacre d'innocents. De même, les discours de haine qui visent des personnes sur la base de leur origine, de leur genre ou de leur orientation sexuelle sont répréhensibles. Il est à déplorer que ces questions constituent des problèmes auxquels la communauté internationale est de plus en plus confrontée, et qu'elle doit traiter de manière unie. Nous devons également traiter la question de la parole anonyme. Ceux qui utilisent l'Internet pour recruter des terroristes ou diffuser des contenus protégés par la propriété intellectuelle volés ne peuvent pas opérer de clivage entre leurs activités en ligne et leur identité dans la vraie vie."

Et pourtant, dans le même temps, le FBI a averti des propriétaires de cafés Internet aux Etats-Unis "[…] que l'utilisation de certaines mesures élémentaires de cybersécurité pourrait être considérée comme des motifs de suspicion d'activité terroriste potentielle"[205].

Les pays développés sont eux aussi le théâtre de tensions similaires entre les intérêts individuels et les intérêts des Etats, tandis que dans les pays industrialisés, la cryptographie est perçue comme une arme dont peuvent faire usage les citoyens respectueux de la loi autant que des terroristes.

Sur le continent africain, seuls des pays d'Afrique du Nord comme l'Algérie, l'Egypte, le Maroc et la Tunisie, ainsi que le Nigéria et l'Afrique du Sud semblent disposer d'une législation portant spécifiquement sur le cryptage. Sur ce continent, l'Afrique du Sud joue un rôle de premier plan en ce qui concerne la législation relative à la cryptographie, mais la déontologie de la principale législation du pays en matière de divulgation est contestée par certains fervents défenseurs des droits humains. Pour certains, la cryptographie semble être la seule solution dans la lutte contre les menaces qui pèsent

---

203 Département d'Etat des Etats-Unis, "International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World," http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

204 Clinton, op. cit.

205 Vanity Fair, op. cit.

sur la confidentialité, à mesure que la société s'adapte à la numérisation des réseaux mondiaux[206].

La cryptographie symétrique forte qui existe actuellement, comme la norme OpenPGP, est à la disposition de toute personne qui ne réside pas dans un Etat soutenant des terroristes, tels que ces pays sont définis par le Département d'État des Etats-Unis. Il est difficile de concevoir que cette restriction dissuadera à long terme les cellules terroristes. Il est tout aussi difficile d'imaginer que les partisans de la cryptographie militaire verront un jour des propositions visant la "mise en dépôt volontaire de clés" déposées auprès des autorités judiciaires de leur gouvernement d'origine[207].

Le risque de conflits entre différents gouvernements protégeant ce qu'ils considèrent être les intérêts légitimes de leurs ressortissants est manifeste. Néanmoins, précisément lorsque les actes perçus comme des infractions traversent de multiples frontières nationales, l'Etat lésé dispose de peu de moyens pour obtenir des réparations, si ce n'est de bloquer l'adresse de Protocole Internet (IP) concernée. L'absence de cadre juridique harmonisé régissant la conduite dans le cyberespace est un sérieux obstacle. Même lorsque l'acte commis dans le cyberespace est considéré

206 Cory Farmer et Judson L. Jeffries, "Telecommunications Surveillance and Cryptography Regulatory Policy in Africa," African Policy Journal, mai 2013. Disponible à l'adresse http://apj.fas.harvard.edu/category/articles/.

207 "Dans ce cas de figure, des copies de clés secrètes seraient mises en dépôt dans un état d'inactivité et protégées par plusieurs couches de sécurité, et seules les entités disposant des autorisations nécessaires et de directives de décryptage pourraient y accéder". Cory Farmer et Judson L. Jeffries, Ibid, p.3.

comme un crime grave dans le pays de la victime présumée, l'auteur présumé peut être hors de portée de la loi[208].

Lorsque les intérêts des citoyens sont formulés en termes de droits humains plutôt que dans le cadre d'un équilibre à trouver entre des intérêts légitimes divergents, les enjeux, à la fois pour les personnes et la société, sont très élevés. Vint Cerf[209], ingénieur et pionnier de l'Internet, a fait observer ce qui suit:

"[…] la technologie est au service des droits, elle n'est pas un droit en elle-même. Pour qu'un principe puisse être considéré comme un droit humain, il doit satisfaire à des critères très élevés. Dans les grandes lignes, il doit figurer parmi les éléments dont les êtres humains ont besoin pour pouvoir mener une vie saine et ayant un sens, comme le droit de ne pas être soumis à la torture ou la liberté de conscience. Il est erroné de placer une technologie quelconque dans cette catégorie magnifiée, car avec le temps, nous finirons par attribuer de la valeur à des concepts à tort"[210].

Malheureusement, le fait de qualifier la liberté d'accès à l'Internet de droit humain laisse le champ libre, dans le débat politique, pour imposer l'idéologie sur le bon sens. Qu'il s'agisse de "neutralité de l'Internet" ou d'"accès ouvert" aux publications, la largeur de bande et le traitement du contenu ont un coût. Trop souvent, des idéologues ont cherché à garantir la "neutralité" et l'"accès" sans que le moindre financement soit accordé, en partant du principe que "quelqu'un d'autre – habituellement l'éditeur –

---

208 Pour qu'un pays puisse enquêter et engager des poursuites judiciaires, les autorités du pays concerné chargées de faire respecter la loi doivent pouvoir collecter des informations et des preuves dans d'autres pays. L'obstacle fondamental dans le cadre des enquêtes portant sur des preuves et des suspects situés dans différents pays est la nécessité pour les autorités concernées de respecter la souveraineté d'autres pays. Généralement, les autorités chargées de faire respecter la loi d'un pays donné ne peuvent entrer dans un autre pays pour examiner différentes pistes, collecter des preuves et arrêter des suspects. De ce fait, les enquêtes internationales nécessitent la coopération et l'assistance des autorités des pays dans lesquels les victimes, les preuves et les suspects sont situés. Même lorsque des suspects ont été identifiés, certains pays n'autorisent généralement pas l'extradition de leurs ressortissants et font valoir qu'il convient plutôt de mener des poursuites judiciaires au niveau national, en invoquant souvent le fait que l'extradition est incompatible avec leur cadre juridictionnel, qu'elle constituerait une atteinte aux protections individuelles garanties à leurs ressortissants et entraînerait des obstacles supplémentaires en ce qui concerne les preuves lors du jugement. Des procureurs ont quant à eux établi que les pays qui refusent d'extrader leurs ressortissants n'engagent pas par la suite de procédures judiciaires au niveau national. G. A. Barletta, private communication, 201.

209 Considéré de manière générale comme l'un des "pères de l'Internet".

210 V. Cerf, "Internet Access is Not a Human Right", New York Times, 4 janvier 2012.

paiera", un argument[211] régulièrement avancé pour garantir la liberté de l'Internet. Il n'en reste pas moins que l'accès généralisé et la réduction au minimum des obstacles sur le plan des infrastructures sont des objectifs souhaitables qui peuvent être atteints dans le cadre de nombreux modèles d'activité différents.

Le secteur privé a joué un rôle de premier plan dans la création et la gouvernance de la société numérique. La liberté d'action sur l'Internet que l'on connaît actuellement est en grande partie due aux idées du secteur privé. Si les sociétés subissent des pressions de la part des pouvoirs publics qui tentent de les contraindre à apporter leur concours à l'application de mesure répressives, elles ont également formé de vastes alliances avec des groupes de défense des droits humains, des universitaires, des investisseurs et des organisations de la société civile pour faire front contre ces pressions. A cet égard, il convient de souligner les actions menées par la Global Network Initiative (GNI)[212]. La GNI a présenté sa conception[213] du rôle de la "liberté d'expression et des facteurs de risque pour la confidentialité" relatifs au secteur privé. Elle a fait observer que de nouvelles technologies (qu'il s'agisse de matériel ou de logiciels) et de nouveaux produits voient le jour rapidement. Ces produits présentent de nouveaux risques et offrent de nouvelles possibilités pour ce qui est de la liberté sur l'Internet. Bien que le secteur privé n'exerce qu'un contrôle limité sur les actions entreprises par les utilisateurs finals de la technologie, il peut donner aux fournisseurs de service de télécommunication les avis les plus poussés du point de vue technologique en vue de réduire au minimum les menaces naissantes pour la liberté sur l'Internet.

Ces dernières années, le secteur des TIC s'est employé de plus en plus énergiquement à définir des moyens de protéger la liberté d'expression et le droit au respect de la vie privée. A titre d'exemple, la GNI fournit à des entreprises des directives et des orientations sur la manière de donner suite à une demande des pouvoirs publics de supprimer, filtrer ou bloquer du contenu, ou à une demande émanant d'organismes chargés de faire respecter la loi et visant à ce que des informations personnelles soient divulguées. Ces types de facteurs de risques sont importants pour les entreprises qui stockent des volumes conséquents d'informations personnelles et sont les gardiens de l'accès à des contenus, en premier lieu les fournisseurs de services de télécommunication et de services Internet.

Il est à prévoir que, à mesure que l'on dotera le matériel d'une forte sécurité paramétrée au niveau du circuit intégré, les pouvoirs publics exerceront des pressions de plus en fortes à l'encontre des fabricants afin de disposer d'un accès par porte dérobée

---

211 Voir par exemple le court documentaire "A Threat to Internet Freedom" réalisé par B. Knappenburger, New York Times, 9 juillet 2014.

212 https://globalnetworkinitiative.org/.

213 D.A. Hope, "Protecting Human Rights in the Digital Age," février 2011, http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf.

(organismes chargés de faire respecter le droit et services de renseignement) à des fins de surveillance, y compris d'individus, de détermination de l'origine d'actions menées sur l'Internet et de collecte de preuves en vue de procédures judiciaires. Perspective plus inquiétante encore, des produits pourraient être mis au point et configurés de sorte qu'il soit possible d'opérer une censure et des restrictions de contenus au niveau du circuit intégré. Bien que les entreprises soient au centre des pressions visant à limiter la liberté, elles sont aussi les mieux informées et sont dans la position la plus avantageuse pour contrecarrer de telles pressions.

La réaction rapide du secteur privé face à la multiplication des menaces qui pèsent sur la sécurité des TIC et des informations qu'elles génèrent, transmettent, reçoivent et stockent est une protection cruciale pour le droit des individus et des institutions d'utiliser les informations numériques librement. Ce droit nécessite la confiance des utilisateurs finals à l'égard des droits de propriété[214] et d'utilisateur[215] sur les données, ainsi qu'à l'égard de la crédibilité[216] et de la confidentialité des données[217]. Certaines personnes souhaiteraient également inclure dans cette liste la possibilité de supprimer des données de l'Internet et de mettre en place des protections juridiques contre les contraintes exercées dans le but de forcer des entités à révéler les mots de passe de sites personnels, sauf s'il s'agit d'appliquer une décision juridique. Les menaces à la liberté d'utiliser des contenus émanent de toute une série d'acteurs, allant des pirates individuels aux groupes de criminels en passant par des groupes appuyés par des Etats.

---

214 Les propriétaires [présumés] d'informations demandent souvent la protection juridique des droits à l'égard de la diffusion et de l'utilisation de leurs informations. Le propriétaire peut définir les critères ou même le contrôle de l'accès à l'information. Ces critères peuvent comprendre le droit de diffusion par l'utilisateur autorisé (ou l'organisation utilisatrice autorisée). Ce contrôle correspond à la pratique pour ce qui est des informations touchant à la sécurité de l'Etat, les secrets commerciaux, et les informations personnelles confidentielles. Les attaques indirectes [et légalistes] visant des droits de propriété peuvent réduire l'utilité de l'information à tel point qu'il pas parfois plus possible de s'en servir.

215 Le propriétaire de l'information peut définir les critères d'utilisation de l'information ou même de contrôle de l'accès à l'information. Ce contrôle est normal lorsque l'information est considérée comme étant protégée juridiquement par la propriété intellectuelle.

216 L'utilisateur des données devrait (et peut être tenu juridiquement de le faire) évaluer (et peut-être étayer par des documents) son degré de confiance à l'égard de l'entité ayant généré l'information et la source (le fournisseur) de l'information, ainsi que les incertitudes effectives concernant le contenu des données (notamment des mesures, des enregistrements de transactions, des statistiques…). Les attaques à l'encontre de la crédibilité de l'information visent à réduire l'utilité des données et à saper la confiance des parties prenantes à l'égard de la compétence des parties (et des institutions) qui utilisent les données concernées.

217 Un point que les utilisateurs jugent particulièrement important pour ce qui est des informations d'identification personnelle spécifiques.

La garantie du respect de la liberté personnelle sur une infrastructure Internet résiliente et sûre ne sera pas le fruit du hasard. Des mesures positives doivent être prises pour concilier les intérêts des Etats et ceux des individus et du secteur privé, tout en protégeant l'ensemble des utilisateurs contre les acteurs malveillants. Le type de mesures que les Etats devront prendre pourra varier d'une société à une autre.

Dans les pays occidentaux, l'on pourrait s'attendre à un recours central au contrôle juridictionnel – confidentiel[218] ou non – afin de statuer sur des cas individuels plutôt que d'autoriser la surveillance à grande échelle par des organismes chargés de faire respecter le droit et par des services de renseignement. La participation active du secteur privé – à la fois des fabricants de matériel et des concepteurs de logiciels – permettrait d'accroître les niveaux de sécurité et de confidentialité pour les utilisateurs. De concert, les fournisseurs de services Internet gèreraient de manière confidentielle la saisie et le stockage sur le long terme des données d'utilisateurs susceptibles d'être contrôlées par les pouvoirs publics uniquement dans des conditions clairement définies et transparentes. Il conviendrait qu'une règle de proportionnalité soit établie, que la course effrénée à l'intrusion dans les réseaux et à la collecte de données à laquelle se livrent des pouvoirs publics cesse, et qu'une coopération intergouvernementale soit mise en place afin de définir les conditions des espionnages à l'égard d'alliés et de conclure des accords à l'image de l'accord relatif à la sphère de sécurité[219]. Le cadre juridique effectif devrait être le résultat d'une législation éclairée par un débat public véritable et ouvert et par des consultations avec des alliés et des organismes internationaux.

La Chine a quant à elle construit son propre Internet national:

> "Le régime autoritaire chinois a non seulement survécu à l'Internet, mais il a aussi fait preuve d'une grande maîtrise pour détourner la technologie à ses propres fins, ce qui lui a permis de mieux contrôler la société chinoise et de donner l'exemple à d'autres régimes répressifs. Le Parti de l'Etat chinois a déployé une armée de cyberpoliciers, d'ingénieurs spécialisés dans le matériel informatique, de concepteurs de logiciels, de contrôleurs de l'Internet et de propagandistes en ligne rémunérés afin de surveiller, filtrer, censurer et guider les utilisateurs de l'Internet chinois. Des sociétés Internet privées, dont bon nombre sont des répliques de sites occidentaux, peuvent ainsi prospérer pour autant qu'elles ne s'écartent pas de la ligne du parti. […]

---

218 Notamment au Tribunal de surveillance du renseignement étranger (Foreign Intelligence Surveillance Court (FISC)). Les seules commissions administratives ne suffisent pas.

219 https://safeharbor.export.gov/list.aspx.

> L'Internet chinois ressemble à un terrain de jeu clôturé, gardé par des agents paternalistes. Comme la majeure partie de l'Internet auquel le reste du monde a accès, il est brouillon et désordonné, il offre des divertissements tels que des jeux, des possibilités d'achats et bien d'autres encore. Le fait de permettre le développement d'un Internet chinois florissant a constitué un élément important de la construction d'une meilleure cage. Mais cet Internet est constamment surveillé et manipulé[220]."

Puisque la Chine vend ses technologie à l'étranger, en Asie centrale et du Sud-Est, en Europe de l'Est et en Afrique, elle gagne des alliés dans le différend qui l'oppose aux Etats-Unis et à l'Europe au sujet de la gouvernance de l'Internet. Les résultats de ce différend définiront probablement les limites de la liberté sur l'Internet à l'échelle mondiale.

220 "China's Internet: A giant cage," The Economist, 6 avril 2013.

Liste des abréviations

AFACT	Conseil Asie-Pacifique pour la facilitation du commerce et le commerce électronique
APS	American Physical Society
ARPANET	Advanced Research Projects Agency Network
ASEAN	Association des nations de l'Asie du Sud-Est
CAPTEL	Centre for Asia Pacific Technology Law and Policy
CCD COE	Centre d'excellence pour la cyberdéfense en coopération
CCS	Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination
CERN	Organisation européenne pour la recherche nucléaire
CERT	Equipe d'intervention en cas d'urgence informatique
CIRT	Equipe d'intervention en cas d'incident informatique
COE	Conseil de l'Europe
COP	Initiative pour la protection en ligne des enfants (UIT)
CSCE	Conférence sur la sécurité et la coopération en Europe
EC3	Centre européen de lutte contre la cybercriminalité (Europol)
SEAE	Service européen pour l'action extérieure (Union européenne)
ENISA	Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information
EPFL	Ecole Polytechnique Fédérale de Lausanne
UE	Union européenne
EUROPOL	Office européen de police
FBI	Bureau fédéral d'investigation
G8	Groupe des Huit
GCA	Programme mondial cybersécurité (UIT)
GDPR	Règlement général sur la protection des données
GGE	Groupe d'experts gouvernementaux
GNI	Global Network Initiative
GPS	Système mondial de positionnement
HLCM	Comité de haut niveau sur la gestion
HLCP	Comité de haut niveau sur les programmes

HLEG	Groupe d'experts de haut niveau
HRC	Comité des droits de l'homme
AIEA	Agence internationale de l'énergie atomique
ICANN	Société pour l'attribution des noms de domaine et des numéros sur Internet
ICSC	Centre international de culture scientifique
TIC	Technologies de l'information et de la communication
INDECT	Système d'information intelligent soutenant l'observation, la recherche et la détection pour la sécurité des citoyens en milieu urbain
CEI	Commission électrotechnique internationale
IGF	Forum sur la gouvernance de l'Internet
IMPACT	Partenariat multilatéral international contre les cybermenaces (Malaisie)
IP	Protocole Internet
ISF	Information Security Forum
ISO	Organisation internationale de normalisation
ISP	Fournisseur de services Internet
IT	Technologies de l'information
ITIS	Institut universitaire des systèmes intelligents
UIT	Union internationale des télécommunications
Groupe HLEG	Groupe d'experts de haut niveau de l'Union internationale des télécommunications
PMA	Pays les moins avancés
LINC	Centre Internet libanais
LITA	Association libanaise des technologies de l'information
MAC	Contrôle d'accès obligatoire
MIT	Institut de technologie du Massachusetts
OTAN	Organisation du Traité de l'Atlantique Nord
SRI	Sécurité des réseaux et de l'information
NSA	Office national de sécurité
OSCE	Organisation pour la sécurité et la coopération en Europe
PDA	Assistant numérique personnel
PGP	Confidentialité plutôt bonne
PMP	Groupe permanent de surveillance sur la société de l'information
RFID	Identification par radiofréquence

SaaS	Logiciel en tant que service (software as a service)
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Surveillance et acquisition de données
SIL	Niveau de sécurité intégrée (Safety Integrated Level)
SLA	Accord de niveau de service
SMAC	Social, Mobile, Analytics and Cloud
SOA	Architecture orientée services
SORM	Système pour les activités opérationnelles d'enquête (System for Operative Investigative Activities)
TCP	Protocole de commande de transmission
UCLA	Université de Californie, Los Angeles
CNUCED	Conférence des Nations Unies sur le commerce et le développement
UN/CEFACT	Centre des Nations Unies pour la facilitation des procédures et des pratiques dans l'administration, le commerce et les transports
GNUD	Groupe des Nations Unies pour le développement
PNUD	Programme des Nations Unies pour le développement
CESAO	Commission économique et sociale des Nations Unies pour l'Asie occidentale
CESAP	Commission économique et sociale des Nations Unies pour l'Asie et le Pacifique
UNESCO	Organisation des Nations Unies pour l'éducation, la science et la culture
GGE	Groupe de travail provisoire d'experts gouvernementaux
UNIDIR	Institut des Nations Unies pour la recherche sur le désarmement
ONUDC	Office des Nations Unies contre la drogue et le crime
US-CERT	CERT des Etats-Unis
WFS	World Federation of Scientists
OMPI	Organisation mondiale de la propriété intellectuelle
ADM	Arme de destruction massive
SMSI	Sommet mondial sur la société de l'information

Contact:
Union internationale des télécommunications
Place des Nations – 1211 Genève 20
Suisse
E-mail: cybersecurity@itu.int
Website: www.itu.int/cybersecurity

ISBN 978-92-61-15302-1

Imprimé en Suisse
Genève, Novembre 2014
Crédits photos: Shutterstock

11/2014