ENQUÊTE DE LA CYBERPAIX

Union international des télécommunications

ENQUÊTE DE LA CYBERPAIX

Par 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

Janvier 2011

Mention légale

Les différents 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 Jody Westby, Henning Wegener et tous les auteurs qui ont contribué à faire connaître leurs vues sur ce sujet, d'une importance croissante. Le Secrétaire général exprime aussi sa reconnaissance au Professeur Antonino Zichichi, Président de la WFS, et adresse ses sincères remerciements au Chef de la Division de la stratégie institutionnelle de l'UIT, Alexander Ntoko, et en particulier à JeoungHee Kim, qui a dirigé et coordonné la présente publication, à Rebekah Lewis, Deepti Venkateswar, Preetam Maloor, Marco Obiso et Elizabeth Aschenbrener, à Claude Briand et son équipe, ainsi qu'à tous les collaborateurs de l'UIT et de la WFS sans l'aide desquels il n'aurait pas été possible de faire paraître la présente publication.

Les lecteurs qui auraient des commentaires à faire voudront bien s'adresser à la Division de la stratégie institutionnelle de l'Union internationale des télécommunications strategy@itu.int.

TABLE DES MATIÈRES

Liste des abréviations

AIS	Systèmes d'information automatisés
ARPA	Advanced Research Projects Agency (Département de la défense des Etats-Unis)
C3	Communication, commande, contrôle
CoE	Conseil de l'Europe
COP	Initiative pour la protection en ligne des enfants (UIT)
CRS	Congressional Research Service (Etats-Unis)
DARPA	Defense Advanced Research Projects Agency (Département de la défense des Etats-Unis)
DNS	Système de noms de domaine
ECOSOC	Conseil économique et social (Nations Unies)
ESCAPE	Electronically Secure Collaboration Application Platform for Experts (IMPACT)
FG Smart	Groupe d'action sur les réseaux intelligents
FGI	Forum sur la gouvernance de l'Internet
FTC	Federal Trade Commission (Etas-Unis)
GCA	Programme mondial cybersécurité (UIT)
GRC	Centre d'alerte mondial (IMPACT)
HRC	Comité des droits de l'homme (HRC)
IMPACT	Partenariat multilatéral international contre les cybermenaces (Malaisie)
IP	Protocole Internet
ISOC	Internet Society
IT	Technologies de l'information
MIT	Massachusetts Institute of Technology
NEWS	Network Early Warning System (IMPACT)
NSF	National Science Foundation
OTAN	Organisation du traité de l'Atlantique Nord
PDA	Assistant numérique personnel
PMP	Groupe permanent de surveillance sur la sécurité de l'information (WFS)
RFID	Identification par radiofréquence
RTI	Règlement des télécommunications internationales (UIT)
SCADA	Télésurveillance et acquisition de données
SMSI	Sommet mondial sur la société de l'information
SOA	Architecture orientée service

TCAO	Travail coopératif assisté par ordinateur
TCP	Protocole de commande de transmission
TIC	Technologies de l'information et de la communication
TNP	Traité sur la non-prolifération des armes nucléaires
UE	Union européenne
UIT	Union internationale des télécommunications
UIT-T	Secteur de la normalisation des télécommunications de l'UIT
UN	Nations Unies
UNCPCJ	Congrès des Nations Unies pour la prévention du crime et la justice pénale
UNESCO	Organisation des Nations Unies pour l'éducation, la science et la culture
UNODC	Office des Nations Unies contre la drogue et le crime
URL	Identificateur uniforme de ressources
WFS	World Federation of Scientists

A propos de l'Union internationale des télécommunications et du Programme mondial cybersécurité

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 en la matière.

Ce programme, qui a pour objet de renforcer la confiance et la sécurité dans la société de l'information, est conçu pour favoriser la coopération et l'efficacité, en encourageant la collaboration entre toutes les parties prenantes concernées et en tirant parti des initiatives existantes pour éviter les doubles emplois. Le GCA est la première alliance réellement mondiale dans le cadre de laquelle secteur public et secteur privé et de multiples parties prenantes font front contre les cybermenaces. En 2008, l'UIT a conclu officiellement un Mémorandum d'accord avec l'International Multilateral Partnership Against Cyber Threats (IMPACT), aux termes duquel le siège ultramoderne d'IMPACT, situé à Cyberjaya (Malaisie), est devenu le siège effectif du programme GCA. IMPACT est une initiative internationale public-privé qui vise à donner à la communauté internationale davantage de moyens pour prévenir les cybermenaces, s'en protéger et y réagir. Grâce à cette collaboration, les 192 Etats Membres de l'UIT, entre autres, disposent de compétences spécialisées, des installations et des ressources pour renforcer efficacement la capacité de la communauté internationale à se prémunir et à se protéger contre les cybermenaces, ainsi qu'à y réagir. Depuis son lancement, le programme GCA a reçu l'appui de leaders et d'experts de la cybersécurité dans le monde entier. Le programme est placé sous le haut patronage de S. E. le Dr Óscar Arias Sánchez, ancien Président de la République

du Costa Rica et Prix Nobel de la paix, et de S. E. Blaise Compaoré, Président du Burkina Faso.

Le programme GCA est à l'origine d'initiatives telles que l'Initiative pour la protection en ligne des enfants (COP) et la passerelle cybersécurité. Dans le cadre du partenariat avec IMPACT et avec l'appui de grands dirigeants internationaux, il sert actuellement à fournir à différents pays du monde des solutions en matière de cybersécurité.

A propos de la World Federation of Scientists et de son Groupe permanent de surveillance sur la sécurité de l'information

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 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 a été communiquée à tous les Etats Membres de l'Organisation des Nations Unies.

Le Groupe PMP est coprésidé par l'ambassadeur Henning Wegener de Berlin et Madrid et par Mme Jody R. Westby, P.-D. G. de Global Cyber Risk LLC, à Washington, DC. Ceux de ses membres qui ont contribué à la présente publication sont les suivants:

MEMBRES DU GROUPE PMP AUTEURS DE CONTRIBUTIONS

William Barletta

William A. Barletta est Directeur exécutif de la United States Particle Accelerator School - programme d'études supérieures aux Etats Unis. Il 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 (Slovénie), où il enseigne la gestion stratégique, et est conseiller principal auprès du Président de Synchrotron de Trieste (Italie). Il est membre de la American Physical Society, membre de son groupe sur les affaires publiques, vice-président de son Forum de physique internationale et vice-président de sa division de physique des

faisceaux. Il est le coauteur et éditeur de cinq ouvrages et l'auteur de plus de 150 articles sur des sujets techniques très variés. barletta@mit.edu

Vladimir Britkov

Vladimir B. Britkov (Ph.D.) est chef du Laboratoire de modélisation de l'information à l'Institut d'analyse des systèmes de l'Académie des sciences à Moscou (Russie). Il est professeur adjoint d'analyse et de modélisation des systèmes à l'Institut de physique et de technologie de Moscou (Université d'Etat). Ses principaux domaines de recherche sont la modélisation et la simulation sur ordinateur et l'application de systèmes basés sur la connaissance pour l'appui à la prise à la décision. Il a été membre du Conseil de direction de l'International Emergency Management Society (TIEMS). Il est membre de différents comités de rédaction de revues scientifiques dans les domaines de la modélisation et de la simulation, ainsi que de divers groupes de travail internationaux. Il est depuis 2003 membre du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists. britkov@gmail.com

Jacques Bus

Jacques Bus est consultant indépendant à *Digitrust.EU* et travaille dans le domaine de la confiance et de la sécurité des technologies de l'information et de la communication (TIC). Il est aussi chargé de recherche à l'Université du Luxembourg. Après douze années de recherche en mathématiques, il a axé ses travaux sur la gestion de la recherche et a collaboré pendant plus de 20 ans au Programme de l'Union européenne sur les recherches dans le secteur des TIC. Il a été pendant les six dernières années de cette période chef de l'Unité *Confiance et sécurité des TIC*. Il est membre du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists. Il est l'auteur de publications et de discours sur les questions de sécurité, de confiance, de respect de la vie privée et de gestion de l'identité. http://www.digitrust.eu

Axel Lehmann

Axel Lehmann est professeur titulaire au Département d'informatique de l'Université de Munich où il enseigne les techniques de modélisation et de simulation. Il est également président de l'Institut universitaire des systèmes intelligents (ITIS). Ses recherches sont principalement axées sur la modélisation et la simulation par ordinateur, l'application de systèmes basés sur la connaissance à l'appui du diagnostic et de la prise de décision, et la conception d'architectures informatiques innovantes. Il a été président de la Society for Modeling and Simulation International, est membre

de la German Informatics Society, de différents comités de rédaction de revues scientifiques dans les domaines de la modélisation et de la simulation et membre de groupes de travail et de comités d'évaluation internationaux, par exemple dans le cadre de l'Union européenne. Il est membre du Groupe PMP de la WFS depuis 2001.
axel.lehmann@unibw.de

Hamadoun I. Touré

Le Dr Hamadoun I. Touré, Secrétaire général de l'Union internationale des télécommunications (UIT) depuis janvier 2007, a été réélu pour un second mandat à la Conférence de plénipotentiaires de l'UIT réunie à Guadalajara, Mexique, en octobre 2010. Il a été Directeur du Bureau de développement des télécommunications de l'UIT (BDT) de 1998 à 2006 et bénéficie d'une vaste expérience professionnelle tant dans le secteur public que dans le secteur privé. Né en 1953, le Dr Touré est titulaire d'une maîtrise d'ingénierie électrique de l'Institut électrotechnique des télécommunications de Leningrad (LEIS, ex-URSS) et d'un doctorat de l'Université d'électronique, de télécommunications et d'informatique de Moscou (MTUCI, Fédération de Russie). Il est résolu à faire de l'UIT une organisation novatrice 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 œuvre des résolutions du Sommet mondial sur la Société de l'information (SMSI) et de la réalisation des Objectifs du Millénaire pour le développement (OMD).
hamadoun.toure@itu.int

Vitali Tsygichko

Le Dr V.N. Tsygichko, colonel en retraite de l'armée russe, est membre de plein droit de l'Académie des sciences naturelles de la Fédération de Russie et, depuis 1985, chercheur principal à l'Institut d'analyse des systèmes de l'Académie des Sciences de Russie (ISA RAS). Il est actuellement expert en matière de sécurité de l'information auprès du Ministère des Affaires étrangères de la Fédération de Russie. Depuis 1967, il est collaborateur de l'Institut central de recherche du Ministère de la défense et travaille sur des simulations mathématiques d'opérations militaires. De 1988 à 1991, il a dirigé un centre autonome de recherche sur les problèmes de sécurité nationale. Ses intérêts scientifiques sont très divers: problèmes méthodologiques et systématiques de la modélisation des processus socioéconomiques; théorie de la prise de décision; analyse appliquée aux systèmes; théorie et méthodes de prévision socio-économiques; sécurité nationale et stabilité stratégique; problèmes liés à la sécurité de l'information et problèmes géopolitiques. Il est l'auteur de plus de 200 articles et de huit ouvrages. Il écrit en permanence dans des revues telles que La pensée militaire, Le bulletin militaire, La revue militaire indépendante et plusieurs

publications étrangères. Il est diplômé de l'Ecole militaire d'artillerie de Riazan, de l'Académie militaire Dzerjinski, détient un doctorat en sciences (ingénierie) et est par ailleurs professeur. vtsygichko@inbox.ru

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, puis Ambassadeur en Espagne. Il a présidé, de 2001 à 2009, le Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists dont il est maintenant coprésident. 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. Entre autres diplômes, M. Wegener est Docteur en droit de la Yale Law School.
henningwegener@hotmail.com

Jody R. Westby

Mme Jody R. Westby est P.-D. G. de Global Cyber Risk LLC, qui a son siège à Washington, DC, et est également membre éminent associé du Carnegie Mellon CyLab. Mme Westby fournit des services juridiques et de conseil à des clients des secteurs public et privé du monde entier dans les domaines du respect de la vie privée, de la sécurité, de la cybercriminalité, de la protection des infrastructures essentielles et de l'espionnage économique. Elle préside le Privacy & Computer Crime Committee (Section of Science & Technology Law) de la American Bar Association (ABA) qu'elle représente à la Conférence nationale des juristes et des scientifiques. Mme Westby a été membre du Groupe d'experts de haut niveau créé par le Secrétaire général de l'UIT et a dirigé l'élaboration du kit pratique de l'UIT pour la législation sur la cybercriminalité. Elle est coprésidente du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists. Elle est coauteur ou éditeur de quatre ouvrages sur la cybercriminalité internationale, sur la cybersécurité et sur le respect de la vie privée et a publié de nombreux articles. Elle s'exprime sur ces sujets face à des auditoires du monde entier. westby@globalcyberrisk.com

Avant-propos

En 2011, nous profitons de tous les bienfaits d'une société mondiale et universelle de l'information, mais ces bienfaits s'accompagnent aussi de la menace de cyberattaques, qui peuvent survenir à tout moment et en tout lieu et causer d'immenses dégâts en un seul instant. Ces dégâts potentiels sont aggravés de manière exponentielle par les liens entre les technologies de l'information et de la communication (TIC) et les infrastructures nationales essentielles.

Le moment est venu d'agir, dès aujourd'hui, pour parer à cette menace de plus en plus présente.

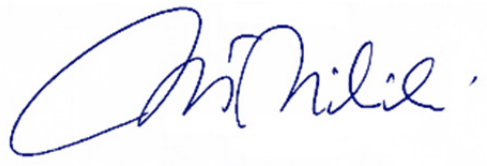
Les dirigeants et gouvernements de toute la planète réunis au Sommet mondial sur la société de l'information (SMSI) ont chargé l'Union internationale des télécommunications (UIT) d'assurer la coordination d'un mécanisme visant à instaurer la confiance et la sécurité dans l'utilisation des TIC. Depuis lors, le Dr Hamadoun I. Touré, Secrétaire général de l'UIT, a lancé le Programme mondial cybersécurité (GCA) et l'UIT dans son ensemble s'est activement employée à s'acquitter de ce mandat en prenant plusieurs initiatives. Surtout, l'UIT reste extrêmement préoccupée par les cybermenaces entre ses Etats Membres.

La World Federation of Scientists (WFS) encourage la collaboration internationale dans les domaines de la science et de la technologie entre les scientifiques et chercheurs de toutes les régions du monde. Elle a pour ambition de faire progresser le libre échange de l'information et de faire en sorte que chacun puisse bénéficier des progrès de la science. En 2009, son Groupe permanent de surveillance sur la sécurité de l'information (PMP) a rédigé la Déclaration d'Erice sur les principes de la cyberstabilité et de la cyberpaix qui appelle à prendre des mesures concertées sur le plan international pour faire en sorte que les réseaux et systèmes informatiques restent stables, fiables et accessibles et que l'on puisse avoir confiance en eux. Cette déclaration a été adoptée par la plénière de la WFS à l'occasion de la 42ème session de séminaires internationaux sur les situations d'urgence planétaires qui s'est tenue à Erice (Sicile) le 20 août 2009 et a été diffusée à tous les Etats Membres de l'UIT.

Pour atteindre l'objectif commun, qui est d'assurer le maintien de la cyberpaix, il est impératif qu'une collaboration s'instaure entre l'UIT et les membres de la communauté scientifique et technologique. Nous ne pouvons pas faire face efficacement à la menace de la cyberguerre sans la participation active de ceux qui

disposent des connaissances spécialisées et du savoir technologique qui font évoluer le paysage mondial.

Le présent ouvrage fait entendre la voix de cette communauté. Il représente une étape nécessaire sur la voie de l'édification de la coopération internationale pour traiter de ces questions importantes. Nous sommes heureux d'avoir ici l'occasion de présenter tous nos points de vue sur cette question fondamentale.



Dr Hamadoun I. Touré
Secrétaire général
Union internationale des télécommunications

Professeur Dr Antonino Zichichi
Président
World Federation of Scientists

1 Introduction

Par Jody R. Westby

La présente publication a pour but de promouvoir le concept de cyberpaix mondiale par les méthodes suivantes:

- analyse du rôle indispensable des TIC dans la vie quotidienne;
- évaluation des cybermenaces et tendances actuelles;
- analyse des incidences de la cybercriminalité et des cyberconflits;
- évaluation de la validité des cadres juridiques en vigueur;
- définition du concept de cyberpaix, qui doit devenir un principe directeur prioritaire du comportement pacifique dans le cyberespace;
- indication de la voie à suivre pour l'avenir.

On peut dire que l'Internet est le système nerveux central de la société. En effet, chaque secteur essentiel de l'infrastructure est tributaire des TIC. Ces technologies sont commandées par des systèmes de télésurveillance et d'acquisition de données (SCADA) et par d'autres processus complexes des technologies de l'information, reliés d'une manière ou d'une autre à l'Internet. Par exemple, les hôpitaux et les centres médicaux utilisent les TIC pour une multitude d'applications, qu'il s'agisse de l'envoi de secours ou d'appareils destinés à maintenir les patients en vie. Les secteurs des transports gaziers et pétroliers se basent sur des systèmes complexes de traitement et de navigation qui sont entièrement informatisés et les sociétés financières se servent de systèmes de paiement de paiement et de traitement électroniques. Les gouvernements sont tributaires des TIC pour fournir des services, gérer des activités sur des zones géographiques diverses, maintenir la sécurité publique et protéger leur territoire. Les entreprises ont besoin de systèmes informatiques qui gèrent la chaîne logistique, les relations avec la clientèle, les flux financiers, et remplissent des tâches de fabrication. Enfin, les systèmes de communication et les services d'utilité publique sont des infrastructures de base absolument essentielles.

L'Internet fait également partie intégrante de la vie quotidienne de chacun. Que ce soit au travail, pour s'informer ou pour se divertir, les TIC sont présentes. L'Internet facilite la diffusion du savoir et de l'information à un niveau jamais encore égalé. Les puissants réseaux sociaux établissent des liens entre les populations sur lesquelles ils exercent une influence indépendante de leurs gouvernements, sans d'ailleurs que ceux-ci n'aient rien vu venir. Ces réseaux permettent à chacun d'acquérir une certaine autonomie, de se faire connaître et de diffuser des idées originales par l'intermédiaire

d'un mécanisme qui ne respecte le plus souvent ni les frontières ni les convenances diplomatiques ou politiques. Aujourd'hui, chacun peut très rapidement influer sur les points de vue, valeurs, idées et partis pris, du fait de sa simple capacité à créer des contenus et à les diffuser dans le monde entier.

Toutefois, l'omniprésence de l'Internet facilite aussi les activités délictueuses et ouvre de nouvelles perspectives à la collecte de renseignements et aux conflits. Les points faibles des systèmes d'exploitation, des logiciels et des installations de sécurité peuvent être exploités pour menacer la fourniture de services de base aux populations civiles, faciliter l'espionnage économique et nuire aux activités des pouvoirs publics. Les virus, les vers, les attaques par déni de service (DDoS), le vol de données propriétaires, le spam et la fraude sont autant de facteurs qui compromettent la fiabilité des TIC et la capacité de fonctionnement des sociétés et des économies.

Des programmes de sécurité efficaces amélioreront la résistance des systèmes et contribueront à détecter et prévenir de tels actes et à y remédier. Les remises à niveau technologiques et les innovations aideront à bloquer et à détecter les attaques, tandis que l'harmonisation des législations sur la cybercriminalité facilitera les enquêtes sur les cybercriminels et les poursuites contre ceux-ci. Il reste beaucoup à faire dans chacun de ces domaines, mais le problème le plus dangereux et le plus potentiellement dévastateur est le cas où des Etats utilisent de telles tactiques pour s'engager dans des cyberconflits[1]. Il existe de nombreux exemples de conflits politiques et militaires qui se propagent dans le cyberespace, ce qui affaiblit la confiance dans les TIC et présente des risques sérieux. Plusieurs de ces situations sont décrites dans les chapitres ci-après.

Avant l'avènement de la société de l'information, le pouvoir et le leadership étaient habituellement concentrés entre les mains des autorités politiques, militaires ou économiques. Les Etats et les organisations internationales dictaient les normes et les valeurs sociales, les conflits armés étaient régis par des lois et des traités axés sur l'intégrité territoriale et les capacités défensives sur terre, dans les airs et en mer. Or, aujourd'hui, l'équilibre des pouvoirs est radicalement modifié sous la pression de l'Internet. Rien n'illustre mieux cette situation que l'histoire de l'Internet lui-même.

Les évènements dans le monde peuvent être un important élément déclencheur. Ainsi, juste après la deuxième guerre mondiale, l'Amérique a fait face à un nouvel ennemi avec la guerre froide, le communisme et la menace de frappes nucléaires. Face aux inquiétudes qu'a fait naître la suprématie scientifique des Soviétiques après le

---

[1] Le terme cyberconflit inclut des situations que l'on peut qualifier de "cyberguerre".

lancement du Spoutnik - premier satellite artificiel de la Terre - le président Eisenhower a fondé au Département de la défense des Etats-Unis la Advanced Research Projects Agency (ARPA), aujourd'hui appelée DARPA, chargée de coordonner toutes les recherches technologiques aux Etats-Unis[2]. J.C.R. Licklider a été détaché du Massachusetts Institute of Technology (MIT) pour diriger le programme de recherches informatiques de l'ARPA. Quelques mois auparavant, il avait publié une série de mémos décrivant un "Réseau galactique" d'ordinateurs interconnectés permettant d'avoir un accès partagé à des programmes et à des fichiers. Vint Cerf, Bob Kahn et autres "pères de l'Internet" ont ensuite noté que "En théorie, ce concept était pour une grande partie analogue à l'Internet d'aujourd'hui".[3]

A peu près à la même époque, les forces aériennes, inquiètes de leur capacité à poursuivre les opérations de commandement et de contrôle en cas d'une attaque nucléaire, ont demandé au Groupe RAND d'effectuer une étude sur un réseau militaire à toute épreuve pouvant assurer "un minimum de communications essentielles"[4]. Le Groupe RAND a conclu ses travaux (1962-1965) sur un rapport de Paul Baran décrivant comment un réseau informatique à commutation par paquets pouvait assurer cette fonction[5]. Parallèlement, et sans que le groupe RAN le sache, trois ingénieurs du MIT débattaient du concept de réseau informatique et de commutation par paquets[6]. Fin 1966, l'un de ces ingénieurs du MIT, Lawrence Roberts, a rejoint l'agence DARPA "pour développer le concept de réseau informatique"[7].

Tout le reste est de l'histoire connue. En 1971, l'ARPANET, comme s'appelait au début l'Internet, comptait 23 serveurs connectant des centres de recherche publics et des

---

2 "A Brief History of the Net", Fortune, 9 octobre 2000, p. 34, http://money.cnn.com/magazines/fortune/fortune_archive/2000/10/09/289297/index.htm (ci-après "Fortune"); voir aussi Dave Krisula, "The History of the Internet", août 2001 (complété en 2009), www.davesite.com/webstation/net-history1.shtml (ci-après "Krisula").

3 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet", Internet Society (ISOC) All About the Internet, www.isoc.org/internet/history/brief.shtml (ci-après "A Brief History of the Internet"); Licklider a publié sa série de mémos sur le "Réseau galactique" en août 1962 et a pris ses fonctions à l'ARPA en octobre 1962.

4 Krisula; *voir aussi* Fortune; Stewart Brand, "Founding Father", *Wired*, mars 2001, p. 148, www.wired.com/wired/archive/9.03/baran_pr.html (ci-après "Brand").

5 Brand, p. 145-153; *voir aussi* Krisula.

6 A Brief History of the Internet; *voir aussi* Brand, p. 146; Krisula.

7 A Brief History of the Internet.

universités dans l'ensemble des Etats-Unis. En 1981, ce réseau prenait le nom d'Internet, et en 1991, le World Wide Web, mis au point par Sir Timothy Berners-Lee[8], voyait le jour à l'Organisation européenne pour la recherche nucléaire (ou CERN). L'association entre l'Internet et le web a fait entrevoir des possibilités d'utilisation commerciale, mais les entreprises ne pouvaient avoir accès au réseau dorsal par l'intermédiaire du réseau NSFNET de la National Science Foundation (NSF).

En 1995, la NSF a donné son accord et a transmis l'accès au réseau dorsal Internet à quatre compagnies commerciales; en 1996, on comptait presque dix millions de serveurs en ligne et l'Internet couvrait l'intégralité du globe. En trente ans, ce réseau, qui était "un concept hérité de la guerre froide pour contrôler les lambeaux d'une société postnucléaire, est devenu une autoroute de l'information"[9]. L'association entre l'Internet et le World Wide Web s'est diffusée dans toutes les économies et toutes les couches de la société et s'est traduite par des transformations sociales qui étaient impensables 20 années plus tôt. On compte aujourd'hui presque deux milliards d'internautes et l'Internet transcende toutes les frontières géographiques. Sa gestion porte aussi bien sur des questions techniques que sur des questions de politiques publiques et intéresse aussi bien les parties prenantes que des organisations intergouvernementales ou internationales.

Paradoxalement, on peut dire que ce résultat de la guerre froide, associé à l'internationalisation des disciplines scientifiques qui a permis la création du web, représente aujourd'hui l'un des plus grands dangers pour la paix mondiale. Même si les facteurs géopolitiques[10] pèsent toujours d'un grand poids dans l'analyse des intérêts des pays et de la sécurité économique, l'Internet a fondamentalement changé l'analyse traditionnelle de la politique étrangère. Les géo-cyberdimensions influencent

---

8 Elizabeth D. Hoover, "The Inventor of the World Wide Web", *AmericanHeritage.com,* 12 novembre 2005, www.americanheritage.com/articles/web/20051112-internet-world-wide-web-tim-berners-lee-computer-geneva-cern-enquire-html-url-world-wide-web-consortium.shtml.

9 "Life on the Internet: Net Timeline", PBS, www.pbs.org/opb/nerds2.0.1/timeline/; *voir aussi* Krisula.

10 On définit la géopolitique comme: "1) L'étude des relations entre politique, géographie, démographie et économie, en particulier en ce qui concerne la politique étrangère d'un pays; 2) a) Une politique d'Etat utilisant la géopolitique. b) Une doctrine nazie selon laquelle les impératifs géographiques, économiques et politiques de l'Allemagne justifiaient le fait qu'elle envahisse et occupe d'autres pays; 3) Un ensemble de facteurs géographiques et politiques liés à une nation ou à une région ou ayant une incidence sur cette nation ou région". D'après American Heritage Dictionary, 2000, www.dictionary.com/search?q=geo-political.

de plus en plus la politique des Etats et les blocs géopolitiques font émerger un nouveau modèle.

Il ne s'agit plus pour les Etats-Unis de maintenir "un minimum de communications essentielles", mais, pour *tous* les pays du monde, de savoir comment préserver la géocyberstabilité et de veiller à ce que leurs infrastructures essentielles ne puissent être utilisées comme armes contre des civils innocents et sans défense, ce qui entraînerait des dégâts et souffrances inutiles.

L'auteur définit la notion de "géo-cyber" comme la relation entre l'Internet et la géographie, la démographie, l'économie et la politique d'un pays et sa politique étrangère. Elle définit la "géocyberstabilité" comme la capacité de tous les pays à utiliser l'Internet au service de l'économie, de la politique et de la démographie, en s'abstenant de toute activité qui pourrait causer des souffrances et des dégâts inutiles[11].

Aujourd'hui, le monde entier fait face à de nouvelles menaces sur Internet et la capacité de chaque Etat à préserver ses fonctions de communication, de commande, de contrôle et ses capacités informatiques contre les attaques de terroristes, de gangs organisés et d'autres Etats, est remise en question. Avec les TIC, les pays font face à des enjeux inédits sur le plan de la sécurité nationale et économique. Des particuliers peuvent aujourd'hui s'en prendre aux autorités et diriger des attaques asymétriques qui peuvent paralyser la totalité de l'infrastructure et bloquer les communications, et les systèmes les plus faibles peuvent désormais menacer la sécurité des pays les plus forts.

Les conflits dans le cyberespace peuvent avoir des conséquences potentiellement fatales lorsque les infrastructures de l'information essentielles sont attaquées. Ils peuvent aussi se traduire par des violations des droits de l'homme, provoquer des actes de violence et causer d'importants dégâts économiques. Tant les particuliers que les Etats sont exposés à des risques très importants et ne sont pas protégés par les cadres juridiques en vigueur, mal adaptés à l'univers en ligne.

Pourtant, il est urgent d'agir. Face à des pays qui se hâtent de mettre en place des cybercontrôles et d'étendre leurs capacités militaires aux cyberconflits, il importe que les Etats parviennent à un accord reconnaissant une nouvelle définition de ce qu'est

---

11 Présenté pour la première fois à la Conférence du ANSER Institute of Homeland Security: "Homeland Security 2005: Charting the Path Ahead", University of Maryland, exposé de Jody Westby, "A Shift in Geo-Cyber Stability and Security", 6-7 mai 2002.

"un minimum de communications essentielles" qui sont protégées des conflits. Une telle mesure éviterait des dégâts et souffrances inutiles entre les parties d'un conflit et protègerait les pays non impliqués. Il est vital de parvenir à un tel niveau de géocyberstabilité si l'on ne veut pas que les forces technologiques destructrices l'emportent sur les avantages de l'Internet.

Logiquement, une telle initiative doit avoir pour point de départ les organisations multinationales. Pour commencer, elles doivent définir le niveau de stabilité minimal des infrastructures et des communications nécessaires pour protéger les civils innocents et préserver les fonctions sociales de base, par le biais d'accords diplomatiques et de la primauté du droit. Elles auront pour cela besoin de l'appui de diverses parties prenantes (particuliers, secteur privé, société civile, milieux universitaires, juristes, experts en politiques, équipes de premier secours et force publique). Ainsi, les TIC et l'Internet peuvent offrir un cadre international de collaboration entre les pays et entraîner une meilleure compréhension et une meilleure acceptation des différentes valeurs culturelles et sociales dans le monde.

Le présent ouvrage repose sur le concept de cyberpaix – principe directeur du comportement dans le cyberespace. La cyberpaix doit être l'objectif auquel s'efforcent de parvenir toutes les nations. Ses avantages l'emportent de loin sur les conséquences néfastes du cyberconflit.

Cette publication, dont les auteurs sont, entre autres, Hamadoun I. Touré, Secrétaire général de l'Union internationale des télécommunications, et des membres du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists, a pour objet d'appeler toutes les parties prenantes à déployer des efforts pour assurer une stabilité minimale de l'Internet et de ses infrastructures et pour faire progresser le concept de cyberpaix mondiale.

2 Le cyberespace et la menace d'une cyberguerre

Par Hamadoun I. Touré

Les technologies de l'information et de la communication (TIC) font désormais partie intégrante de la vie quotidienne de nombreux habitants de la planète. Les communications, réseaux et systèmes numériques assurent des ressources vitales et des infrastructures indispensables à l'ensemble de l'humanité, ressources sans lesquelles beaucoup ne pourraient prospérer, ni même survivre. Ces nouvelles structures et nouveaux systèmes présentent de nouveaux défis pour le maintien de la paix et de la stabilité. Sans mécanismes de maintien de la paix, des villes et des collectivités dans le monde seront vulnérables à des attaques d'une variété inégalée et sans limites. De telles attaques peuvent être perpétrées totalement à l'improviste. Soudainement, les ordinateurs et téléphones mobiles cesseront de fonctionner, les écrans des distributeurs de billets et des guichets bancaires automatiques resteront blancs, la désorganisation des systèmes de contrôle aérien, ferroviaire et routier plongera les autoroutes, ponts et voies navigables dans le chaos le plus total et les produits périssables ne parviendront pas aux populations affamées. Du fait de coupures électriques, les hôpitaux, les domiciles des particuliers, les centres commerciaux et des régions entières seront plongés dans l'obscurité. Les pouvoirs publics ne seront pas en mesure d'évaluer les dégâts, ni de communiquer avec le reste du monde pour lancer l'alarme, ni de protéger les populations vulnérables en cas de nouvelle attaque. Tel est le tableau apocalyptique que présenterait une communauté paralysée par la perte instantanée de ses réseaux numériques. Tels pourraient être les ravages causés par une nouvelle sorte de guerre, une "cyberguerre".

Un nouveau domaine: cyberespace, cybersécurité et cyberguerre

La menace de la cyberguerre est aujourd'hui plus présente que jamais. A l'heure actuelle, avec les progrès technologiques et le développement des infrastructures numériques, des populations entières sont connectées à des systèmes complexes et interdépendants. Avec la demande de connexions Internet et de supports numériques, les TIC sont, de plus en plus, intégrées dans des produits qui auparavant fonctionnaient sans elles, par exemple automobiles, bâtiments ou systèmes de contrôle pour les grands réseaux d'électricité et de transport. L'alimentation électrique, les systèmes de transport, les opérations militaires et la logistique - pour ainsi dire tous les services modernes - sont tributaires de l'utilisation des TIC et de la stabilité du cyberespace. On entend par "cyberespace" l'univers physique et conceptuel dans lequel existent tous ces systèmes. On peut donc considérer que la notion de "cyberguerre" s'applique à la guerre menée dans le cyberespace, qu'elle

utilise les TIC ou les prenne pour cible[12]. La dépendance croissante vis-à-vis des réseaux électriques intelligents et d'autres systèmes de contrôle et de commande fondés sur Internet fait que le cœur même des ressources en matière d'énergie, de transport et de défense est à la portée de ceux qui cherchent à anéantir les Etats et les populations civiles[13]. Ainsi, le renforcement de la cybersécurité et la protection des infrastructures de l'information essentielles sont aujourd'hui indispensables à la sécurité et à la prospérité économique de chaque pays.

La vulnérabilité aux attaques commises dans le cyberespace contre les infrastructures essentielles augmente, de pair avec la dépendance vis-à-vis des TIC. Même si le terme exact de "cyberguerre" n'est toujours pas défini, les violentes attaques perpétrées contre les infrastructures informatiques et les services Internet au cours des dix dernières années laissent entrevoir la forme que pourrait revêtir un conflit dans le cyberespace et l'étendue de ce conflit. Des liens ont été établis entre des attaques commises en Géorgie[14], en Estonie[15], en Corée du Sud et aux Etats-Unis[16] et la cyberguerre. De nombreuses pannes d'électricité au Brésil ont été imputées à des cyberattaques et en 2008, des pirates informatiques se sont introduits sur le site web du gouvernement dont ils se sont rendus maîtres pendant plus d'une semaine[17]. Ces

---

12 Steven Elliot, "Analysis on Defense and Cyberwarfare", Infosec Island, 8 juillet 2010, https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html (ci-après "Elliot").

13 Ellen Messmer, "Cyberattack Seen as Top Threat to Zap U.S. Power Grid," *NetworkWorld*, 2 juin 2010, www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html (selon elle, la menace d'une cyberattaque coordonnée, qui pourrait être associée à une attaque physique, est considérée comme la menace "à fort impact et à faible fréquence" la plus préoccupante pour le réseau électrique nord-américain) (ci-après "Messmer").

14 Thomas Claburn, "Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google And Elsewhere," InformationWeek, 12 août 2008, www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702

15 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", Wired, 21 août 2007, www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

16 Choe Sang-Hun et John Markoff, "Cyber attacks Jam Government and Commercial Web Sites in U.S. and South Korea," The New York Times, 8 juillet 2009, www.nytimes.com/2009/07/09/technology/09cyber.html; Jack Date, Jason Ryan, Richard Sergay et Theresa Cook, "Hackers Launch Cyberattack on Federal Labs", ABC News, 7 décembre 2007, http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1.

17 Michael Mylrea. "Brazil's Next Battlefield: Cyberspace", Foreign Policy Journal, 15 novembre 2009, http://foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace (ci-après "Mylrea").

pannes d'électricité au Brésil illustrent bien l'ampleur possible des nouvelles sortes de cyberattaques: on peut assimiler la situation à une scène de film de science-fiction dans laquelle les métros, les feux de signalisation et la deuxième plus grande source d'énergie hydraulique au monde, le barrage d'*Itaipu*, cessent subitement de fonctionner, avec des conséquences pour plus de 60 millions de personnes[18].

La cyberguerre n'épargne pas non plus le secteur privé. Des géants des services sur le web comme *Google*[19] et *Twitter*[20] ont déjà été attaqués en 2009 et, dès 2000, des attaques par refus de service ont été lancées contre des compagnies aussi renommées que *CNN, Ebay* ou *Amazon*[21]. En conséquence, certains de ces services ont été indisponibles pendant plusieurs heures, voire plusieurs jours. Des pirates informatiques ont pris pour cible les systèmes de contrôle aérien, en désactivant des équipements essentiels comme les services téléphoniques et les feux de piste[22]. Il semblerait que six pays au moins aient été victimes d'une cyberattaque au cours des trois années écoulées et qu'au moins 34 sociétés privées aient été attaquées au cours des seuls premiers mois de 2010[23]. Malgré la gravité de ces menaces, il n'est pas trop tard pour éviter les scénarios potentiellement catastrophiques en créant des produits, des pratiques et des normes plus sûrs grâce à la concertation internationale[24]. Sécuriser l'Internet et mettre les TIC à l'abri des perturbations et destructions doivent être des activités prioritaires si nous voulons protéger les populations civiles, assurer le fonctionnement efficace des structures de base et encourager la poursuite du développement de nouveaux services.

---

18 Id.

19 Andrew Jacobs et Miguel Helft, "Google, Citing Attack, Threatens to Exit China", The New York Times, 12 janvier 2010, www.nytimes.com/2010/01/13/world/asia/13beijing.html.

20 Eliot Van Buskirk. "Denial-of-Service Attack Knocks Twitter Offline (Updated)", Wired.com, 6 août 2009, www.wired.com/epicenter/2009/08/twitter-apparently-down/.

21 Voir Abraham D. Sofaer et Seymour E. Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, p. 14, http://media.hoover.org/documents/0817999825_1.pdf.

22 Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain, United States Government Accountability Office, septembre 2007, GAO-07-1036, www.gao.gov/new.items/d071036.pdf. (En 1997, des pirates ont attaqué l'aéroport de Worcester aux Etats-Unis, désactivant le service téléphonique avec la tour de contrôle et paralysant le système de commande des feux de piste).

23 Elliot.

24 Joshua Pennell, "Securing the Smart Grid: The Road Ahead", p. 2, NetworkSecurityEdge.com, 5 février 2010, www.networksecurityedge.com/content/securing-smart-grid-road-ahead.

La cyberguerre - menace pour les infrastructures nationales

Le concept de cyberguerre recouvre la prise pour cible, non seulement de moyens et de systèmes militaires, mais aussi d'infrastructures essentielles à une société - y compris les réseaux électriques intelligents et les réseaux de surveillance et d'acquisition de données (SCADA) - grâce auxquelles elle peut fonctionner et se défendre. Même si le support est différent (le cyberespace et, à l'intérieur de ce cyberespace, les TIC), les attaquants peuvent utiliser des armes et s'engager dans un conflit offensif-défensif analogue à une guerre traditionnelle. En règle générale, la tactique de la cyberguerre implique la collecte de données ou l'infiltration de systèmes informatiques en vue de perturber des systèmes dont le fonctionnement est essentiel[25]. Parmi les cyberarmes potentielles, on peut citer les suivantes: virus et vers informatiques, exploits pour la collecte de cyberdonnées, brouilleurs de communications de données sensibles, logiciels informatiques de contrefaçon infectés, armes à impulsion électromagnétique, moyens de reconnaissance informatiques et bombes à retardement avec cheval de Troie intégré.

La dépendance croissante vis-à-vis des réseaux intelligents rend l'approvisionnement en énergie de nombreux pays particulièrement vulnérable aux attaques. Les réseaux électriques intelligents sont des systèmes numérisés qui relient les fournisseurs de services collectifs à une centrale de commande, souvent appelée réseau SCADA. Les réseaux SCADA rassemblent des informations sur l'alimentation électrique et l'utilisation de l'électricité, tandis que les réseaux intelligents font circuler sous forme numérisée ces informations entre les consommateurs et les fournisseurs[26]. Ces technologies sont aujourd'hui appliquées à un grand nombre de processus et de systèmes: gestion de l'approvisionnement en eau, gazoducs, transmission et distribution de l'énergie électrique, énergie éolienne, systèmes de communication de masse, fabrication, production, transports en commun, surveillance de l'environnement, contrôle du trafic aérien et feux de signalisation[27]. De plus en plus, les fournisseurs relient leurs réseaux intelligents à l'Internet pour permettre un accès à distance et une amélioration des fonctionnalités.

L'interconnexion de ces réseaux offre des avantages très intéressants puisqu'elle permet de réaliser des économies d'énergie et d'accélérer les communications entre

---

25 Elliot.

26 "Smart Grid", U.S. Department of Energy, www.oe.energy.gov/smartgrid.htm; "SCADA", *TopBits.com*, www.tech-faq.com/scada.html (ci-après "SCADA").

27 SCADA.

clients et fournisseurs, mais elle sert aussi à centraliser les données et à gérer d'immenses réseaux électriques sur un réseau doté de multiples points d'accès. Dès lors qu'ils comportent un grand nombre de points terminaux et qu'ils sont interconnectés, les réseaux électriques intelligents et les réseaux SCADA présentent de nombreuses failles par lesquelles les attaquants peuvent les infiltrer[28]. Par exemple, un compteur intelligent (compteur électrique connecté au réseau) peut être piraté et infecté relativement aisément et peut ensuite être utilisé pour introduire un ver qui se propagera à d'autres compteurs et peut finir par faire sauter le réseau électrique[29]. Bien que de nombreuses entreprises cherchent à sécuriser leurs réseaux en isolant les centres de commande des autres réseaux ("technique de l'étanchéité"), ces tentatives échouent souvent, sans que l'administrateur du système s'en rende compte[30]. Les bombes logiques sont une autre façon pour les attaquants de désorganiser ou même de détruire un réseau intelligent; les pirates peuvent infiltrer le réseau pour y cacher des logiciels malveillants et attendent d'activer ces bombes ultérieurement pour lancer un assaut concerté ou causer des pannes d'électricité limitées[31]. Les bombes de ce type créent un nouveau problème de sécurité: en effet, le risque est soit qu'elles explosent accidentellement, soit qu'un autre pirate les découvre par la suite et les fasse exploser[32] .

D'ores et déjà, certains pays qui ont investi dans des réseaux électriques intelligents font état de tentatives d'attaque, à raison de plusieurs milliers par jour[33]. Selon certaines estimations, les cyberattaques sont la menace la plus grave qui plane sur les

---

28 Katie Fehrenbacher, "10 Things to Know About Smart Grid Security", 9 octobre 2009, Earth2Tech, Gigaom, http://gigaom.com/cleantech/10-things-to-know-about-smart-grid-security/ (ci-après "Fehrenbacher").

29 *Id*.

30 "SCADA Security and Terrorism: We're Not Crying Wolf", p. 26, BlackHat, www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

31 Siobhan Gorman. "Electricity Grid in U.S. Penetrated By Spies", *The Wall Street Journal,* 8 avril 2009, http://online.wsj.com/article/NA_WSJ_PUB:SB123914805204099085.html.

32 Ellen Messmer. "Cyberwar' author: U.S. needs radical changes to protect against attacks", *NetworkWorld*, 7 avril 2010, www.networkworld.com/news/2010/040710-clarke-book-review.html (ci-après "Radical Change").

33 *Id.* (on y lit que le réseau électrique des Etats-Unis subit déjà plusieurs centaines de milliers de tentatives d'attaque par jour); Fehrenbacher (les 40 millions de compteurs intelligents installés dans le monde ont déjà subi plusieurs infractions à la sécurité).

réseaux électriques nationaux[34]. Une attaque à distance pourrait parfaitement cibler des infrastructures matérielles comme les groupes électrogènes et les transformateurs électriques, ce qui les amènerait, fondamentalement, à s'autodétruire[35]. Une telle attaque aurait vraisemblablement des conséquences à long terme dans la mesure où les compagnies d'électricité n'ont pas l'habitude de stocker des pièces de rechange onéreuses dont la fabrication et la livraison peuvent prendre des mois[36]. L'attaque d'un réseau électrique intelligent aurait pour effet de priver le consommateur d'électricité et serait aussi à l'origine de graves difficultés financières. Le prix des groupes électrogènes peut atteindre plusieurs millions de dollars et les investissements dans ces réseaux peuvent se monter au total à plusieurs dizaines de milliards pour certains pays[37].

Outre les dangers de graves dégâts matériels et de pertes financières immédiates, la menace de cyberattaques sape la confiance dans les technologies nouvelles et actuelles telles que les réseaux électriques intelligents et, par voie de conséquence, dans la fiabilité des ressources électroniques, financières et dans le domaine de la santé. Cette perte de confiance, à elle seule, pourrait causer de très importants bouleversements socio-économiques[38]. Le développement de l'utilisation de réseaux électriques intelligents associés à des réacteurs nucléaires (et d'installations de fabrication d'armes nucléaires) peut engendrer des risques et des dégâts potentiels encore plus importants. Au-delà des stratégies traditionnelles d'attaques et de défense, la cyberguerre pourrait aussi impliquer l'attaque de systèmes internes à une entité ou à un pays dans le but d'en détourner ou d'en perturber le fonctionnement

---

34 Messmer.

35 Mylrea.

36 "Cyberwar: War in the fifth domain", 7 janvier 2010, *The Economist*, www.economist.com/node/16478792 (ci-après "Fifth Domain").

37 *Smart Grid: Hardware and Software Outlook*, Zpryme, 2009, p. 2, www.zpryme.com/SmartGridInsights/2010_Smart_Grid_Hardware_Software_Outlook_Zpryme_Smart_Grid_Insights.pdf (on y lit que selon les estimations l'industrie des réseaux électriques intelligents aux Etats-Unis pesait 21,4 milliards USD en 2009, chiffre qui devrait atteindre 42,8 milliards en 2014); Jonathan Weisman et Rebecca Smith,"Obama Trumpets Energy Grants", *The Wall Street Journal*, 28 octobre 2009, http://online.wsj.com/article/SB125663945180609871.html (annonce par le président Obama de l'octroi de 3,4 milliards USD de subventions pour les projets de réseaux électriques intelligents évolués).

38 Fifth Domain.

temporairement au lieu de les endommager directement[39]. Un pays pourrait choisir de recourir à ce type de cyberattaques si, par exemple, il voulait neutraliser l'appui apporté par des alliés à un ennemi ciblé, pendant une durée suffisante pour pouvoir atteindre un objectif précis[40].

Spécificités et répercussions de la cyberguerre

Bien que l'on puisse dire que la cyberguerre ressemble à la guerre traditionnelle sur certains plans, les spécificités du cyberespace lui confèrent des dimensions radicalement nouvelles. Dans la mesure où les systèmes dans le cyberespace sont reliés par des réseaux informatiques et de communication, une cyberattaque peut entraîner la défaillance de plusieurs systèmes, bien souvent dans un grand nombre de pays. De nombreux processus de transfert de données mettent en jeu plusieurs pays et de nombreux services Internet reposent sur d'autres services situés à l'étranger; par exemple, lorsqu'un hébergeur loue un espace web dans un pays donné, alors que l'espace en question se trouve en réalité sur le serveur d'un autre pays. Même de brèves interruptions de service peuvent causer de graves dégâts financiers aux entreprises qui utilisent le commerce électronique. Les réseaux de communication civils ne sont pas les seuls systèmes vulnérables aux attaques, la dépendance vis-à-vis des TIC est également un risque majeur pour les communications militaires. A la différence des combattants traditionnels, les cybercriminels n'ont pas besoin d'être présents sur le lieu de l'attaque, réelle ou présumée. Et en portant leur attaque, ils peuvent utiliser des techniques de communication anonymes et de chiffrement pour cacher leur identité[41].

En outre, des outils logiciels qui sont couramment disponibles sur le Net sont utilisés pour automatiser les attaques. A l'aide de ces logiciels et d'attaques préinstallées, à lui tout seul, un cybercriminel peut attaquer des milliers de systèmes informatiques en une seule journée sur un seul ordinateur. S'il a accès à plusieurs ordinateurs - par exemple par l'intermédiaire d'un botnet - ces attaques peuvent avoir une portée encore plus grande. Ainsi, l'analyse des attaques contre des sites web de l'administration publique en Estonie montre qu'elles ont été commises par des milliers d'ordinateurs appartenant à un "botnet", c'est-à-dire un groupe d'ordinateurs infectés

---

39 Voir, par exemple, *Id.* ("Il est probable que le but de l'utilisation des cyberarmes est de déclencher, non pas une apocalypse électronique, mais une guerre limitée.").

40 *Id.*

41 *CERT Research 2006 Annual Report*, Carnegie Mellon University, Software Engineering Institute, p. 7 et suivantes, www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

sur lesquels s'exécutent des programmes commandés à distance[42]. Les botnets rendent en outre difficile la recherche des personnes qui sont à l'origine des attaques, car l'analyse des traces initiales ne mène qu'aux membres du botnet. Selon les données actuelles, jusqu'à 25% de l'ensemble des ordinateurs connectés à l'Internet pourraient être infectés par des logiciels dont le but est de les inclure dans un botnet.

Les outils logiciels permettent également de simplifier les attaques en autorisant des internautes ou des unités militaires peu expérimentés à lancer des cyberattaques. En outre, les attaques utilisant les TIC coûtent généralement moins cher que les opérations militaires traditionnelles et peuvent être perpétrées par de petits pays. Aujourd'hui, un pays qui dispose de faibles capacités militaires est néanmoins en mesure de paralyser sévèrement les infrastructures essentielles par le biais de cyberattaques. Cette asymétrie potentielle rend la cyberguerre intéressante du point de vue stratégique pour donner à tous des chances égales dans une situation qui, autrement, rappellerait celle de *David contre Goliath*. La crainte de la cyberguerre, renforcée par la réalité des cyberattaques, même si ces dernières sont pour l'heure limitées, sape la confiance du public dans les TIC. Ainsi, les cyberconflits pourraient avoir d'importantes incidences psychologiques qui risqueraient de désorganiser l'utilisation efficace des nouvelles technologies et de freiner les progrès dans de nombreux secteurs.

---

42 *Comprendre la cybercriminalité: guide pour les pays en développement*, p. 72, Union internationale des télécommunications, avril 2009, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (ci-après "Understanding").

3 Facteurs sociétaux de dépendance et confiance

3.1 Dépendance des sociétés modernes vis à vis des TIC et de l'Internet

Par Jacques Bus

L'ordinateur et les technologies informatiques font parties de notre environnement depuis la seconde moitié du vingtième siècle et les débuts de l'Internet remontent à 38 ans seulement, lorsqu'il était un réseau de communication dans le cadre du projet ARPA (DARPA). Toutefois, au cours des quinze dernières années, avec l'invention du World Wide Web (par commodité, nous appelons dans le présent article l'association entre Internet et web "l'Internet"), l'Internet a envahi la vie sociale et économique à une vitesse fulgurante. Nous pouvons avoir aujourd'hui accès aux réseaux de communication et aux réseaux sociaux, n'importe quand et n'importe où; nous avons accès à l'information, pratiquement sans limite; nous pouvons discuter et nouer des relations avec des personnes du monde entier; enfin, nous pouvons, confortablement installés à la maison, comparer ou commander des services et des produits au moment qui nous convient.

Selon les estimations de l'UIT pour l'année 2009, 25,9% de la population mondiale (soit 1,8 milliard de personnes) a une connexion Internet. Les gens passent chaque semaine deux fois plus de temps à surfer sur Internet qu'à regarder la télévision. On dénombre dans le monde 4,6 milliards d'abonnements au téléphone mobile, ce qui représente 67% de la population. A lui seul, Facebook comptait en juillet 2010 plus de 500 millions d'utilisateurs actifs et, à eux trois, Facebook, Myspace et Twitter rassemblaient, toujours en juillet 2010, 220 millions de visiteurs actifs. L'un des changements majeurs dans le monde est la transformation du téléphone mobile en téléphone Internet, qui remplace l'ordinateur personnel comme moyen de prédilection pour se connecter à l'Internet. D'ores et déjà, 9,5% de la population mondiale a un téléphone mobile large bande.

L'Internet a déjà profondément modifié la société sur toute la planète et cette évolution ne s'arrêtera pas en si bon chemin. De nombreuses publications[43]

---

[43] *Trust in the Information Society: A Report of the Advisory Board RISEPTIS,* www.think-trust.eu/; David-Olivier Jaquet-Chiffelle, ed., *Identity Revolution: Multidisciplinary Perspectives,* FIDIS, mai 2009, www.fidis.net/resources/identity-revolution/.

présentent des scénarios du futur décrivant le visage possible du monde d'ici à 25 ans. L'utilisation de jetons d'identité pour avoir accès aux transports publics, les dossiers de santé informatisés, l'accès aux services publics et aux services en réseau seront chose courante. Les réseaux sociaux se développeront et trouveront de nouvelles applications, plus efficaces et plus passionnantes. Les couplages de données faciliteront l'apparition de nouveaux services d'information qui aideront les chercheurs à travailler plus efficacement, les voyageurs à mieux profiter de leurs déplacements, les citoyens à comprendre les règles administratives et les motifs des hommes politiques, etc. Des agents et des processus fondés sur des bases de politique nous soulageront d'une grande partie des tâches administratives, telles que la prise de rendez-vous, la préparation de réunions et la conformité aux dispositions juridiques officielles.

La révolution sociétale fondée sur les TIC modifiera radicalement l'équilibre des pouvoirs, non seulement sur le plan national, où les citoyens auront à disposition pléthore d'informations sur les processus politiques, qu'ils pourront utiliser dans le processus démocratique, mais aussi sur le plan international.

L'accès à l'Internet facilite l'intégration des citoyens dans la vie économique et politique et leur permet de comprendre le fonctionnement et le mode de vie d'autres cultures. Nous avons vu comment, aux Etats-Unis, le président Obama a utilisé les réseaux sociaux dans sa campagne et nous pouvons supposer qu'il en ira de même à l'appui de la prise de décisions au niveau de l'Etat.

Avec les TIC, les compagnies internationales peuvent en outre s'organiser de manière à tirer le meilleur parti possible des opportunités qui s'ouvrent à elles dans le monde, ce qui peut réellement doper le développement économique et la croissance, en particulier dans les pays à faible revenu. D'ores et déjà, nous constatons que de grands pays en développement tirent parti de la situation et s'affirment comme des acteurs économiques et politiques de premier plan.

Cette révolution, comme toutes celles qui l'ont précédée, a beau ouvrir des perspectives, elle a aussi son revers.

Les infrastructures et services de l'information et de la communication font désormais partie intégrante de nos économies, mais elles sont extrêmement vulnérables, ainsi qu'en témoigne le nombre d'attaques constatées presque quotidiennement. La plupart de nos infrastructures essentielles (par exemple dans les domaines de l'énergie, de l'approvisionnement en eau, des transports et des systèmes financiers) sont fortement tributaires des TIC pour les fonctions de communication et de commande. Il existe donc un risque élevé d'accidents ou d'attaques délibérées visant ces infrastructures essentielles, ce qui risque de créer le chaos et d'entraîner des

pertes économiques considérables, notamment en cas d'intrusions et d'attaques visant les systèmes et les bases de données des organismes nationaux chargés de la sécurité.

La vulnérabilité de nos infrastructures sociétales TIC en fait une proie facile pour la "cyberguerre" ou "le cyberterrorisme" et menace donc la stabilité géopolitique. L'organisation délibérée d'attaques visant les systèmes essentiels d'un Etat avec l'approbation, l'appui ou le contrôle d'un autre Etat est quelquefois appelée "cyberguerre". Il faut toutefois préciser que le terme "guerre" dans ce contexte peut prêter à confusion dans la mesure où, bien souvent, aucune comparaison n'est possible avec ce qui vient à l'esprit quant on parle de guerre, à savoir la destruction à long terme d'infrastructures matérielles et les pertes massives de vies humaines.

Au cours des dernières années, le terme "cyberguerre" a été appliqué à plusieurs attaques dirigées, par exemple, contre l'Estonie[44], la Géorgie, la Corée du Sud et les Etats-Unis. Ces attaques ont quelquefois débuté par une "guerre psychologique" à l'initiative d'amateurs et à des fins de propagande et à laquelle, dans une deuxième phase, ont participé des spécialistes des cyberattaques (délinquants ou autres) dans le cadre d'une campagne à grande échelle, par l'intermédiaire de botnets lançant des attaques par refus de service contre les infrastructures sociales et économiques. Dans d'autres cas, des cyberattaques ont été perpétrées juste avant ou pendant des actes de guerre classique. A ce jour, les dégâts causés par les cyberattaques ont été pour l'essentiel limités et les capacités ont pu être rétablies après quelques jours, sans que ces attaques ne provoquent directement de pertes de vies humaines.

Il est dans la plupart des cas très difficile de prouver que des Etats jouent un rôle dans ces conflits, ce qui témoigne qu'il est urgent de conclure des accords internationaux sur la limitation des cyberattaques et sur les moyens de s'en défendre, ainsi que sur la coopération internationale pour parvenir à les endiguer. Manifestement, la vieille doctrine de la dissuasion qui prévalait au temps de la guerre froide n'est pas facilement applicable au cyberespace. On ne voit pas bien quelle forme prendrait la dissuasion et, surtout, il est difficile d'identifier l'ennemi (en raison de l'anonymat des attaques et de l'utilisation de serveurs mandataires).

Mais laissons de côté pour le moment le débat politique sur le terme "cyberguerre". Il ne fait aucun doute que la cybercriminalité devient un phénomène extrêmement inquiétant. Le nombre de menaces malveillantes et relevant du code pénal augmente

---

[44] Voir aussi Kertu Ruus, "Cyber War I: Estonia attacked from Russia", *European Affairs*, Vol. 9, N° 1-2, 2008, http://findarticles.com/p/articles/mi_7054/is_1-2_9/ai_n28550773/.

de façon exponentielle. Pour la seule année 2008, Symantec a détecté 1,6 million de menaces, ce qui représente 60% du nombre total de menaces détectées au cours de toutes les années précédentes. Plus de 8 millions de résidents des Etats-Unis ont été victimes d'usurpation d'identité. Le coût moyen d'une violation de la protection des données aux Etats-Unis s'élevait, selon les estimations, à 6,7 millions USD. En février 2010, on a appris que 750 000 systèmes informatiques d'entreprise dans le monde étaient infectés et contrôlés par des botnets. Selon Amit Yoran, ancien fonctionnaire aux Etats-Unis, les entreprises ne sont tout simplement pas préparées à se défendre, même si l'industrie de la sécurité aux Etats-Unis a ensuite minimisé le problème.

Howard Schmidt (Conseiller spécial du Président des Etats-Unis et coordonnateur cybersécurité) a reconnu que l'utilisation de l'Internet à des fins malveillantes posait un problème de plus en plus grave et a établi des priorités claires. Il réfute le terme de "cyberguerre" qui est pour lui "un concept terrible". Il ne pense pas qu'il puisse y avoir de gagnants dans un tel contexte et propose de cibler la délinquance et l'espionnage en ligne.

En dépit des divergences d'opinion, de l'avis général, il est tout à fait justifié de s'inquiéter de la sécurité de l'Internet et de la confiance qu'on peut lui accorder. L'évolution actuelle risque de se traduire par un renforcement des craintes des citoyens et par leur refus du nouvel univers numérique. L'incapacité de la politique et de la technologie à contrer cette évolution sociétale négative pourrait avoir de très lourdes répercussions économiques.

Dans son discours du 21 janvier 2010, Hillary Clinton, Secrétaire d'Etat des Etats-Unis, a insisté sur l'importance de l'ouverture et de la liberté de l'Internet pour la coopération et le développement dans le monde. Elle a fait référence aux "Quatre libertés" énoncées par Roosevelt - liberté d'expression et de culte, liberté de vivre à l'abri du besoin et de la peur - et aux conséquences importantes de l'Internet pour ces libertés, en particulier la liberté d'expression. L'Internet, qui a entraîné une véritable révolution des échanges d'informations et des réseaux sociaux, peut grandement faciliter la création de richesses pour tous, en particulier lorsque la "liberté de se connecter" est pleinement prise en compte. Toutefois, cette révolution a également entraîné une hausse de la délinquance et est une source d'inquiétudes auxquelles il faut répondre.

Les politiques ont clairement reconnu l'importance fondamentale de l'Internet sur la scène géopolitique internationale. Ils se rendent compte que les administrés attendent de leurs gouvernements qu'ils leur accordent sécurité et protection puisque les juridictions et les frontières nationales ne parviennent plus à remplir cette tâche. Le droit du consommateur, tel qu'il s'applique dans de nombreux pays, ainsi que la

responsabilité du fait des produits et services, ne sont plus adaptés dans un monde où le client et le fournisseur vivent dans des juridictions différentes, entre lesquelles il n'existe pas de coopération et où les services sont acheminés au coup par coup par des branches de sous-services utilisant des données dématérialisées provenant du monde entier.

Les leaders mondiaux font aujourd'hui face à des défis d'une ampleur sans précédent. L'attention des politiques doit se concentrer, par exemple, sur les changements climatiques et sur les mutations rapides de la puissance économique mondiale et de la sécurité de l'énergie, ainsi que sur les risques du numérique à l'échelle de la planète. La solution de tous ces problèmes passe par un leadership mondial énergique et tourné vers l'avenir.

Dans ce contexte, l'essentiel est d'appliquer ce que l'histoire nous a appris au sujet des structures et des valeurs sociétales, de la sécurité, de la confiance et des relations internationales. Nous devons entamer un processus mondial de transformation en vue de transposer nos cultures, nos valeurs sociétales et nos atouts dans ce domaine ainsi que les méthodes de coopération internationale et de les rendre applicables dans un monde qui reconnaît la nouvelle réalité numérique.

La confiance est indispensable

Le concept de confiance et son rôle dans la société

"*La confiance est omniprésente dans la vie quotidienne. Si nous ne prenons que quelques exemples du très large éventail d'occasions dans lesquelles elle joue un rôle, nous constatons que, de tous les phénomènes sociaux, la confiance est certainement l'un des plus fondamentaux. C'est justement cela qui en rend l'analyse très difficile: comment peut-on ne serait-ce qu'entrevoir ce que recouvre une force sociale aussi changeante?*"[45]

La confiance et la fiabilité sont des concepts de base de l'existence humaine. Nous les appliquons intuitivement et les évaluons toujours en fonction du contexte. Mais, lorsque nous les transposons dans l'environnement numérique, les difficultés commencent.

---

[45] Kieron *O'Hara, Trust: From Socrates to Spin*, Icon Books, Cambridge, 2004, page 10, http://eprints.ecs.soton.ac.uk/9361/.

Luhman[46] a défini la confiance comme un mécanisme qui simplifie la vie et permet de faire face aux nombreuses incertitudes et à la complexité de la vie contemporaine. Ainsi, la confiance renforce la capacité de tresser des liens efficaces avec une réalité beaucoup plus complexe et imprévisible que ce que nous sommes capables d'appréhender. A cet égard, la confiance est un mécanisme nécessaire à la vie humaine, que ce soit pour communiquer, coopérer, conclure des transactions économiques, etc. Elle favorise l'épanouissement de l'homme en encourageant l'activité, l'audace et l'esprit d'aventure et de créativité et en élargissant la portée des relations entre l'individu et autrui.

Selon une autre perspective, on pourrait dire que faire confiance revient à espérer un comportement bienveillant de son interlocuteur dans une certaine situation. Ainsi que l'explique Hardin[47], "La confiance appartient à la même catégorie cognitive que le savoir et la conviction. Dire "Je vous fais confiance" revient à dire "Je sais ou crois savoir certaines choses à votre sujet qui me laissent à penser que je peux avoir confiance en vous et que vous agirez avec bienveillance, même dans des situations imprévisibles.".

La confiance est une relation tripartite (*A compte sur B pour faire X*). L'évaluation de la confiance qu'a *A* en *B* pour qu'il fasse *X* joue un rôle important dans la décision prise par *A* de participer à une transaction, à un échange ou à une communication avec *B*. La confiance, qui simplifie la vie et réduit le risque, facilite l'activité économique, la créativité et l'innovation. Elle est extrêmement tributaire du contexte. Elle dépend de plusieurs facteurs: le temps (on peut facilement perdre confiance en quelqu'un, et en outre le concept évolue avec le temps); l'histoire et la mémoire; l'endroit et la situation; la culture; le rôle (privé ou professionnel); les émotions; ainsi que de plusieurs autres variables (par exemple, de considérations sociologiques comme la réputation, la récurrence et le fait d'être recommandé par quelqu'un).

Compte tenu de ce qui précède, il apparaît clairement que la confiance est un concept qui peut se renforcer par étapes dans une situation donnée et entre deux parties. Un complément d'information, par exemple par d'autres moyens ou par l'intermédiaire de relations, peut contribuer à renforcer la confiance et à pérenniser une bonne relation.

---

46 Niklas Luhmann, *"Trust: A Mechanism for the Reduction of Social Complexity", Trust and Power*, New York: Wiley, 1979, p. 4-103.

47 Russell Hardin, *Trust and Trustworthiness*; Russell Sage Foundation Series on Trust, Vol. 4, 2002.

En règle générale, on considère dans la présente analyse que les parties *A* et *B* sont des êtres humains, ce qui n'exclut pas la possibilité qu'ils agissent au nom d'organisations ou de groupes. Toutefois, en pratique, on pourrait aussi évoquer la confiance placée dans d'autres entités, par exemple gouvernement, entreprise, système ou service, base de données ou service d'information (tel qu'un journal ou un blog technologique), voire dans une entité virtuelle comme un agent logiciel. Hardin appelle cela "confiance dans les actes, le comportement ou l'intégrité d'une entité". Cette confiance peut être le résultat de l'obligation de rendre compte, de la transparence, de l'assurance et de la responsabilité, d'audits, d'une certaine réputation ou de la connaissance des intentions de l'entité.

Le concept de confiance en tant que capital social, ou "confiance sociale" a été analysé et développé par Fukuyama [48], Putnam[49] et d'autres experts. Il s'agit d'un concept statistique exprimant l'opinion des individus sur la confiance qu'ils peuvent accorder à tous les aspects de la société dans laquelle ils vivent, et plus précisément: leur confiance dans le gouvernement, les institutions, les lois, les systèmes, etc. On constate qu'il existe une forte corrélation entre un niveau élevé de confiance sociale et un niveau élevé de croissance économique et de prospérité.

Nous allons principalement utiliser le terme de "confiance" ("trust"), même dans les cas où Hardin utiliserait le terme anglais de "confidence". Néanmoins, il est important, aux fins de l'analyse, d'établir une distinction entre, d'une part, la confiance entre les personnes qui utilisent des systèmes et services numériques en réseau dans leurs interactions et, d'autre part, la confiance qu'une personne peut avoir dans une entité autre qu'humaine ou une institution.

La technologie numérique a révolutionné les communications et la collaboration entre les hommes en introduisant un nouvel intermédiaire composé d'un ensemble complexe d'"institutions" reposant sur la technologie (réseaux, services numériques, bases de données et réseaux sociaux). Lorsque nous parlons de confiance entre êtres humains, nous devons donc envisager aussi la confiance dans cette infrastructure technologique.

---

48 Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, 1995.

49 Robert D. Putnam, Robert Leonardi et Raffaella Y. Nanetti, *Making Democracy Work: Civic Traditions in Modern Italy,* Princeton University Press, 1993.

H. Nissenbaum[50] ne traite que de la confiance entre les personnes qui utilisent des systèmes numériques pour communiquer et énumère les facteurs qui motivent systématiquement la tendance à faire confiance (ou non):

1. Antécédents et réputation.
2. Déductions fondées sur des caractéristiques personnelles: qualités, prudence, loyauté, désir que les autres aient une bonne image de vous, comportement, habillement, etc.
3. Relations: relations mutuelles et réciproques, relations familiales, relations par affinités ou par communauté d'objectifs.
4. Relations: relations mutuelles et réciproques, relations familiales, relations par affinités ou par communauté d'objectifs.
5. Facteurs liés au contexte (groupes et communautés - publicité; récompense ou châtiment; normes; garanties ou "filets de sécurité" comme la loi sur la responsabilité ou le droit du consommateur).

Plusieurs de ces points, en particulier les points 1) et 3), englobent des aspects de ce que Hardin[48] définit comme la "confiance en intérêt incorporé". Il est dans l'intérêt de celui auquel on fait confiance d'agir avec bienveillance de sorte, par exemple, à ne pas perdre sa réputation, ce qui pourrait entraîner une rupture de la relation avec celui qui lui fait confiance (par exemple, un pilote qui perd sa réputation risque aussi de perdre son emploi). H. Nissenbaum recense également certains obstacles qui empêchent la confiance en ligne:

1. Identités manquantes (mais il faut tenir compte du droit à l'anonymat).
2. Caractéristiques personnelles manquantes (mais il faut tenir compte du droit au respect de la vie privée).
3. Contextes indéchiffrables (inconnus et prêtant à confusion, d'où un manque de clarté, mais qui peut aussi avoir un effet libérateur).

On peut considérer que ce troisième point implique une plus grande complexité en ligne. Il autorise bien sûr une plus grande liberté, mais, parallèlement, il faut davantage de confiance, et donc une plus grande dépendance, pour assurer le succès d'une transaction ou d'une communication. Toujours selon H. Nissenbaum, la sécurité n'est pas systématiquement synonyme de confiance. Si la sécurité est assurée, la

---

[50] Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?" Boston University Law Review, Vol. 81, N° 3, juin 2001, p. 635-664, www.nyu.edu/projects/nissenbaum/main_cv.html.

confiance n'est pas nécessaire. Néanmoins, cette dernière aide à vivre dans un univers mouvant et extrêmement complexe, mais passionnant, tandis que davantage de sécurité diminue l'intérêt et la complexité. Pour d'autres auteurs, la sécurité se situe à une extrémité de l'échelle de confiance, et la naïveté se situe à l'autre.

Sachant que dans l'infrastructure mondiale de l'information, la confiance (envers les étrangers) augmente à mesure qu'on apprend à les connaître, on peut lire ce qui suit dans le magazine *the Economist*: "Le fait qu'un si grand nombre de personnes, pour peu qu'on leur en donne l'occasion [...], veuillent vivre dans des pays autres que le leur, rend absurde le consensus politique et philosophique établi de longue date selon lequel c'est chez lui que l'animal humain est le mieux"[51]. En outre: "L'erreur de la philosophie est de supposer que l'homme, du fait qu'il est un animal social, devrait appartenir à une société donnée"[52]. Néanmoins, il faut faire attention de ne pas généraliser trop rapidement un comportement minoritaire, dans la mesure où seule une infime minorité de gens qui voyagent davantage et plus loin que ne le permettent les séjours de vacances organisés par des agences dans leur pays d'origine.

Pourtant, la mondialisation, sous l'impulsion des nouvelles TIC et du web, améliore la compréhension et renforce la confiance en encourageant la diffusion d'informations sur l'histoire et la réputation des sociétés, ainsi que sur leurs caractéristiques et sur la vie de leurs habitants et en facilitant la communication dans le monde. Cette évolution risque en fait d'éroder davantage le concept selon lequel "c'est chez lui que l'animal humain est le mieux". Peut-être faudra-t-il repenser complètement les sociétés, leur cohésion et le rôle que la confiance doit y jouer.

La confiance dans la société numérique

Comme nous l'avons vu plus haut, il faut établir une distinction entre:

- La confiance entre les personnes, dans une société qui utilise couramment les techniques numériques pour les communications et les transactions.
- La confiance des personnes dans les infrastructures des réseaux et systèmes numériques qu'elles utilisent pour les services, les communications, le stockage des données, les calculs, etc.

Commençons par le premier point.

---

51 "The Others", *The Economist*, 17 décembre 2009, www.economist.com/node/15108690.

52 *Id*.

Les problèmes posés par la confiance (entre les personnes) dans la société numérique, par comparaison avec "la société d'hier" sont notamment les suivants[53]:

- Les changements dans la collecte, le stockage, le traitement, la mise à disposition et la protection des données. En effet, on recueille et on stocke des données, non seulement à des fin de communication, mais aussi à des fins de surveillance (surveillance des piétons dans la rue, des visiteurs de sites web ou des internautes qui consultent des annonces publicitaires sur le web).
- L'identification, la réputation, l'authentification et la responsabilité ont un autre sens sur l'Internet. Pour convaincre de son identité, il est nécessaire de présenter des preuves (attributs, informations confidentielles ou biométriques). Il est très facile de détruire une réputation en diffusant des informations gênantes ou fausses, qu'il est ensuite très difficile de corriger. La possibilité de trouver refuge dans d'autres juridictions remet en question l'obligation de responsabilité et de transparence en l'absence d'accords internationaux sur l'application des lois et l'extradition.
- La complexité croissante, y compris celle des technologies, sans que des homologations et des normes donnent des garanties suffisantes, ainsi que le manque de transparence des procédures et méthodes de collecte et d'utilisation des données aboutissent à créer un environnement indéchiffrable et préjudiciable à la confiance qui devrait s'établir entre les internautes dans l'univers en ligne. Les gens peuvent être déroutés par ce qui se passe autour d'eux et ignorent souvent quelles données sont collectées à leur sujet et quelle utilisation en est faite.

On a plus facilement confiance lorsque l'identité et/ou d'autres informations d'authentification (preuves d'identité, attributs ou déclarations) concernant une personne sont connues ou peuvent être confirmées, éventuellement par un tiers digne de confiance. La réputation et d'autres informations circulant sur le web ou sur les réseaux sociaux peuvent renforcer la confiance. En outre, les citoyens ont davantage confiance dans une transaction avec un tiers s'ils peuvent contrôler la diffusion et l'échange de données les concernant avec ce tiers. La confiance est également renforcée par la transparence des opérations de collecte et de traitement de données et par la réputation des entités qui s'en chargent.

En ce qui concerne le second point, la confiance entre les personnes suppose, dans notre univers technologique, que l'on ait confiance dans les systèmes utilisés pour

---

53 Voir H. Nissenbaum.

communiquer, pour échanger des données ou pour confirmer l'identité et d'autres informations comme la réputation ou les preuves d'identité. Les internautes doivent avoir confiance dans les outils, systèmes et infrastructures qu'ils utilisent pour leurs transactions et communications. Nous disons qu'un système ou un service est digne de confiance jusqu'à un certain point si on peut être fondé à espérer qu'il fonctionnera conformément à sa description et à ses promesses et n'effectuera pas d'opération non prévue. Une confiance fondée peut reposer sur différents moyens: responsabilité (responsabilité du fait des produits), transparence du traitement et du stockage de données, homologation des systèmes techniques et possibilité d'audit à posteriori. Elle peut également être renforcée par l'existence de moyens et de méthodes compréhensibles et efficaces permettant de confirmer les allégations d'identité, la réputation ou l'identité. On a besoin de services et d'outils qui aident à créer et renforcer la confiance dans la qualité de service, la sécurité, la résistance, la protection des données et de la vie privée, conformément à des principes préalablement définis et faciles à comprendre. Tous ces éléments pourraient être assurés par des fournisseurs de services tiers aussi bien que par des organismes publics.

Comme le dit Vitali Tsygichko[54], les systèmes d'information automatisés (AIS) jouent un rôle particulièrement important dans notre société en ce sens qu'ils font de plus en plus partie intégrante des systèmes d'administration publique, dans l'ensemble des économies nationales. Ces systèmes sont au cœur des méthodes d'appui à la prise de décisions dans presque toutes les organisations socio-économiques. Les organismes publics, l'économie et les organismes bénévoles, mais aussi la sécurité nationale, sont pour une grande partie tributaires, pour leur efficacité, de la qualité de fonctionnement des systèmes AIS.

Il est donc très important de réfléchir à la fiabilité de ces systèmes. Celle-ci a trait en premier lieu à la validité des modèles sous-jacents qu'ils utilisent, à la fiabilité des équipements logiciels et matériels, au niveau de la qualification professionnelle des collaborateurs qui en assurent la maintenance et à l'efficacité des mesures prises pour les protéger des menaces extérieures.

Selon V. Tsygichko, pour assurer la fiabilité des systèmes AIS, il est nécessaire d'élaborer un cahier des charges pour la sécurité, la fiabilité (y compris le modèle correspondant en tant que représentation de la réalité) et l'intégrité des données. On peut utiliser, comme critère d'évaluation, les risques de violation de la sécurité. La **gestion des risques** est définie comme un ensemble de processus impliquant la

---

[54] Vitali Tsygichko est membre associé de PMP InfoSecur et a participé à ces discussions.

détection et l'analyse des risques ainsi que la prise de décisions, y compris le fait de maximiser les avantages des risques et d'en minimiser les inconvénients.

En complément des moyens techniques nécessaires au renforcement de la confiance, il faudra établir des règles et des règlements acceptables par la société. Les administrés n'auront confiance dans le traitement de leurs données personnelles qu'aux conditions suivantes: une réglementation doit assurer et faire appliquer le respect de la vie privée et la protection des données personnelles; les organisations doivent respecter la perception qu'ont les administrés d'une culture de la responsabilité grâce à une bonne protection du consommateur et à des procédures de règlement des différends; les méthodes d'audit et la transparence doivent faire l'objet d'une réglementation; enfin, les responsabilités doivent être clairement attribuées dans la chaîne des acteurs d'une transaction.

Sur le plan des politiques générales, une infrastructure TIC fiable ne peut être créée et ne peut fonctionner durablement que si des mesures d'incitation adaptées sont également réparties tout au long de la chaîne de valeur.

La transparence et la responsabilité doivent garantir l'équité et la force exécutoire. Il importe de remédier aux problèmes relatifs à la fiabilité des systèmes, et en particulier en ce qui concerne l'intégrité des logiciels et des données. A cette fin, peut-être faudrait-il élaborer un système d'assurance contre les risques de violation de la sécurité, qui, à son tour, encouragerait l'élaboration de méthodes et d'outils d'évaluation des risques. On obtiendrait ainsi, à terme, un système durable et en grande partie autoréglementé.

Le renforcement de la confiance entre les internautes passe par l'élaboration d'un système mondial, fiable et interopérable d'**Identification** et d'**Authentification**, ainsi qu'en témoigne la fabrication, dans nombre de pays, de cartes d'identité et de passeports électroniques fiables et conformes à des normes reconnues sur le plan international. Mais, pour les transactions en ligne, il faut avoir sur l'Internet une gestion des allégations et des preuves d'identité qui assure le droit au respect de la vie privée. La responsabilité, qui est essentielle pour l'économie de l'Internet, ne peut être obtenue qu'en rendant les personnes et les organisations responsables de leurs actes publics et contractuels. Il suffit normalement pour cela d'apporter des preuves de son identité, de présenter des attributs ou d'utiliser des données confidentielles qui ne sont connus que de la personne en question. On peut utiliser différentes données, différentes preuves d'identité ou différents attributs dans différentes situations, ce qui

entraîne la création de différentes "identités". Cameron, Posh et Rannenberg[55] ont proposé des métanormes pour la gestion des allégations d'identité.

L'Internet, avec ses nombreux réseaux sociaux différents, donne aussi la possibilité aux particuliers et aux organisations de construire leur histoire, de se créer des cercles d'amis et une réputation dans différentes communautés. Selon la terminologie du projet FIDIS[56], cela pourrait finir par créer des "identités partielles". Dans des situations où la transparence est nécessaire, on peut établir des liens avec des méthodes d'identification, d'authentification et de signature numérique permettant de protéger la vie privée, ce qui pourrait aussi contribuer à renforcer la confiance dans l'Internet en tant que moyen au service de l'activité sociale et économique.

Résumé

Nous avons analysé la pertinence de la confiance dans notre société ainsi que diverses opinions sur ce thème. Nous avons en particulier analysé les évolutions et les problèmes qui apparaissent à mesure que notre société devient de plus en plus tributaire des communications numériques et des transactions sur Internet. L'absence d'identification suffisante respectant le besoin d'anonymat dans certains cas, l'absence de caractéristiques personnelles, ainsi que la nécessité de protéger la vie privée et, surtout le contexte indéchiffrable créé par l'infrastructure technologique utilisée pour nos communications, privent les êtres humains des mécanismes indispensables pour créer la confiance qui leur permet de vivre et encourage leur créativité dans une société mondialisée.

Il nous faut donc élaborer, dans le cyberenvironnement, de nouveaux mécanismes fiables pour encourager les gens à se faire confiance, quel que soit l'endroit où ils se trouvent.

Nous devons mettre en place des réseaux de communication sûrs et fiables, des systèmes informatiques qui garantissent la conformité aux lois sur la protection des données et sur le respect de la vie privée, un cadre mondial et interopérable fiable d'identification et de gestion des preuves d'identité/allégations, ainsi que des services qui respectent les lois sur la responsabilité et sur la protection du consommateur. Ces

---

55 Kim Cameron, Reinard Posch et Kai Rannenberg, *Proposal for a Common Identity Framework: A User-Centric Identity Metasystem,* Joint "ICT Security" – "ICT for Government and Public Services" Workshop on Identity Management in the Future Digital Society, 14 octobre 2008, www.identityblog.com/?p=1048.

56 "About the FIDIS Network of Excellence", www.fidis.net/about/.

technologies doivent être conçues et élaborées dans une optique de confiance, de sécurité et de respect de la vie privée afin de permettre l'application des lois et la transparence, tandis que, inversement, les lois et règlements doivent être mis au point dans l'optique des progrès et des potentialités technologiques.

Les secteurs public et privé doivent collaborer sur le plan international à l'édification d'une infrastructure équilibrée des technologies et de législations/réglementations pour donner aux administrés confiance dans l'utilisation des potentialités du nouvel univers numérique.

Ainsi, l'humanité verra s'ouvrir des perspectives inédites de communiquer, de coopérer et d'effectuer des transactions économiques à l'échelle mondiale sur la base de mécanismes fiables, analogues à ce qui existait autrefois dans de petites communautés fondées sur les rapports humains directs. Ce sera là une étape décisive sur la voie de la stabilité mondiale.

3.2 Répercussions socio-économiques de la cybercriminalité

Par Jacques Bus[57]

La fourniture de services numériques, et de manière générale, les infrastructures numériques en cours de mise en place dans notre société, sont porteuses de grandes promesses. Parallèlement, comme toutes les technologies, elles peuvent être utilisées à des fins malveillantes. Nous pouvons distinguer les quatre grands problèmes suivants dans le domaine socio-économique:

1) **La nature mondiale du cyberespace**: l'existence de services et de communications transfrontières sur l'Internet pose, sur le plan socio-économique et sur celui de la sécurité nationale, des problèmes qui, jusqu'à maintenant, relevaient de la souveraineté d'un pays (contrôle des importations et des exportations, contrôle des passeports, formalités douanières, attaque d'un pays par un autre, etc.), ou à l'intérieur même d'un pays, des mesures de police à l'encontre des citoyens. Les inconvénients de l'absence de contrôles frontaliers dans le cyberespace n'ont pratiquement pas été analysés en profondeur, ni sur le plan national, ni sur le plan international. Il est toutefois manifeste que cette absence favorise la criminalité en créant une sorte d'immunité dont bénéficient les délinquants, en partie parce qu'il peut être difficile d'attribuer à un auteur précis des actes commis sur le web, et en partie parce que ceux qui commettent de tels actes se trouvent dans des pays qui les mettent à l'abri des mesures de police sur le plan international.

2) **Complexité des services**: les transactions et les services sur le web sont de plus en plus conçus comme des chaînes ad hoc de sous-services, qui recouvrent un grand nombre de juridictions et utilisent un grand nombre de données dématérialisées. Ces sous-services ou ces données peuvent relever de régimes juridiques différents, voire contradictoires. Les consommateurs ont du mal à s'en rendre compte ainsi qu'à en assimiler les conséquences. Les Etats ne peuvent plus garantir la responsabilité du fait du produit, ni la protection de leurs consommateurs. Face à cette situation, ils ont besoin d'accords internationaux et de la coopération internationale pour faire appliquer la loi. En outre, les services doivent assurer la transparence sur l'ensemble de la chaîne de services et s'adapter automatiquement aux conditions fixées par les consommateurs. Dans la situation actuelle, les possibilités

---

[57] L'auteur souhaite remercier pour leur contribution Udo Helmbrecht et son équipe à l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information).

de tromperie et de fraude sont innombrables et indétectables, et aujourd'hui les Etats ne peuvent assurer aucune protection.

3) **Réseaux sociaux et forums de discussion**: ils sont souvent utilisés pour établir des liens à des fins malintentionnées, visant en particulier les enfants ou les personnes âgées. Cela n'a rien de nouveau et les tromperies et escroqueries ont toujours existé. Néanmoins, une authentification insuffisante et l'absence de moyens de preuve sûrs et respectueux de la vie privée pour la vérification des données personnelles (nom, date de naissance, âge, sexe, informations professionnelles, mots de passe) en font une activité facile et rentable. En outre, les virus se propagent sur les sites de réseaux sociaux, sur lesquels la confiance peut jouer le rôle de vecteur. Le taux de réussite des attaques diffusées sur ces réseaux est très élevé. Bien que l'usurpation d'identité soit la menace numéro 1 pour les banques, elles n'offrent pas encore de services permettant à leurs clients de s'identifier.

4) **La criminalité internationale**: on a constaté à de nombreuses reprises au cours des dernières années, non seulement que les délinquants internationaux transfèrent leurs activités criminelles sur le web, mais aussi qu'il existe un marché noir international de moyens illégaux (botnets, usurpation d'identité, virus, etc.) et de vol de données (informations personnelles, informations sur les cartes de crédit, informations confidentielles sur une entreprise). La criminalité sur et par le web devient de mieux en mieux organisée à l'échelle internationale, s'étend à plusieurs juridictions, y compris celles où le pouvoir judiciaire est très faible, et privilégie au maximum la recherche de gains financiers. De nombreux exemples témoignent de cette évolution. Ainsi, la FTC a obtenu en mars la fermeture d'une entreprise semi-légale de logiciels malveillants de type "scareware", dont le chiffre d'affaires annuel dépassait les 180 millions USD. Le prix des virus, de l'appui technique et des kits "do-it-yourself" pour les actes punis par la loi est sûr d'être amorti. Le prix du cheval de Troie Zeus est de 700 USD (4 000 USD pour la version la plus récente) sur le marché noir (Zeus est utilisé pour déjouer les systèmes d'authentification tels que les systèmes à deux facteurs ou le système de code à trois chiffres de Mastercard). Il existe plusieurs strates de fournisseurs légaux et semi-légaux qui profitent de cette économie souterraine.

Les études et statistiques font apparaître des chiffres faramineux concernant les pertes pour la société et l'économie causées par ces activités illégales. Les chiffres

peuvent atteindre 1 billion USD dans le monde[58], soit presque 2% du PIB mondial. Selon les estimations de Boston Computing Network, les virus ont fait perdre aux entreprises des Etats-Unis plus de 7,6 milliards USD au cours des six premiers mois de 1999. Pour l'Allemagne, les pertes financières causées par les usurpations d'identité s'établissent, d'après les évaluations, à 15 millions € par an et les pertes sur les cartes de crédit à 155 millions € par an.

En règle générale, la plupart des chiffres relatifs aux pertes économiques reposent sur des suppositions discutables et sont forcément des extrapolations des données connues, tandis que de nombreux problèmes sont passés sous silence. La conclusion n'en est pas moins que le coût socio-économique de la cybercriminalité est très important et est souvent sous-estimé par ceux qui décident d'investir dans des mesures de sécurité. Il conviendrait d'analyser beaucoup plus sérieusement la rentabilité des investissements dans ce domaine.

La lutte contre la cybercriminalité nécessite de désigner des responsables des actes commis dans le cyberespace, y compris pour les actes secondaires commis dans le cadre de services d'envergure internationale. Une coopération juridique et diplomatique est nécessaire au plus haut niveau politique sur le plan international afin de définir des méthodes et procédures communes pour assurer la fiabilité des services et les responsabilités pour ces services et les mesures à prendre en matière d'économie et d'activité publique.

D'une part, le progrès technique doit permettre de trouver des solutions qui préservent l'unité du réseau mondial auquel les entreprises et les particuliers ont accès pour travailler, communiquer et s'informer, à la maison et en déplacement, de manière conforme aux législations applicables. D'autre part, les gens ont le droit au respect de leur vie privée sur le web, et devraient donc avoir la possibilité d'intervenir sur ce réseau au sein d'un cercle de confiance limité défini par eux-mêmes dans certaines situations et avec la garantie des fournisseurs que les données échangées ne seront pas utilisées à d'autres fins.

Malheureusement, nous assistons aujourd'hui au développement d'une économie des données privées qui va dans une direction opposée. Les entreprises de collecte et de

---

58 "McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property", communiqué de presse de McAfee, février 2010, www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html; voir aussi Unsecured Economies Protecting Vital Information, McAfee, 2009, http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

traitement de données gagnent de l'argent exclusivement en appliquant un modèle d'entreprise axé autour des données privées de la clientèle. Les clients peuvent penser qu'ils sont clients de ces fournisseurs de services et donc qu'ils peuvent être tenus responsables du service fourni. Mais en réalité, comme le consommateur ne paie rien à ces entreprises, elles sont un produit. Les entreprises de marketing, les analystes de données, les profileurs, les publicitaires, et d'autres, sont les véritables clients auxquels les sites de réseaux sociaux, les portails de services, etc., vendent les données relatives aux consommateurs.

En fait, il semble que la vie privée devienne victime de l'évolution socio-économique dans les domaines de la numérisation et des réseaux. Le prix de stockage de données baisse très vite et on peut imaginer qu'elles seront un jour stockées sans limitation ni en quantité, ni en temps. Cette évolution aura de profondes incidences sur nos interactions et sera aussi à l'origine de nouvelles formes de délinquance (violations de la vie privée, établissement de profils non autorisé, exploration de données non autorisée) ainsi que de nouvelles méthodes de contrôle politique. Une bonne partie de ces activités pourrait contrevenir aux droits constitutionnels existants et leurs répercussions sur la stabilité sociale, économique et politique ne sont pas encore analysées.

Outre les répercussions possibles du cyberenvironnement sur la criminalité et les droits de l'homme, il faut compter avec une autre menace, complètement différente, pour la société et les économies: la vulnérabilité extrême de la future infrastructure numérique de la société. Les sociétés dans leur ensemble risquent d'être confrontées à de graves pertes économiques et sociales lorsque leurs réseaux de communication ou autres infrastructures essentielles seront victimes d'attaques et de perturbations, que ce soit à des fins criminelles (chantage), terroristes (pour semer la terreur et l'instabilité) ou encore de dissuasion, à l'initiative d'autres Etats. Face à de telles attaques, les Etats ne peuvent guère prendre que des mesures défensives. Il leur est difficile d'adopter des stratégies offensives comme la dissuasion ou la contre-attaque, dans la mesure où ces attaques sont souvent anonymes, d'origine inconnue ou dirigées depuis des Etats voyous. Si l'on n'accorde pas une attention suffisante à la sécurité des réseaux et des systèmes et à la confiance qu'on peut avoir, le progrès technologique aggravera ces problèmes, le risque étant que les conflits internationaux et nationaux deviennent à l'avenir incontrôlables.

Enfin, il faut aussi envisager les risques à long terme pour la société. Des attaques de quelques secondes peuvent avoir des effets prolongés. Des années peuvent être nécessaires pour rétablir la confiance perdue en quelques instants. La rupture de confiance entre les personnes, entre les particuliers et les entreprises, entre les administrés et l'Etat, ainsi qu'entre les Etats eux-mêmes peut avoir des effets

dévastateurs sur les sociétés et sur la stabilité mondiale à long terme. Elle fait obstacle à la croissance économique future qui, dans la conjoncture actuelle d'après crise, est fortement tributaire de l'utilisation croissante des TIC. On ne peut pas se permettre la stagnation dans ce domaine, en raison d'un manque de confiance.

Des réseaux et des informations fiables, y compris par l'authentification dans le cyberenvironnement, doivent assurer la sécurité des citoyens (sur le plan physique, dans la vie économique et dans la vie privée). La fiabilité des systèmes, des infrastructures et des institutions TIC garantira une certaine confiance sociale, ce qui est essentiel pour la prospérité économique, ainsi que le montrent de nombreuses études.

L'instabilité sociale et les dégâts économiques (en termes de croissance) sont difficilement mesurables, mais peuvent être très importants. Il faut donc être préparé, prendre d'énergiques mesures de protection et prévoir la remise en état rapide et le rétablissement par eux-mêmes des différents systèmes.

En résumé

La mondialisation du cyberespace, les insuffisances dans l'identification des utilisateurs et l'attribution des actes, la complexité des services diffusés à l'échelle internationale, le développement mondial des sites de réseaux sociaux et l'apparition de réseaux et de marchés liés à

la criminalité internationale font craindre une augmentation de la cybercriminalité et font peser des menaces sur la durabilité d'une société stable – fondement de l'épanouissement personnel et de la prospérité économique.

La vulnérabilité de nos infrastructures sociales TIC et le champ illimité de la collecte et du stockage de données menacent la liberté personnelle et la stabilité internationale.

La confiance que les citoyens accordent à la société et aux pouvoirs publics – garants de la paix, de la sécurité et de la prospérité – est minée par les dangers et les incertitudes nés du progrès technique et par le risque élevé de pertes économiques.

Il est donc urgent de prendre des mesures politiques sur le plan mondial pour remédier à ces problèmes, sur la base d'une solide analyse des tendances technologiques, sociales, économiques et politiques et de leurs conséquences.

4 Evolutions techniques et menaces

4.1 Possibilités, tendances et menaces actuelles

Par Axel Lehmann, Vladimir Britkov, Jacques Bus

L'évolution technique et la demande exprimée par le marché sont les moteurs de l'innovation en matière de produits. A cet égard, lorsqu'on analyse les orientations futures des innovations dans le domaine des TIC et les possibilités qu'elles offrent, il faut tenir compte des progrès techniques actuels et prévus ainsi que des tendances de la demande future des consommateurs et du marché. En conséquence, les trois premières parties du présent chapitre seront consacrées à ces tendances et demandes et seront suivies d'une analyse des principales menaces existantes ainsi que de conclusions.

Au début du présent chapitre, nous récapitulerons les analyses et évaluations qui seront présentées plus loin et partirons du principe que les innovations techniques qui devraient voir le jour iront non seulement de pair avec des progrès rapides des microtechnologies et des nanotechnologies, mais conduiront aussi à la mise au point d'équipements informatiques et de détecteurs intégrés à grande échelle, de techniques réseau et de communication inédites et de services et d'applications innovants. Ces innovations auront aussi pour conséquence les deux grands axes évolutions suivants:

- convergence des ordinateurs et des téléphones mobiles individuels vers des dispositifs individuels de communication et informatiques multifonctions, portatifs et mobiles;
- évolution des technologies et des services actuels de l'Internet et du web vers l'Internet de demain. L'Internet des objets, qui se caractérisera par des communications et une mobilité massives entre les utilisateurs et toutes sortes d'équipements et d'objets ("choses"), ouvrira la voie à l'Internet de demain, qui sera placé sous le signe de l'efficacité, de la fiabilité et de la confiance.

Ces avancées techniques seront encore favorisées par la demande du marché et par celle des consommateurs, qui voudront disposer de produits, de services et d'applications TIC novateurs. D'après une étude publiée par Forbes, les secteurs des loisirs et des communications, de l'énergie et des soins de santé seront de puissants

moteurs d'innovation en matière de produits TIC, dont ils constitueront les principaux domaines d'application[59].

A cet égard, les trois sous-chapitres suivants traiteront des principaux facteurs qui influeront sur l'évolution future des TIC et les conséquences qui en résulteront – évolution technique, demande du marché et demande des consommateurs et "Internet des objets". Les deux derniers sous-chapitres porteront sur les perspectives qu'ouvriront ces innovations et sur les menaces et difficultés qu'elles feront surgir, tant pour les individus que pour les pouvoirs publics.

Evolutions techniques

Il va sans dire qu'au cours de la décennie actuelle, la miniaturisation et la numérisation ont grandement favorisé les progrès réalisés en vue de mettre en place un "univers **numérique**" dans lequel des données, des informations et des connaissances de toutes sortes sont stockées, transmises et traitées sous forme **numérique**. Il ressort d'analyses des grandes tendances des technologies de base actuelles que sont les semi-conducteurs que la loi de Moore selon laquelle "le nombre de transistors double sur une puce tous les deux ans environ" restera sans doute encore valable pendant encore au moins une décennie. Les techniques de conception et de fabrication actuelles permettent d'intégrer des milliards de transistors sur une seule puce. Même si à terme, de nouvelles technologies telles que les biotechnologies ou l'informatique quantique supplanteront progressivement les technologies actuelles des semi-conducteurs, ces tendances générales de plus en plus marquées à la miniaturisation et à la numérisation et au développement des fonctionnalités et de l'applicabilité se poursuivront et déboucheront sur une nouvelle diversification des TIC et des produits et applications reposant sur ces technologies.

A cet égard, il faut prendre en considération quatre grands axes d'évolution s'agissant des systèmes **numérique**s et des principes d'organisation dans le contexte des avancées relatives aux matériels, aux logiciels et aux microprogrammes:

- systèmes informatiques individuels ou multiples;
- réseaux, protocoles et services de communication;
- nanotechnologies, sciences des matériaux, capteurs, acteurs et systèmes intégrés;

---

59 Robert Krysiak, "Semiconductor Mega-trends in 2010", Forbes, jan. 2010, www.forbes.com/2010/01/04/stmicrœlectronics-healthcare-entertainment-technology-cio-network-semiconductors.html.

- mécanismes d'exploitation et d'organisation décentralisés pour les systèmes **numérique**s.

Etant donné que l'intégration à très grande échelle des transistors sur une seule puce, conjuguée à l'accroissement des fréquences d'horloge ont posé des problèmes de surchauffe, les **microprocesseurs** actuels sont conçus sous la forme de processeurs multicœurs fonctionnant à des fréquences d'horloge réduites, mais avec une qualité de fonctionnement nettement supérieure grâce au traitement parallèle opéré sur la puce. De nouvelles innovations seront rendues possibles dans le domaine des processeurs grâce aux technologies des semi-conducteurs à plusieurs couches, qui permettront d'accroître le nombre de processeurs centraux et de réduire la consommation d'énergie des puces. Il en résultera de nettes améliorations de la qualité de fonctionnement grâce aux processeurs multicœurs et aux systèmes de multiprocesseurs, qui augmenteront encore la capacité de la mémoire cache et de la mémoire principale, et aux progrès réalisés dans le domaine des systèmes monopuces. Autant de tendances qui se traduiront par une amélioration des performances de la gamme complète des ordinateurs, qu'il s'agisse des ordinateurs monopuces ou des éléments de calcul intégrés, voire des superordinateurs. Par ailleurs, du fait des avancées réalisées dans le domaine des réseaux de communication et de commutation, une multitude de structures et d'architectures d'ordinateurs interconnectés deviendra disponible.

Grâce à l'amélioration des techniques de miniaturisation, des systèmes de stockage externe rapides dotés de capacités de stockage accru et nécessitant des temps d'accès réduits seront également accessibles. Parallèlement aux méthodes architecturales évoluées et aux techniques logicielles perfectionnées, il deviendra possible de procéder à l'exécution massive en parallèle d'applications logicielles complexes. De même, la mise au point de technologies innovantes et de nouvelles batteries à faible consommation d'énergie améliorera ou facilitera grandement la mobilité des ordinateurs et de toutes sortes d'équipements informatiques.

Pour ce qui est **des réseaux, des protocoles et des services de communication**, les améliorations apportées en permanence aux techniques de communication hertziennes et satellitaires offrant une connectivité accrue et de plus grandes largeurs de bande déboucheront sur des innovations majeures. A cet égard, la création dynamique de réseaux virtuels, par exemple de réseaux privés virtuels[60], constitue une

---

[60] James Henry Carmouche, IPsec Virtual Private Network Fundamentals, Cisco Press, 19 juillet 2006, www.ciscopress.com/bookstore/product.asp?isbn=1587052075.

évolution primordiale. Cette technique, déjà en place actuellement, permet de créer et d'utiliser, pour une période limitée, des réseaux d'applications et des réseaux orientés vers les utilisateurs comprenant certains éléments et services de réseaux.

La mise en place de réseaux de recouvrement contribuera elle aussi à accroître la souplesse et les possibilités d'utilisation des infrastructures informatiques et de communication actuelles. Cette approche technique, qui constitue aujourd'hui un thème de recherche essentiel, est considérée comme un moyen efficace de surmonter les limitations qui caractérisent aujourd'hui les protocoles IP/TCP en place et de passer du protocole IPv4 au protocole IPv6, ce qui est important si l'on veut généraliser l'utilisation de l'Internet et de l'"Internet des objets". Des progrès techniques doivent impérativement être accomplis dans ces deux directions, afin d'encourager l'innovation dans le domaine des technologies et applications de l'Internet. En raison de l'essor spectaculaire de l'Internet actuel, notamment si l'on se place sous l'angle de la diversité et du nombre d'objets qui y sont connectés, il est indispensable d'accroître sensiblement l'espace d'adresses actuel des objets Internet (IPv4) dans l'optique du protocole IPv6[61]. En conséquence, il faut concevoir des techniques de transformation particulières permettant une transition évolutive entre ces deux normes. Il faut, d'une part, et parallèlement au passage de l'IPv4 à l'IPv6, mettre au point de futurs protocoles IP/TCP normalisés pour que toutes sortes d'objets puissent communiquer entre eux par l'intermédiaire d'un "Internet futur". Même si des solutions concrètes doivent encore être trouvées pour ces deux axes de recherche, on peut d'ores et déjà penser que ces bases techniques sur lesquelles reposera l'Internet de demain seront en place dans quelques années et permettront d'enrichir les applications de l'Internet avec des fonctionnalités évoluées et nouvelles, par exemple pour "l'Internet des objets".

En marge des lignes d'évolution décrites plus haut concernant le développement des systèmes fondés sur les TIC, il faudra tenir compte des progrès rapides, tant sur le plan technique que celui de la production, dans les domaines des **nanotechnologies, des sciences des matériaux et des composants numériques spécialisés, par exemple les capteurs utilisant des semi-conducteurs, les acteurs ou les systèmes intégrés**, lors de

---

[61] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", The Internet Society, décembre 1998, www.ietf.org/rfc/rfc2460.txt; Walter Goralski, "The illustrated Network: How TCP/IP Works in a Modern Network", The Morgan Kaufmann Series in Networking, 2008, www.freshwap.net/forums/e-books-tutorials/120250-illustrated-network-how-tcp-ip-works-modern-network.html.

l'analyse des tendances futures des TIC et des menaces associées. Ces avancées déboucheront par exemple sur l'apparition des composantes des TIC suivantes:

- interfaces utilisateurs tangibles[62];
- écrans en polymères;
- prêt-à-porter électronique (ordinateurs "vestimentaires")[63];
- capteurs passifs et actifs (technologies d'identification par radiofréquence (RFID)[64]);
- environnement à "intelligence ambiante"[65] ou systèmes "intelligents".

Parallèlement à ces avancées techniques, de nouveaux **produits et services logiciels et de microprogrammes améliorés** et des mécanismes d'organisation novateurs offriront la possibilité d'améliorer et d'enrichir les fonctionnalités et services. Au nombre de ces avancées figurent diverses technologies logicielles innovantes (conception de logiciels de type multi-agents), les architectures orientées vers les services (SOA), les nouveaux services offerts sur le web ou systèmes de gestion (par exemple pour le stockage ou l'extraction efficaces des données et pour l'équilibrage efficace de charge) et l'utilisation d'infrastructures de grille comprenant de gigantesques réseaux de ressources informatiques et de communication réparties. L'informatique en grille ou

---

62 Hiroshi Ishii, "The tangible user interface and its evolution", Communications of the ACM, Vol. 51, Issue 6, juin 2008, http://portal.acm.org/citation.cfm?id=1349026.1349034.

63 Steve Mann with Hal Niedzviecki, *Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer*, Doubleday of Canada, novembre 2001.

64 *RFID Adoption and Implications*, European Commission (Enterprise & Industry Directorate-General, ICT for Competitiveness and Innovation), DG Enterprise & Industry, The Sectoral e-Business Watch, Impact Study No. 07/2008, Final Report, septembre 2008, www.ebusiness-watch.org/studies/special_topics/2007/rfid.htm;. Arun N. Nambiar, "RFID Technology: A Review of its Applications", Proceedings of the World Congress on Engineering and Computer Science 2009, Vol II, WCECS 2009, 20-22 octobre 2009, San Francisco, Etats-Unis d'Amérique, www.iaeng.org/publication/WCECS2009/WCECS2009_pp1253-1259.pdf.

65 E. Aarts, R. Harwig, M. Schuurmans, chapter "Ambient Intelligence," in Peter J. Denning, ed., *The Invisible Future: The Seamless Integration Of Technology Into Everyday Life*, McGraw-Hill Companies, 2001 at 235-250; D. Wright, S. Gutwirth, M. Friedewald et al., *Safeguards in a World of Ambient Intelligence*, Springer, 2008, www.springer.com/computer/database+management+&+information+retrieval/book/978-1-4020-6661-0.

informatique répartie[66], qui figure parmi les applications les plus prometteuses et intéressantes, ouvrira une ère nouvelle dans le domaine des TIC, tant du point de vue économique et de la qualité de fonctionnement que sous l'angle de la disponibilité et de la fiabilité.

En marge de toutes les avancées techniques décrites plus haut, il faut tenir compte de deux évolutions importantes concernant les **principes d'organisation et d'exploitation** lors de l'analyse des grandes tendances en matière d'innovation des TIC et des menaces associées, à savoir la **virtualisation et la décentralisation**. La multiplication constante des fonctionnalités et l'accroissement de l'interconnectivité de composants **numérique**s hétérogènes d'une part, et la demande existante concernant l'efficacité de leur utilisation d'autre part, ont donné naissance à des systèmes virtuels, par exemple des processeurs virtuels, des systèmes de stockage virtuels, voire des ordinateurs virtuels. Par ailleurs, la complexité grandissante des systèmes informatiques et de communication en réseau et l'utilisation de réseaux virtuels empêchent fréquemment un fonctionnement efficace à partir de mécanismes de commande centralisés. En revanche, on fait appel à des mécanismes d'exploitation toujours plus nombreux pour la commande décentralisée des systèmes, ces mécanismes s'étant révélés plus souples et efficaces que les mécanismes centralisés. Comme exemples de systèmes décentralisés, on citera les applications logicielles multi-agent ou la commande de système bioanalogique.

La mise en œuvre et l'application de ces deux principes parallèlement (virtualisation et décentralisation) ont déjà ouvert de nouvelles perspectives quant à l'efficacité d'utilisation des ressources numériques en réseau. Ces réseaux peuvent former des "grilles"[67], une grille informatique pouvant comporter des nœuds d'ordinateurs en réseau, une grille de données constituée de systèmes de stockage répartis interconnectés ou encore des grilles d'équipements composées de dispositifs spéciaux auxquels il est possible d'avoir accès à distance. Dans le cas de l'informatique dématérialisée, il est possible d'avoir accès et d'utiliser à distance ces ressources en réseau et interconnectées via des fournisseurs. Malgré les indéniables avantages qu'ils présentent sur le plan économique et sur celui de la qualité de fonctionnement, ces réseaux ne sont toutefois pas sans risque. Le principal problème, qui représente aujourd'hui un risque majeur, a trait à la maîtrise de la complexité de tels systèmes, notamment du point de vue de leur fiabilité et de leur sécurité. Dans l'état actuel des

---

66 Vladimir Britkov, "Grid and Cloud Computing", Paper to the World Federation of Scientists Permanent Monitoring Panel on Information Security, mai 2010 (ci-après dénommé "Britkov").

67 Britkov.

connaissances scientifiques, il est impossible de confirmer que ces systèmes en réseau – dont certains sont déjà en service – fonctionnent correctement, ou de les valider par rapport à des applications précises, ni même de les tester de manière détaillée en raison de leur espace d'états considérable. A ce jour, cette situation n'a pas bénéficié de toute l'attention voulue, alors même qu'elle fait apparaître un problème fondamental s'agissant des innovations TIC[68]. A ce problème s'ajoute d'autres risques liés à l'apparition de pannes et de défaillances et aux possibilités d'utilisation abusive et de manipulations. Des tels risques nécessitent donc une évaluation d'ensemble des innovations dans le domaine des TIC et exigent que des travaux de recherche plus approfondis soient menés concernant les mesures à prendre pour y remédier.

Evolution de la demande des consommateurs et de la demande du marché

Il existe d'ores et déjà une très forte demande des marchés et des consommateurs concernant l'informatique ubiquitaire, la communication et l'accès à l'information, demande qui suppose l'utilisation d'équipements numériques et de fonctionnalités de mise en réseau "en tout lieu et à tout moment". La forte mobilité des consommateurs d'une part, et la diffusion et la mise à disposition d'informations et de connaissances à l'échelle du globe d'autre part font que les fonctionnalités améliorées ou nouvelles de produits TIC et l'efficacité de leur utilisation sont de plus en plus demandées. Cette demande ne cessera d'augmenter et sera générée par des marchés différents. A titre d'exemple, il existe une demande croissante de coopération répartie au niveau local et indépendante du temps dans les différents secteurs d'activité et les économies.

Cette demande repose implicitement sur le postulat selon lequel nous allons vivre et travailler dans un monde entièrement numérique, dans lequel chaque objet ou élément d'information pourra être traité et utiliser à tout moment, où que l'on se trouve. Cette demande déterminée par les consommateurs et le marché a pour conséquence de stimuler fortement l'innovation technique, s'agissant par exemple de l'utilisation efficace d'applications multimédia ou vidéo, de l'accès ubiquitaire au web, des tâches liées au travail coopératif assisté par ordinateur (TCAO) ou encore du recours à une infinie diversité de services et applications (reposant sur le web). Toutefois, l'évolution vers "l'Internet des objets", même si elle donne naissance à des composants et produits TIC novateurs et utiles, risque aussi de poser de nouveaux problèmes d'ordre social et de gouvernance et de faire peser des menaces sur la

---

68 Vladimir Britkov and Axel Lehmann, "Security challenges arising from innovations in information and communication technologies (ICT), "*International Seminar on Nuclear War and Planetary Emergencies*, 38th Session. E. Majorana Centre for Scientific Culture, Erice, Italy, 19-24 août 2007 p. 503-515.

sécurité. Il est donc indispensable d'analyser de manière approfondie dès maintenant (voir le chapitre ci-après), ces innovations et leurs conséquences.

Comme nous l'avons vu plus haut, les progrès actuels et futurs dans le domaine des matériels, des microprogrammes et des logiciels donneront naissance à de nouveaux produits et à des applications novatrices reposant sur les TIC, qui couvriront notamment les différents domaines d'application suivants:

- assistance à l'autonomie à domicile (par exemple pour les personnes âgées)[69];
- systèmes de commande intelligents (pour les transports, la logistique, l'aéronautique pour la navigation, les économies d'énergie, etc.);
- maisons intelligentes[70];
- soins de santé.

S'il est vrai que, dans les secteurs des loisirs et de la communication, la demande est avant tout liée à la qualité de fonctionnement des TIC et aux aspects économiques, dans d'autres domaines d'application (systèmes de commande ou de surveillance dans les secteurs de l'énergie ou des soins de santé), ce sont les critères de sécurité ou de fiabilité qui priment. Comme nous l'avons vu dans le sous chapitre précédent, l'accroissement constant du nombre et des fonctionnalités des appareils numériques utilisés dans ces applications, allié à leur interconnectivité quasi illimitée, pose le problème de "l'explosion de l'espace d'états". Des travaux soutenus de recherche fondamentale et appliquée doivent donc être effectués d'urgence, afin de concevoir des méthodes appropriées de conception, de vérification et de validation ainsi que des stratégies de test pour garantir ces exigences de qualité.

---

69 Kizito Ssamula Mukasa, Andreas Holzinger, Arthur I. Karshmer, "Intelligent User Interfaces for Ambient Assisted Living," Proceedings of the 13th International Conference on Intelligent User Interface, ISBN: 978-1-59593-987-6, 2008, http://portal.acm.org/citation.cfm?id=1378856; Fraunhofer IRB Verlag, ISBN 978-3-8167-7521-8, http://verlag.fraunhofer.de/PDF/English_Publications_2010.pdf.

70 P. Rashidi, D. J. Cook, "Keeping the Resident in the Loop: Adapting the Smart Home to the User," in Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions, Sept. 2009, Vol. 39, Issue: 5 at 949–959, http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=3468; The CASAS Smart Home Project, Washington State University, USA, http://ailab.eecs.wsu.edu/casas/.

L'"Internet des objets"

Selon le concept de l'"Internet des objets", non seulement les personnes, mais aussi tous les différents types d'objets, de dispositifs ou de produits que nous utilisons dans la vie courante ("objets") peuvent être connectés entre eux par l'intermédiaire d'un Internet du futur. Ces "objets" peuvent recevoir, mémoriser, traiter, ou transmettre des données et des informations en communiquant avec d'autres "objets", qu'ils s'agissent de personnes ou de services. A cette fin, il est nécessaire que beaucoup plus "d'objets" disposent d'une adresse Internet, ce qui sera possible avec le protocole IPv6, et soient utilisés individuellement ou dans des sous-réseaux en tant que point d'origine, de destination ou d'accès pour les communications, la coopération et l'informatique[71].

La mise en œuvre progressive de cet objectif permettrait de concrétiser l'idée "d'informatique et de communication ubiquitaire" lancée il y a une vingtaine d'années par Mark Weiser[72]. L'une des principales caractéristiques de cette conception est l'évolution des objets techniques vers des "objets intelligents" dotés de capacité de calcul et de raisonnement limitées et connectés au cyberespace via l'Internet. Un "objet" intelligent pourrait être, par exemple, un capteur actif qui reçoit des informations en provenance d'autres "objets", traite ces informations et, en fonction de sa situation actuelle, réagit en envoyant des messages de réponse à d'autres "objets". Une communication pourra ainsi être établie entre des personnes et des "objets", mais aussi entre les "objets" eux mêmes, ce qui offrira des possibilités d'applications entièrement nouvelles, avec des risques pour la sécurité informatique (confidentialité, authenticité et sécurité des données).

Menaces actuelles

Comme nous l'avons indiqué précédemment, l'ampleur et le degré de complexité et d'ouverture de notre monde numérique en réseau sont tels qu'il n'est guère surprenant que le nombre d'abus augmente rapidement et que les menaces

---

71 *L'Internet des objets - un plan d'action pour l'Europe*, communication de la Commission au Parlement européen, du Conseil, au Comité économique et social européen et au Comité des régions, http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf; "Appendix F: The Internet of Things (Background), Disruptive Technologies: Global Trends 2025, SRI Consulting Business Intelligence, www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf.

72 Mark Weiser, "The Computer for the Twenty-First Century," Scientific American, Sept.1991 at 94-110, www.cim.mcgill.ca/~jer/courses/hci/ref/weiser_reprint.pdf.

potentielles, si l'on n'y prend garde, deviennent de plus en plus nombreuses du fait de l'expansion future des TIC.

De nombreux rapports ont été établis par des sociétés proposant des solutions de sécurité TIC – par exemple MacAfee[73], Symantec[74], Kaspersky[75] – ou par d'autres entités s'occupant de questions de sécurité à caractère général ou s'intéressant à la sécurité de leurs propres systèmes et produits informatiques[76]. Les catégories de cyberdélits les plus fréquemment évoquées dans ces rapports sont les suivantes:

1. **Logiciels malveillants ou maliciels**: logiciels reposant sur l'intention perçue du créateur plutôt que sur des caractéristiques particulières. Parmi les maliciels figurent les virus informatiques, les vers, les chevaux de Troie, les logiciels-espions, les logiciels publicitaires malhonnêtes, les logiciels utilisés pour le vol de données financières, la plupart des outils de dissimulation d'activité (rootkits) et d'autres logiciels malveillants et non sollicités[77]. Symantec a indiqué qu'entre 2007 et 2008, le nombre de nouvelles menaces malveillantes était passé de 624 000 à 1 656 000.
2. On entend par **spam** l'utilisation abusive de systèmes de messagerie électronique (et notamment de la plupart des supports de radiodiffusion et des systèmes de diffusion numérique), pour envoyer massivement et indifféremment des messages non sollicités. La forme de spam la plus répandue est le spam par courrier électronique, ou les messages électroniques non sollicités à caractère commercial envoyés en très grande quantité. Le coût modique d'un message crée ainsi une valeur potentielle très élevée. Toutefois, de plus en plus de spams sont aujourd'hui envoyés à des fins délictueuses et contiennent des logiciels malveillants, ou à des fins de tromperie pour faire des paiements, obtenir des informations, etc. (phishing).

   Pour dissimuler l'adresse de l'expéditeur et pouvoir ainsi envoyer un volume important de données, les malfaiteurs ont souvent recours à des "zombies"

---

73 McAfee Security Advice Center, http://home.mcafee.com/advicecenter/.

74 "Internet Security Threat Report", Symantec, www.symantec.com/business/theme.jsp?themeid=threatreport.

75 Kaspersky, http://www.kaspersky.co.uk/index.html.

76 "Security Tech Center", http://technet.microsoft.com/en-us/security/default.aspx; SANS, www.sans.org/.

77 Concernant cette définition et pour plus de précisions, voir le site: http://en.wikipedia.org/wiki/Malware.

ou à des "bots" (c'est-à-dire à des ordinateurs faisant office de serveurs esclaves distants commandés depuis l'extérieur à l'insu de leur propriétaire) ou à des réseaux de "zombies" (également dénommés "botnets"). D'après des estimations, 350 milliards de messages spam en tout auraient été envoyés en 2008, dont 90% via des botnets, ce qui représente 85% du nombre total de messages circulant dans le monde.

3. Les sites web et les serveurs de hameçonnage (**phishing**) visent à usurper l'identité ou à pirater les sites web ou les adresses électroniques d'entités de confiance (par exemple des banques), dans l'intention frauduleuse d'obtenir des données sensibles (nom de l'utilisateur, mot de passe ou données de cartes de crédit par exemple). Des logiciels malveillants pourront être installés sur un ordinateur en vue de diriger l'utilisateur vers un site web de hameçonnage, et non pas vers le site de confiance recherché, ou un message spam pourra être envoyé au moyen d'adresses usurpées qui inviteront l'utilisateur à cliquer sur un lien qui mènera vers un site de hameçonnage. D'après des rapports, il existait près de 55 000 serveurs de hameçonnage en 2008, soit une hausse de 66% par rapport à 2007.

4. Les robots (**bots**) et réseaux de robots (**botnets**) sont créés à l'aide d'ordinateurs de nombreux utilisateurs à leur insu. Ceux-ci sont soit directement utilisés, soit "loués" à des fins délictueuses sur le marché noir. D'après Symantec, on recense chaque jour environ 75 000 ordinateurs infectés par des robots et 15 197 nouveaux serveurs de commande et de contrôle de robots différents. Ces serveurs de l'économie souterraine créent ainsi un véritable marché noir des informations subtilisées (cartes de crédit, identifiants électroniques, etc.), également utilisé pour la vente ou la location de logiciels malveillants ou encore de botnets.

Bien qu'il semble en général que la plupart des attaques proviennent des Etats-Unis, suivis du Brésil et de la Chine, n'importe qui peut lancer de telles attaques à tout moment, même depuis des sites distants. Bien que nous ayons tous encore en mémoire le virus "Conficker", qui a consisté à exploiter une faille de sécurité le jour même où la vulnérabilité a été connue, on peut conclure sans risque de se tromper que le nombre de vulnérabilités de ce type est en diminution, grâce à l'attention accrue que les grandes sociétés de services et de conseils informatiques accordent à la sécurité des systèmes d'exploitation et des applications.

Le principal secteur visé par ces activités délictueuses est le secteur financier, puisqu'il attire plus de 70% des opérations de hameçonnage, les fournisseurs de services Internet arrivent au deuxième rang, avec 11% seulement de telles opérations.

Dans la publication intitulée "*Whitebook: Emerging ICT Threats*", le consortium FORWARD[78] analyse systématiquement les menaces qui se font jour actuellement et les menaces futures dans ce domaine et met en évidence quatre grandes lignes d'évolution: *nouvelles technologies, nouvelles applications, nouveaux modèles économiques* et *nouvelle dynamique sociale*. Vingt-huit menaces, classées dans huit catégories, y sont également recensées:

1. *mise en réseau*: menaces liées à la mise en œuvre et au déploiement de nouvelles technologies de réseau et aux services d'infrastructure (acheminement, DNS) sur l'Internet;
2. *matériel et virtualisation*: menaces dues aux nouvelles avancées matérielles et logicielles relatives à la virtualisation et à l'informatique dématérialisée;
3. *dispositifs déficients*: menaces consécutives à l'utilisation de nouveaux systèmes informatiques présentant des limitations, tant sur le plan informatique que sur le plan des contraintes de puissance;
4. *complexité:* menaces résultant de la complexité et de la dimension des systèmes futurs, qui entraînent des interactions imprévues sur le plan de la dépendance et ont des conséquences sur la sécurité;
5. *manipulation de données:* menaces dues au fait que les utilisateurs (et donc les systèmes) stockent de plus en plus de données en ligne, si bien que ces données deviennent de plus en plus sensibles et recherchées;
6. *infrastructures d'attaque*: menaces liées au fait que les cyberdélinquants mettent au point et déploient activement des plates-formes offensives (telles que des "botnets") et ne se contentent plus de lancer des attaques éclair, mais mettent en place des bases opérationnelles sur l'Internet en vue de lancer des campagnes malveillantes;
7. *facteurs humains*: menaces résultant d'attaques internes, en particulier dans le contexte de la sous-traitance et menaces liées aux nouvelles attaques d'ingénierie sociale;
8. *insuffisance des exigences de sécurité*: menaces relatives aux systèmes traditionnels et grand public qui n'ont pas été dotés de mécanismes de protection suffisants et sont actuellement utilisés et déployés dans des scénarios pour lesquels les mécanismes de protection sont insuffisants.

---

78 "The FORWARD Emerging ICT Threats Whitebook", www.ict-forward.eu/whitebook/.

En classant ces différentes menaces par catégorie, il a été possible d'établir un ordre de priorité concernant les travaux complémentaires (dans le domaine de la recherche) à entreprendre pour atténuer ces menaces, compte tenu de leur gravité, de leur probabilité prévue et des mesures actuellement en place. Il a été conclu que la priorité absolue devait être accordée aux menaces relatives *au parallélisme, à l'ampleur, aux structures d'appui de l'économie souterraine, aux logiciels malveillants sur les dispositifs mobiles et aux réseaux sociaux*.

Dans l'état actuel des choses, il y a de bonnes raisons de s'inquiéter des menaces existantes, d'où la nécessité pour les spécialistes de différentes disciplines ainsi que pour les hommes politiques et les diplomates de prendre d'urgence des mesures concertées au niveau mondial. Même si pour contrer ces menaces, il faut avant tout axer les efforts sur une amélioration de la réglementation, des normes, des techniques ou des instruments concernant la sécurité, dans d'autres cas, il est indispensable d'entreprendre des travaux de recherche scientifique fondamentale et de trouver des solutions pour en assurer la mise en œuvre sur le plan pratique.

Conclusion

Les travaux de recherche futurs et la mise au point de nouveaux produits TIC influeront considérablement sur les comportements individuels, sociaux et culturels dans le monde entier, tant dans la sphère publique que dans la sphère privée. L'évolution (ou révolution) actuelle des systèmes numériques, de l'Internet et des services et applications qui leurs sont associés deviennent des ressources essentielles dans notre vie quotidienne. Cet univers numérique procure d'immenses avantages et ouvre de nombreuses perspectives pour l'humanité tout entière et le progrès technique, tout en offrant de nouvelles possibilités de surmonter certains des problèmes qui se posent à l'échelle du globe, par exemple dans les domaines de l'énergie ou des soins de santé. Les principaux avantages et possibilités inhérents aux technologies et applications futures des TIC sont traités dans le présent chapitre.

Malgré ces aspects positifs, de nouveaux problèmes encore plus préoccupants ont vu le jour, pour lesquels il est nécessaire d'intensifier les travaux de recherche fondamentale et de trouver des solutions appropriées: le problème essentiel tient au fait qu'il n'existe pas de méthodes de conception et d'analyse ayant fait leurs preuves sur le plan scientifique, afin de maîtriser l'énorme complexité des futurs systèmes numériques interconnectés, notamment du point de vue de la sécurité, de la fiabilité, des fonctionnalités et de la sécurité (confidentialité, authenticité et sécurité des données). L'un des défis les plus importants, pour les milieux de l'informatique et de la recherche scientifique concernant le web, est de concevoir des solutions pour résoudre ce problème de fond. A cet égard, la diffusion à l'échelle mondiale d'une liste

ouverte des problèmes les plus ardus, par exemple celle qu'a établie la World Federation of Scientists, conjuguée à l'adoption de mesures correctives efficaces, s'il en existe, pourrait s'avérer très utile.

Toutefois, cette insuffisance de maîtrise ne se limite pas aux techniques actuelles de conception et de production et il faut toujours tenir compte des conséquences d'erreurs humaines, de pannes et de défaillances techniques ou des utilisations abusives et des manipulations. Des mesures correctives s'imposent donc, compte tenu autant que possible des contraintes existantes.

En outre, aucune mesure appropriée n'a été mise en place pour informer les utilisateurs, les consommateurs et les institutions des principaux problèmes et des risques ou menaces liés à l'utilisation des ressources TIC. Il conviendrait d'associer les professionnels des médias à l'élaboration de matériels d'information sur les questions de sécurité informatique, afin de toucher des publics différents. Comme nous le verrons dans le chapitre II, les sociétés modernes sont tributaires des TIC et de l'Internet, qui est en pleine mutation. Les conséquences qu'auront l'évolution technique future vers la numérisation devront donc être analysées de manière approfondie et diffusées, afin de créer le climat de confiance nécessaire.

4.2 Censure de l'Internet par les gouvernements: cyberrépression

Par Henning Wegener

La liberté d'expression et le libre accès à l'information sont au cœur même de la société de l'information et constituent des composantes essentielles de la stabilité et de la paix dans le cyberespace, au sens où ces termes sont définis dans le chapitre VI de la publication "A Concept of Cyber peace" du même auteur. Porter atteinte à l'exercice de ces droits revient à compromettre les principaux avantages qu'offre l'Internet ou à empêcher les internautes d'en bénéficier et doit en conséquence être considéré comme l'une des principales menaces qui pèsent actuellement sur le cyberespace[79].

De tout temps, la liberté d'opinion et le libre accès à l'information ont été la clé de voûte des sociétés civilisées. Il s'agit de composantes indispensables des droits de l'homme et des libertés civiles, et, par conséquent, de fondements essentiels de la quasi-totalité des constitutions modernes. En effet, on pourrait mesurer le progrès de l'humanité à l'aune de la liberté qu'ont les individus d'obtenir des informations, d'avoir des opinions et de les faire connaître. Cela étant, la définition des limites auxquelles cette liberté fondamentale doit être assujettie pour des raisons de sécurité publique, de décence et d'ordre public a toujours été au centre du débat politique interne et représente un effort constant et nécessaire en vue de concilier et d'optimiser les libertés individuelles et l'intérêt général.

La censure qu'exercent les gouvernements en dépassant systématiquement ces limites et en contrôlant l'opinion publique et l'échange de vues, surtout en ce qui concerne les textes écrits, a toujours été un phénomène récurrent dans l'histoire de l'humanité et a de tout temps été à l'origine de combats pour la liberté de pensée.

---

79 La Fédération mondiale des scientifiques a déjà examiné ce problème dans la communication qu'elle a soumise au Sommet mondial sur la société de l'information (SMSI) lors de la phase de Tunis tenue en 2005, intitulée "La sécurité de l'information dans le contexte de la fracture numérique", en particulier dans la recommandation 5 intitulée "Refus de l'accès à l'information par le biais du filtrage de l'Internet", p. 12 et notes explicatives, p. 24-30, www.itu.int/wsis/docs.2/tunis/contributions/co1,pdf, et www.unbiw.de/infosecur. Voir également la communication d'Henning Wegener "Cyber Repression: Framing the Problem. Assessing the State of Debate and Thinking of Counter-Strategies," in Rights and Responsibilities in Cyberspace. Balancing the Need for Security and Liberty, 2010, EastWest Institute and World Federation of Scientists, qui porte sur un thème analogue www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

A l'ère de l'Internet, la donne n'a pas changé, mais prend des formes différentes. Les techniques **numérique**s ont donné une dimension nouvelle aux possibilités d'accès à l'information et à la communication: telles sont les caractéristiques essentielles de la société de l'information qui est la nôtre aujourd'hui. Comme dans tout autre domaine, l'Internet ouvre des horizons nouveaux, complique les mesures de la quantité et de la qualité et fait qu'il n'y a plus de distances et de temps, créant ainsi de nouveaux phénomènes ambivalents.

En effet, l'Internet accroît non seulement de manière exponentielle le volume d'informations et l'accès à l'information, mais multiplie aussi les possibilités d'intervention dans les processus techniques sous-jacents et de manipulation des contenus **numérique**s. Les techniques **numérique**s permettent d'utiliser des logiciels de filtrage pour bloquer un espace d'information dans l'ensemble de l'Internet, ou uniquement sur certains serveurs et permettent aux pouvoirs publics d'exercer une censure, même à grande échelle. Il faut donc examiner à nouveau la question de la liberté d'opinion et d'information en tant que droit de l'homme, car l'Internet est en passe de devenir un nouveau champ de bataille dans la lutte pour la défense des droits de l'homme et de la liberté d'opinion.

Les principales techniques utilisées par les pouvoirs publics pratiquant une censure sont le blocage IP, le filtrage et le réacheminement DNS, le filtrage par URL, par le biais du scannage pour des mots clés cibles ou le filtrage des paquets, qui met fin à une transmission par paquets TCP une fois que des mots clés controversés sont décelés. L'une des caractéristiques est que le logiciel de filtrage actuel ne réagit que d'une manière mécanique à l'apparition de certains mots ou de certaines phrases et dépasse bien souvent l'objectif recherché (engorgement).

Les fournisseurs de logiciels de filtrage ayant recours à ces techniques, entre autres, sont légion et comprennent la plupart des grands noms de l'informatique, mais aussi de sociétés spécialisées. Plusieurs pages web spécialisées permettent d'évaluer de manière comparative et de classer ces solutions logicielles du point de vue de leur efficacité, tandis que d'autres pages web gérées par les partisans d'une liberté d'expression totale sur l'Internet dénoncent l'émergence même de ces technologies.

Les techniques de filtrage doivent être examinées conjointement avec les possibilités de contournement. La technicité qui a marqué la mise au point des filtres caractérise également les technologies utilisées pour éviter, contourner ou endommager les filtres. Il est très difficile, pour ne pas dire impossible, d'exercer une censure totale de l'information sur l'Internet en raison des techniques réparties sous-jacentes du réseau. Les internautes disposent donc d'un certain nombre de ressources et de solutions grâce auxquelles ils peuvent contourner cette censure. La plupart d'entre elles

consistent à avoir accès à une connexion Internet ne faisant l'objet d'aucun filtrage, le plus souvent dans une juridiction différente qui n'est pas soumise aux mêmes lois en matière de censure. Pour ceux qui pratiquent une censure gouvernementale sur l'Internet, la difficulté réside bien évidemment dans le fait que tant qu'il existe dans le monde un seul système publiquement accessible non soumis à une censure, il sera toujours possible d'avoir accès à des documents censurés. Parmi les techniques disponibles pour cet accès "clandestin" figurent l'utilisation de serveurs par défaut, la mise en place de réseaux privés virtuels et le téléchargement de logiciels à code source ouvert permettant de surfer et de dialoguer sur le Net et de transférer des fichiers de manière anonyme (citons à titre d'exemple les outils Psiphon, I2P ou Tor).

Le filtrage de contenus remplit certes également une fonction de protection sociale importante et il semble légitime de bloquer des pages à contenu pédopornographique ou des sites incitant à la violence, à la haine raciale et au crime en général et il en est de même de l'utilisation croissante de l'Internet par le terrorisme national ou international. Les contenus qui ne peuvent être diffusés légalement en dehors de l'Internet doivent être passibles de sanctions pénales et être interdits également sur l'Internet. A cet égard, le secteur des logiciels de filtrage répond à des besoins légitimes.

Toutefois il convient là aussi de faire une distinction importante:

Quelles que soient l'efficacité des filtres et, partant, les conséquences de la censure, et quels que soient les intérêts commerciaux en jeu, l'essentiel est que dans les sociétés dites "libres" principalement, mais en aucun cas exclusivement, des démocraties occidentales, dans lesquelles il existe un consensus fort autour des valeurs, les restrictions à la liberté d'expression et à l'accès à l'information sont clairement réglementées par la loi, leur champ d'application est régi par la règle de l'adéquation et de la proportionnalité et il est possible de les évaluer dans le cadre de procédures d'examen juridiques accessibles au public. L'existence d'un cadre juridique précis et d'un contrôle judiciaire indépendant constituent en effet les critères déterminants permettant d'établir une distinction entre le contrôle légitime du contenu d'une part, et la censure illégitime d'autre part, et offrent un moyen de tenir compte des différences entre les valeurs culturelles et ce que l'on entend par vie privée. Les contenus offensants pour la culture, la religion, la morale et les autres convictions profondément ancrées au sein des sociétés de certains pays ne devraient pas échapper à tout contrôle au nom d'une liberté absolue sur l'Internet et ceux qui dénoncent à juste titre la censure politique exercée par les gouvernements devraient s'abstenir de prendre parti dans ce domaine.

Etant donné que le filtrage de l'Internet par les gouvernements, les limites à respecter en ce qui concerne les restrictions de la liberté d'expression, les compromis à trouver et le rôle que joue le secteur de l'informatique dans la fourniture des bases techniques du contrôle de l'Internet sont autant d'aspects qui ont trait à la question délicate de la souveraineté nationale, nous nous abstiendrons, dans le présent article, d'imputer la faute ou la responsabilité à un gouvernement pris individuellement et de mentionner le nom de tel ou tel pays, ou d'un fournisseur de services ou de matériel et de logiciels informatiques. L'objectif est ici de cerner le problème et de faire le point des débats sur la question, et non pas de formuler des conclusions hâtives. Dans ce même souci de modération, les pages web ou articles que nous mentionnons ne sont cités qu'à titre de référence et ne signifient pas que l'auteur de l'article s'identifie à leur contenu ou l'approuve.

Etant donné que l'Internet ne connait pas de frontières, il ne suffit pas de mettre en place des règles au niveau national pour gérer la liberté sur la Toile. Ainsi, l'Union européenne a institué dès 1999 un nouveau régime, à l'échelle de l'Union européenne, en vue de réglementer les modalités d'accès admissible aux contenus et procédures pertinentes de l'Internet ("Programme pour un Internet plus sûr"). Ce régime repose essentiellement sur le principe de l'autoréglementation dans le secteur de l'Internet et des moteurs de recherche, afin d'exclure les contenus à caractère illicite ou préjudiciable et d'assurer la conformité aux législations nationales. Dans certains domaines, ce dispositif d'autoréglementation fonctionne de manière satisfaisante, même s'il est parfois nécessaire de promulguer une législation complémentaire.

A l'échelle mondiale, un cadre juridique internationale a été établi, notamment dans les deux grands traités sur les droits de l'homme élaborés durant les premières années ayant suivi la création de l'ONU, à savoir la *Déclaration universelle des droits de l'homme (1948)* et la *Convention internationale sur les droits politiques et civils (1966)*. Presque tous les pays ont signé et ratifié ces traités, désormais considérés comme faisant partie intégrante du droit international coutumier et ayant également de ce fait force exécutoire pour les Etats non signataires. Le hasard veut que dans ces deux traités, le principe de la liberté d'expression et d'opinion soit consacré à l'Article 19, selon lequel tout individu a le droit de chercher, de recevoir et de répondre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit. Ce droit comprend incontestablement la possibilité de recevoir des informations par le biais de l'Internet et le droit d'accès à ces informations (au même titre que le droit de *ne pas* y accéder). C'est pourquoi le Sommet mondial sur la société de l'information (SMSI, 2003 et 2005) a solennellement réaffirmé que ces principes étaient essentiels à la société de l'information et qu'ils en constituaient un pilier indispensable, tout particulièrement dans la *Déclaration de*

principe de Genève (principes 4, 5 et 55). Il convient de noter que le texte du SMSI met l'accent sur la dimension relative à la liberté, amoindrissant ainsi l'importance des réserves ajoutées dans la Convention internationale.

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. L'une des problématiques de cette évolution est que les entreprises occidentales spécialisées dans les technologies fournissent non seulement leurs techniques de filtrage aux gouvernements ayant recours à la censure, mais collaborent également avec eux pour l'utilisation de ces techniques, contribuant ainsi à créer des systèmes de censure efficaces et bien conçus. Ce phénomène est au cœur de la présente analyse, qui vise aussi à suggérer des possibilités d'action au niveau international contre de telles pratiques. Comme l'a fait remarquer Jo Glanville, rédacteur en chef du périodique "Index on Censorship"[80], "pour la première fois de son histoire, la censure est devenue une entreprise commerciale"[81].

Nous écrivons les présentes lignes à un moment où le nombre de gouvernements exerçant une censure sur l'Internet, avant tout au détriment des droits et des libertés politiques, et la maîtrise des techniques de filtrage connaissent un essor sans précédent.

Un grand nombre d'organismes privés, notamment l'initiative OpenNet, qui fait figure de pionnière, Reporters sans frontières et le rapport sur la censure de l'Internet

---

80 Index on Censorship (GB) est l'une des principales organisations de défense de la liberté d'expression, www.indexoncensorship.org.

81 Jo Glanville, "The big business of net censorship", The Guardian, 17 novembre 2008, www.guardian.co.uk/commentisfree/2008/nov/17/censorship-internet.

(Internet Censorship Report)[82], qui utilise souvent les mêmes données et classements, suivent l'évolution de la censure gouvernementale sur l'Internet.

Ces sources montrent toutes à l'unanimité que la censure sur le Net progresse à un rythme inouï. A partir de listes et de données nationales, elles concluent qu'à l'heure actuelle, la censure sur Internet touche aujourd'hui près de 1,72 milliards d'individus, soit 25,3 pour cent de la population mondiale actuelle.

La liste des Etats ayant recours à la censure est longue, puisqu'au moins 25 Etats, et sans doute plus de 30, privent leurs citoyens de la possibilité d'accéder à la gamme complète d'informations disponibles en ligne. On trouve sur l'Internet plusieurs listes établies par des organisations qui surveillent de tels pays. L'initiative OpenNet les classe dans différentes catégories (dominant, substantiel, nominal et indirect) a également mis en place une "liste noire". Reporters sans frontières a également établi une liste des 13 principaux "ennemis de l'Internet". La plupart des pays surveillés axent leur intervention sur l'interdiction des contenus à caractère politique (liberté, démocratie, élections libres, voies de recours juridiques, rapports sur des événements politiques sensibles) que leur propre système de gouvernement n'autorise pas, mais beaucoup d'entre eux vont beaucoup loin encore. Certains gouvernements appliquent essentiellement des restrictions sur les questions morales ainsi que sur l'ordre culturel et moral en place. Les contrôles peuvent être plus ou moins stricts et rigoureux. Dans certains pays, les responsables de la censure bloquent des pages, mais dirigent ensuite l'internaute vers une page explicative, en fournissant un accès s'il s'avère qu'il existe un intérêt "légitime" spécial pour les informations en question, ce qui assure une certaine transparence. Dans d'autres pays, la censure s'exerce d'une manière sporadique et inefficace et aucune sanction n'est appliquée en cas de non-respect des blocages.

Toutefois, en règle générale, la censure exercée par les gouvernements est sans limites et porte sur un large éventail de connaissances, sans fournir la moindre

---

82 OpenNet Initiative, www.opennet.net. Le projet comprend un réseau international d'enquêteurs qui ont pour tâche de déterminer l'étendue et la nature des programmes gouvernementaux de filtrage de l'Internet. Au nombre des établissements universitaires participant à ce projet figurent le Centre for International Studies de l'Université de Toronto's Munk School of Global Affairs, le Berkman Center for Internet & Society at Harvard Law School, l'Oxford Internet Institute de l'Université d'Oxford et le SecDev Group, qui a remplacé l'Advanced Network Research Group de l'Université de Cambridge (Cambridge Security Programme). Voir également le lien www.chillingeffects.org, qui présente les activités d'un groupe encore plus important d'établissements universitaires qui "supervisent le contexte juridique dans lequel s'exercent les activités liées à Internet".

justification ou explication des raisons qui la sous-tendent, et est même le fait de pays par ailleurs très respectables. Plus le régime d'un pays est éloigné du modèle démocratique occidental, plus les effets de la censure par le biais du filtrage d'Internet se font sentir. Certains Etats poussent même la mainmise qu'ils exercent sur leur population par le biais de la censure de l'Internet à l'extrême, puisque les internautes surpris en train d'accéder à des pages interdites sont passibles de sanctions et que dans d'autres pays, ils sont poursuivis par une cyberpolice agressive. Il semblerait que le nombre d'internautes en détention soit alarmant. Certaines sociétés informatiques internationales fournissant les logiciels sont même soupçonnées de complicité concernant ces mesures de poursuite et de contribuer ainsi aux souffrances humaines qui en résultent.

Les conséquences de la censure à grande échelle sont graves et ne sauraient être sous-estimées. Les individus voient non seulement leurs droits en vertu du droit international bafoués, mais sont également privés des avantages importants de l'ère de l'information. Par ailleurs, ils ont une vision fausse des réalités mondiales et leur participation à l'enrichissement des processus de communication à l'échelle du globe s'en trouve limitée. Le filtrage massif de l'Internet peut également modifier l'état d'esprit collectif d'une nation. Il faut également tenir compte du fait que cette censure a un effet doublement négatif: d'une part, les citoyens sont privés d'informations et d'une vision mondiale libre de toute entrave et, d'autre part, la censure constitue également l'instrument de leur répression sur le plan politique, puisqu'elle restreint leur liberté d'action.

Cette situation, conjuguée au bilan de plus en plus préoccupant de la censure sur l'Internet, nécessite l'adoption de mesures. L'Union européenne, pour sa part, a reconnu cet état de choses et a pris des mesures pour y remédier. L'UE n'accepte pas que les régimes répressifs reçoivent l'aide de sociétés informatiques pour consolider la dictature qu'ils exercent sur les esprits. Nous devons également à l'Union Européenne d'avoir, la première, utilisé le terme extrêmement approprié "cyberrépression" pour désigner de telles pratiques.

L'Union Européenne ne fait pas cavalier seul, puisque le lobby international de l'Internet, qui milite pour la liberté de l'information et l'intégrité de l'Internet à travers le monde, joue un rôle actif et fait preuve de vigilance, en étendant même son action au-delà des nombreuses organisations connues que nous avons déjà évoquées, qui suivent l'évolution de la cyberrépression en la dénonçant publiquement.

Etant donné que les internautes avertis savent comment éviter ou contourner les filtres, un grand nombre de défenseurs de la liberté sur l'Internet au niveau international s'emploient à fournir aux habitants des pays soumis à une censure les

contre-logiciels correspondants tels que ceux décrits plus haut. Ces techniques de lutte contre le filtrage sont d'ailleurs devenues une véritable industrie, qui contribue à réduire l'efficacité de la censure exercée par les gouvernements, sans toutefois pouvoir l'éliminer entièrement. L'initiative Open Net, notamment, joue un rôle actif dans ce domaine, en fournissant des systèmes particulièrement efficaces (comme le système Psiphon), conçus pour permettre à un ordinateur classique de remplir les fonctions de serveur par défaut personnel chiffré, et de contourner ainsi les "pare-feux" obligatoires mis en place par le gouvernement et de naviguer librement sur la Toile. Toutefois, certains fournisseurs de filtres dénoncent activement l'application de ce système et d'autres dispositifs analogues, ce qui illustre à nouveau le caractère problématique des activités commerciales des sociétés multinationales qui, délibérément ou en provoquant des dommages collatéraux non souhaités, facilitent ou favorisent dans les faits la cyberrépression. Bien évidemment, il faut préciser que les pays avancés sur le plan des techniques numériques sont en mesure de concevoir les filtres au niveau national et que bon nombre d'entre eux en fabriquent déjà, ce qui permettra aux fournisseurs de logiciels étrangers de s'en tirer à bon compte.

Comme nous l'avons souligné plus haut, notre but n'est pas ici de procéder à une analyse détaillée par pays, étant donné que l'on trouve sur l'Internet d'amples informations sur ce sujet. Toutefois, le bref aperçu de la situation que nous présentons et les débats publics qui se font jour à cet égard soulèvent la question de savoir comment répondre à la nécessité évidente de prendre des mesures et ce que la communauté internationale peut faire pour lutter contre la cyberrépression, qui constitue une violation du droit international.

La définition des limites d'un filtrage de l'Internet acceptable sur le plan international et les sanctions possibles posent à l'évidence des problèmes juridiques et politiques majeurs. Les questions de juridiction et de souveraineté nationales, le fait qu'il est pour ainsi dire impossible de définir des limites valables au sens large entre les libertés civiles et l'intérêt général supérieur, les questions de choix de la législation applicable et des moyens de la faire respecter et la question plus générale de la gouvernance de l'Internet rendent vaine, et probablement superflue, toute tentative de codification au niveau international. A cela s'ajoute la question de la diversité culturelle et du respect qui s'impose à cet égard. Il ne saurait y avoir une seule et même définition de l'*ordre public* culturel et religieux dans tous les pays, même si l'on peut légitimement concevoir un ensemble universel de convictions fondamentales communes et si la Déclaration universelle et les Conventions doivent être considérées comme universellement contraignantes. Comme c'est le cas essentiellement en droit international, il n'est pas aisé de formuler des définitions et de mettre rapidement en application des sanctions.

Toute réforme du filtrage de l'Internet à l'échelle du globe doit donc être envisagée du point de vue des processus et des *stratégies dans le temps*. Il conviendrait de privilégier *des procédures* susceptibles de susciter une prise de conscience à l'échelle mondiale, de sensibiliser l'opinion et d'exercer des pressions, qui constitueront, pour les gouvernements concernés, un enjeu public majeur et une raison de fournir des justifications détaillées.

Les gouvernements nationaux, les professionnels du secteur et les organismes de la société civile ont une responsabilité importante à cet égard, puisqu'elles ont la capacité de modeler l'opinion. Les gouvernements peuvent encourager la mise au point et la fourniture de techniques anti-filtrage, soumettre l'exportation des techniques de filtrage à des mesures de contrôle des exportations appropriées et recourir à la voie diplomatique au niveau national pour faire pression sur les gouvernements pratiquant une censure, dans un souci de transparence, pour qu'ils rendent publiques et justifient leurs politiques de restrictions.

Le secteur de l'informatique – qu'il s'agisse des fabricants de logiciels et des sociétés fournissant des services FAI et les associations qui en relèvent – ont une responsabilité évidente à cet égard et devraient adopter un code de conduite en vertu duquel leurs techniques ne pourraient être utilisées à des fins de censure politique. Bien qu'il ne soit pas réaliste de demander aux entreprises de faire entièrement abstraction de leurs intérêts économiques, et même s'il serait absurde de rejeter la responsabilité de la censure gouvernementale essentiellement sur le secteur privé, des mesures collectives prises volontairement par les entreprises ont également des retombées sur le plan de l'image, qu'elles contribueront à améliorer. La mise en place d'une politique d'autorégulation, assortie de normes communes précises, a donné de bons résultats au sein de l'Union européenne et permet aussi de renforcer la capacité de résistance des différentes entreprises aux pressions exercées par les gouvernements enclins à pratiquer une censure et désireux de faire affaire avec ces dernières. Ainsi, l'initiative Global Network Initiative, prise par des entreprises spécialisées dans les technologies des Etats-Unis d'Amérique, prescrit l'application de telles normes ("Charte sur la gouvernance"), réagit aux demandes de censure émanant des gouvernements et œuvre en faveur de la liberté sur l'Internet[83].

Les établissements universitaires et les organisations de défense des droits de l'homme qui dénoncent inlassablement la cyberrépression (dont nous avons cité le nom plus haut) sont aujourd'hui de plus en plus encouragés et soutenus par les

---

[83] Global Network Initiative, www.globalnetworkinitiative.org.

gouvernements qui défendent leur action. Toutefois, en raison du caractère transfrontières et international de l'Internet, et de la portée mondiale de la cyberrépression du point de vue des droits de l'homme, l'essentiel est peut-être d'aborder cette question sous un angle radicalement nouveau dans le cadre des programmes des organisations internationales.

En premier lieu, on pourrait parvenir à une large entente au niveau international en ce qui concerne la mise au point et les bases techniques du filtrage actuel de l'Internet et créer un mécanisme de surveillance international.

En deuxième lieu, on pourrait envisager de mettre en œuvre une procédure de réclamations au niveau international, qui serait accessible à toutes les parties concernées et obéirait à un certain nombre de normes d'élaboration de rapports.

A quelle organisation ou instance internationale pourrait-on confier cette tâche?

On pourrait d'emblée envisager de confier cette tâche au Forum sur la gouvernance de l'Internet (FGI), mis en place en 2006 en application des décisions du SMSI ("Agenda de Tunis"). Les restrictions que la censure politique sur l'Internet impose au fonctionnement et à la gestion de la Toile relèvent à l'évidence des tâches assignées à ce Forum pourraient aisément être inscrites dans son mandat (art. 72 a), b), e) et k) de l'Agenda de Tunis), même s'il n'est pas fait expressément mention dans ces textes du problème de la cyberrépression. Malheureusement, le FGI s'est contenté, durant les cinq années qui ont suivi sa création, de procéder à des discussions certes intéressantes et constructives, notamment sur la question de la liberté sur l'Internet, mais n'a entrepris aucune activité opérationnelle. L'élaboration d'une procédure de surveillance permettant de suivre, d'analyser et d'évaluer de manière impartiale les pratiques en matière de filtrage serait donc possible et souhaitable[84], conformément au mandat du Forum, si celui-ci, comme cela semble probable, est prolongé. (Le Forum annuel du SMSI, en revanche, offre un cadre de discussions ouvertes et qui, du fait qu'il n'est pas investi d'un mandat opérationnel, serait donc moins approprié.)

L'UNESCO, qui s'enorgueillit dans le cadre de son acte constitutif d'être le seul garant sur le plan international de la liberté de l'information, a été investie d'un mandat

---

[84] Le FGI a du moins démontré que la question de la censure n'était pas sans rapport avec ses travaux. Au cours des débats actuels sur la poursuite de ses activités et sur la prorogation éventuelle de son mandat, il a été proposé de renforcer le dialogue sur la liberté d'expression et de consacrer davantage d'attention aux dimensions de la gouvernance relatives au développement et aux droits de l'homme. *Voir* le document A/65/78 (E/2010/68) de l'Assemblée générale de l'ONU du 7 mai 2010.

précis par le SMSI, sous les rubriques "Accès à l'information et au savoir" et "Dimension éthique de l'Internet". L'UNESCO a adopté des déclarations et des recommandations par lesquelles les Etats Membres et les organisations internationales s'engagent à assurer un accès libre et sans restrictions à l'Internet[85] et son Directeur général n'a de cesse de dénoncer publiquement les violations de la liberté de l'information et de la presse. Il serait donc parfaitement logique, dans l'exercice de ces tâches, d'engager un dialogue et, à terme, de procéder à un examen périodique des pratiques en matière de censure.

Etant donné qu'il est question ici de droits de l'homme et des deux principales conventions internationales énonçant les obligations qui en découlent pour les Etats, le principal cadre au sein duquel il conviendrait d'entreprendre une action au niveau international devrait être celui des organisations de l'ONU spécialisées dans la défense des droits de l'homme, le Conseil des droits de l'homme créé en 2006 et l'organisme spécialement chargé d'examiner les violations *du Pacte international relatif aux droits politiques et civils*. Le Conseil des droits de l'homme, qui est investi d'un mandat très étendu, serait habilité à mettre en place une procédure de réclamations en bonne et due forme dont pourraient se prévaloir tous les Etats Membres de l'ONU. On pourrait aussi intégrer obligatoirement la question de la liberté sur Internet et de la censure dans le processus d'examen périodique universel, en vertu duquel les résultats de chaque pays en matière de droits de l'homme font l'objet d'une évaluation mutuelle. Quelle que soit la procédure retenue, le fait de mettre en lumière d'une manière collective les violations des droits de l'homme dans ce domaine permettrait d'exercer une pression positive sur les gouvernements soupçonnés d'enfreindre la loi et de leur rappeler les exigences à satisfaire à cet égard, preuves à l'appui. Dans le cadre de cette procédure de réclamations, on pourrait également mettre en avant le rôle ambigu que joue le secteur informatique international dans l'instrumentalisation de la

---

85 "Déclaration sur les principes fondamentaux concernant la contribution des organes d'information au renforcement de la paix et de la compréhension internationale, à la promotion des droits de l'homme et à la lutte contre le racisme, l'apartheid et l'incitation à la guerre", Organisation des Nations Unies pour l'éducation, la science et la culture, 28 novembre 1978, http://portal.unesco.org/en/ev.php-URL_ID=13176&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html; "Recommandations sur la promotion et l'usage du multilinguisme et l'accès universel au cyberespace, Organisation des Nations Unies pour l'éducation, la science et la culture, 15 octobre 2003, http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html (qui préconisent "l'accès universel à l'Internet en tant que moyen de promouvoir le respect des droits de l'homme définis aux Articles 19 et 27 de la Déclaration universelle des droits de l'homme").

cyberrépression. Comme dans le cas du Conseil des droits de l'homme, l'évaluation périodique par pays effectuée par le Comité des droits de l'homme de l'ONU pourrait englober la liberté d'accès à l'Internet.

Même si ces mécanismes de nature purement procédurale présentent des insuffisances, le recours à un système très médiatisé obligeant les intéressés à "se conformer ou à se justifier", qui pourrait aboutir à terme à des pressions de la part du public et susciter une réprobation générale, pourrait même ouvrir la voie à une plus grande sensibilisation de l'opinion mondiale et, en définitive, à une rationalisation des comportements dans l'univers du numérique.

5 Cyberconflit et Géocyberstabilité

5.1 Cyberconflits

Par Giancarlo A. Barletta,[86] William A. Barletta,[87] Vitali N. Tsygichko[88]

Introduction: données du problème

La guerre de l'information est aussi ancienne que les guerres entre les hommes. Les raisons de ces guerres, à de rares exceptions près, sont toujours les mêmes: il s'agit notamment de saper la confiance de l'adversaire, d'endommager ou de détruire ses lignes de communication et de créer une illusion quant à la nature et au règlement du conflit. Ces motivations sont toujours les mêmes. La grande nouveauté du XXI^{e} siècle, qui se caractérise par des infrastructures électroniques de l'information omniprésentes dotées de liaisons numériques dont la largeur de bande ne cesse d'augmenter est: a) que les attaques informatiques capables de détruire le tissu social d'un pays sont toujours plus virulentes et fréquentes; b) qu'il existe un risque réel de dommages matériels importants; c) que les acteurs autres que gouvernementaux, voire les acteurs du secteur privé qui participent aujourd'hui à une guerre asymétrique, ont désormais la possibilité et les moyens de lancer des attaques informatiques soutenues; et d) qu'une situation sous-jacente et généralisée de conflit que l'on pourrait qualifier de "cyberguerre froide" est en train de voir le jour. La généralisation de nouvelles technologies de l'information a considérablement accru les capacités de combat des armements conventionnels et des autres techniques militaires. C'est pourquoi les militaires considèrent aujourd'hui les technologies de l'information et de la communication (TIC) à la fois comme une arme et comme une

---

86 Global Cyber Risk, LLC; Washington, DC, Etats-Unis d'Amérique.

87 Massachusetts Institute of Technology, Cambridge, MA, Etats-Unis d'Amérique.

88 Institute for Systems Analysis, Russian Academy of Sciences, Moscou, Russie.

cible et assimilent le cyberespace à un espace de conflit, au même titre que l'air, l'espace, la terre ou les océans[89].

Ces vingt dernières années, les pays industrialisés ont mis en place des réseaux ubiquitaires grâce auxquels il est possible de relier les principales ressources économiques, matérielles et sociales par l'intermédiaire des TIC pour améliorer leur niveau de vie, promouvoir la prospérité économique, étendre leur influence et renforcer leur place sur la scène internationale. De même, pour les pays en développement, les technologies de l'information représentent un moyen rapide, sur le plan économique, de participer pleinement à l'économie mondiale. Les dispositifs intelligents destinés au secteur (qui contiennent à la fois des détecteurs et des microprocesseurs) ne manquent pas, tout comme les équipements grand public dotés de microprocesseurs et de fonctionnalités hertziennes (ou cellulaires), par exemple les téléphones cellulaires, les assistants numériques personnels et les agendas électroniques. L'existence de réseaux de communication étendus permet d'utiliser à grande échelle des ressources informatiques pour faciliter le commerce, fournir des services, surveiller l'environnement et traiter des problèmes de société complexes. Tous ces dispositifs évoluent rapidement et offrent la possibilité de communiquer avec d'autres dispositifs en tout point du globe.

Comme le fait observer un ancien général de l'armée américaine, ces mêmes TIC permettant de connecter les principales ressources économiques, physiques et sociales ont été adoptées et adaptées par l'armée et des groupes paramilitaires, ce qui a contribué à une véritable révolution dans le domaine militaire, révolution qui est en train de bouleverser la manière dont les guerres sont planifiées, organisées et menées. Cette "révolution" s'accompagne d'une évolution dans la manière d'effectuer des missions de renseignement, de surveillance et de reconnaissance, de commander et de contrôler les forces armées et leurs opérations, d'optimiser les mouvements logistiques, de permettre la navigation de précision et l'emploi d'armes "intelligentes". Chose très importante: cette révolution permet aussi d'utiliser le "réseau" comme

---

89 Ainsi, "Les forces aériennes des Etats-Unis ont pour mission de fournir des options souveraines pour la défense des Etats-Unis d'Amérique et de ses intérêts à l'échelle mondiale, à savoir voler, combattre et gagner dans l'espace aérien, l'espace et le cyberespace". Sovereign Options for Securing Global Stability and Prosperity", 26 mars 2008, Office of the Secretary of the Air Force, www.stormingmedia.us/98/9868/A986884.html. Le point de vue des Etats-Unis est présenté plus en détail dans la publication Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues, Congressional Research Service (CRS) Report, RL31787, 14 septembre 2006, www.fas.org/irp/crs/RL31787.pdf (dénommé ci-après "CRS Report").

support à partir duquel, par l'intermédiaire duquel et dans lequel il est possible de conduire des opérations militaires[90].

Les technologies de l'information favorisent et facilitent de nouvelles relations de cause à effet au sein des sociétés et permettent naturellement de stimuler la croissance économique, de progresser dans le domaine des droits de l'homme et de faire connaître la répression exercée par certains gouvernements. Les autorités nationales de commandement ont accès à une communication verticale nettement facilitée et, chose plus importante encore sous l'angle du progrès des droits de l'homme et du bien-être économique, les flux d'information ascendants et horizontaux n'ont cessé de s'accroître. Les sociétés modernes de l'information augmentent continuellement tant le nombre et les caractéristiques des nœuds d'information (où l'information est créée et utilisée) que le nombre et la largeur de bande des liaisons. En outre, de plus en plus de nœuds et de liaisons sont dotés de capteurs autonomes de leur statut opérationnel.

Cette connectivité fortement non linéaire a pour conséquence d'accroître simultanément la résistance du réseau informatique et les risques ainsi que les retombées des attaques malveillantes dont sont victimes les nœuds et les liaisons du réseau dorsal ainsi que les difficultés qu'il y a à prévoir les conséquences de défaillance des réseaux. L'essor rapide des TIC et l'évolution de la société mondiale de l'information qui en résulte pourraient avoir des retombés géopolitiques négatives très diverses: accélération de la polarisation mondiale entre pays riches et pays pauvres, fracture technologique grandissante entre pays très industrialisés et pays en développement, excluant ainsi un nombre croissant de pays marginalisés sur le plan économique de toute évolution de la civilisation et favorisant l'instabilité politique et les conflits. En conséquence, à mesure que la complexité des réseaux de l'information évolue, le risque de guerre de l'information tend à faire peser des risques grandissants sur les valeurs de la société.

Interdiction publique des cyberattaques et cyberguerre menée par les gouvernements

Les agressions contre les réseaux et systèmes informatiques et contre les données numériques ont donné lieu à la promulgation de législations sur la cybercriminalité dans maints pays. Bien que la plupart des pays industrialisés aient adopté une

---

[90] Gen. John Casciano, "Threat Considerations and the Law of Armed Conflict", août 2005 (on file with WFS Information Security PMP).

législation en matière de cybercriminalité, les différences importantes qui existent lorsqu'il s'agit de définir ce que l'on entend par cyberdélit, de détecter et d'identifier un comportement délictueux dans le cyberespace et dans les dispositions de procédure et de fond applicables ont considérablement freiné la coopération internationale en vue de fournir une assistance pour les enquêtes sur la cybercriminalité. La Convention sur la cybercriminalité du Conseil de l'Europe a été élaborée sous la forme d'un accord multilatéral destiné à harmoniser les législations sur la cybercriminalité à l'échelle mondiale. Toutefois, la réalité n'a pas été à la hauteur des attentes, puisque seuls 26 pays avaient ratifié la Convention du Conseil de l'Europe à la mi-2010, soit près de neuf ans après son ouverture à la signature. Le kit d'aide en ligne de l'UIT sur la législation relative à la cybercriminalité a été élaboré pour offrir une solution de rechange plus souple et offre des exemples de textes législatifs harmonisés avec la Convention du Conseil de l'Europe et les diverses législations sur la cybercriminalité des pays industrialisés, que les pays du monde entier peuvent utiliser lorsqu'ils rédigent ou modifient leurs propres lois en la matière.

Parmi les autres lois applicables à certains types de cyberactivités figurent celles destinées à assurer la protection des systèmes et équipements matériels des fournisseurs de communications, les dispositions en vertu desquelles les activités d'espionnage économique sont interdites, les lois sur la propriété intellectuelle, etc. En somme, ces législations visent à interdire juridiquement les différents types de cyberattaques contre les infrastructures, les systèmes et les données, quels qu'ils soient.

L'émergence de technologies de l'information toujours plus performantes et omniprésentes élargit constamment l'éventail des possibilités qui s'offrent aux utilisateurs. Il n'est donc pas surprenant que les pays aient de bonnes raisons de légiférer sur les comportements dans le cyberespace, quel que soit au demeurant leur propre comportement vis-à-vis d'autres pays. Etant donné que les technologies de l'information ne connaissent pas les frontières internationales, les cyberdélinquants n'ont jamais à se rendre physiquement dans l'Etat où se trouve la victime. Il faudrait donc prévoir de plus fortes incitations en faveur d'une coopération entre les Etats-nations, d'autant que les ressources informatiques des Etats constituent une cible particulièrement attrayante pour les cyberdélinquants. Au reste, les organisations à vocation internationale telles que l'UIT ont fait de la coopération une de leurs priorités, tant pour promouvoir une collaboration fructueuse dans les réseaux d'information et par l'intermédiaire de ces réseaux que pour éviter ou, du moins, décourager les agissements répréhensibles dans le cyberespace.

Etant donné que les gouvernements ont de plus en plus recours à l'Internet pour faciliter la diffusion d'informations et de services à leurs citoyens, la société de

l'information représente une cible attrayante pour les escrocs, qu'il s'agisse de délinquants, de groupes terroristes sous-nationaux ou d'Etats-nations hostiles. L'agression[91] lancée contre l'infrastructure nationale de l'information de l'Estonie en avril 2007 illustre bien la vulnérabilité prévue d'un cybergouvernement et l'absence de facteurs qui auraient permis de décourager les cyberdélinquants. Bon nombre de spécialistes ont affirmé à cet égard que la complexité technique de l'agression dépassait largement celle d'incidents signalés précédemment. Certains vont jusqu'à dire que cette attaque a été menée en connivence ou avec la complicité d'une entité nationale, mais plusieurs experts des Etats-Unis ont écarté de telles hypothèses. Il convient cependant de faire observer que l'affaire estonienne n'as pas été accompagnée d'exigences politiques ou financières, ni même de revendications de la part des auteurs supposés de l'attaque[92], rendant ainsi peu probable l'hypothèse d'une escroquerie sans motivations politiques. Les affaires GhostNet[93] et Aurora qui ont eu lieu en 2009 sont d'autres exemples de cyberattaques de plus grande envergure. L'une de ces attaques visait les serveurs de Google et faisaient partie d'une opération d'espionnage industriel et politique apparemment concertée, qui "a exploité les failles de sécurité de pièces jointes électroniques pour s'infiltrer dans les réseaux

---

91 On a beaucoup parlé de cette cyberattaque dans la presse internationale. Voir par exemple l'article: "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, 17 mai 2007, www.guardian.co.uk/world/2007/may/17/topstories3.russia.

92 Début juin, un responsable du Groupe de la jeunesse russe pro-Poutine a déclaré être à l'origine de l'attaque. www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html. On ignore si cette déclaration est fondée ou non.

93 *Tracking GhostNet: Investigation of a Cyber Espionage Network*, Information Warfare Monitor, 1 septembre 2009, www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/. "L'enquête a finalement relevé que plus de 1 295 serveurs avaient été contaminés dans 103 pays. On considère que pas moins de 30% des serveurs infectés constituaient des cibles de choix, parmi lesquelles on retrouve des ordinateurs de Ministères des affaires étrangères, d'ambassades, d'organisations internationales, d'agences de presse et d'ONG. Les systèmes informatiques tibétains qui ont fait l'objet de notre enquête ont été infectés par d'innombrables intrusions qui ont permis aux pirates d'avoir un accès sans précédent à des renseignements potentiellement sensibles. Mais il serait illusoire de croire que tous les logiciels malveillants de la Chine sont utilisés par l'Etat chinois pour mener des opérations d'espionnage ciblées ou délibérées. Les chiffres montrent en effet que la Chine compte aujourd'hui le plus grand nombre d'internautes au monde. Le nombre élevé de jeunes de la génération du numérique explique aussi en grande partie l'essor des logiciels malveillants chinois. Du fait de l'accroissement du nombre d'internautes ingénieux, il est à prévoir que la Chine (et les chinois) représentera une proportion accrue des cyberdélits."

de grandes sociétés financières, de défense et de technologie et d'instituts de recherche des Etats-Unis"[94].

Comme le montre l'affaire estonienne, des cyberattaques puissantes et de grande envergure peuvent constituer *de facto* une agression directe et réelle contre des entités civiles et publiques, dont l'ampleur dépasse la simple criminalité. Les caractéristiques de telles offensives peuvent être les suivantes: a) dommages matériels importants causés à des installations essentielles; b) multiples préjudices ou perte de vies humaines; c) déstabilisation des institutions financières; et d) interruption du fonctionnement des infrastructures essentielles. La coordination ou la continuité de telles agressions pendant de longues périodes peut même en aggraver les conséquences. Dans ces conditions, les Etats-nations, qu'ils connaissent ou non l'identité ou les motifs des cyberdélinquants, pourraient considérer[95] une cyberattaque de grande ampleur comme un acte de terrorisme ou l'équivalent fonctionnel d'une agression armée justifiant un examen particulier et un traitement spécial.

Il faudrait tout au moins que le risque démontré de désorganisation à grande échelle d'une société de l'information suscite une culture de la coopération mutuelle au-delà des frontières nationales. Dans le cas de l'Estonie, les autorités, en réponse à la première série d'incidents visant les sites gouvernementaux, ont lancé des plans d'intervention qui prévoyaient une série d'attaques contre les services financiers, tels que les opérations bancaires en ligne. Or, en l'espace de quelques jours, "[les services bancaires du secteur privé et les organes d'information en ligne ont été massivement touchés et les attaques ont compromis le fonctionnement du reste de l'infrastructure réseau de l'Estonie]"[96]. Pendant la même période, les mesures de parade prises en coopération avec les fournisseurs d'accès à l'Internet du monde entier ont consisté à renforcer le blocage du trafic provenant de certaines groupes d'adresses IP et de verrouiller le système bancaire estonien pour l'isoler de la totalité du trafic

---

94 Ariana Eunjung Cha et Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say", The Washington Post, 14 janvier 2010, www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

95 Ainsi, en 2009, l'ancien directeur des services de renseignements des Etats-Unis, Mike McConnell, a classé les cyberarmes dans la catégorie des armes de destruction massive (ou qui pourraient le devenir) CRS Report at 3.

96 "ENISA commenting on massive cyber attacks in Estonia", communiqué de presse de l'ENISA, 24 mai 2007, www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia.

international. Il est intéressant de noter que les ressources nécessaires pour accroître la portée des cyberattaques ont nettement dépassé les ressources utilisées pour lancer ces attaques.

Ce déséquilibre marqué entre les agressions et les moyens de défense dans le cyberespace n'est pas passé inaperçu. Sauf en cas d'attaques de si grande envergure, les organismes militaires et les services de renseignements des Etats-Unis et d'autres Etats-nations (Russie, Chine, Inde, Pakistan et Iran) "procèdent déjà à des recherches et à des vérifications pour identifier les réseaux numériques qui peuvent être exploités par suite de failles entre les adversaires potentiels". Dans ces pays, les décideurs agissent comme si nous vivions déjà à l'ère de la cyberguerre. De fait, ce sont des pays comme les Etats-Unis qui disposent d'installations asymétriques et de la capacité de lancer ou de parrainer des cyberattaques (notamment dans le cadre d'opérations secrètes) contre les pays moins bien équipés pour réagir en conséquence. En outre, les autorités de ces pays, et d'autres pays d'ailleurs, savent parfaitement que cet écart important entre agressions et moyens de défense, lorsqu'il va de pair avec le quasi-anonymat d'un cyberdélinquant donné, permet de recruter, directement ou indirectement, de petits "groupes" de cybermercenaires ou de "combattants illégaux" qui fournissent aux autorités nationales des arguments plausibles pour nier être à l'origine d'une attaque.

Dans la pratique, les dommages que peut causer une attaque varient considérablement selon l'état de préparation de la société et les dispositifs de sécurité intégrés dans l'infrastructure visée par l'agression. Pour les décideurs politiques ou militaires, "l'important, pour lutter contre une cyberattaque, est de déterminer rapidement la nature de l'attaque et le type d'adversaire, puis de réagir comme il se doit. Aujourd'hui, la localisation des intrusions informatiques relève des autorités chargées du maintien de l'ordre ... Les forces armées traditionnelles n'ont pas le droit d'exécuter cette mission au niveau national ... [de sorte que] les forces de l'ordre jouent un rôle déterminant dans la sécurité et la défense nationales[97]". Il s'ensuit que les Etats-nations, tant pour leurs institutions militaires que pour les forces de l'ordre, ont besoin de puissants outils numériques d'expertise judiciaire, d'une structure juridique adaptée à leur utilisation, de solutions crédibles pour préserver l'intégrité des preuves et de sanctions véritablement dissuasives pour les auteurs des infractions.

---

97 Bonnie N. Adkins, "The Spectrum Of Cyber Conflict: From Hacking to Information Warfare: What Is Law Enforcement's Role?" Air Command and Staff College, Maxwell Air Force Base, AU/ACSC/003/2001-04, avril 2001, http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA406949.

Etant donné que ces outils peuvent avoir un "double usage", les pays dotés des moyens d'expertise judiciaire et des capacités de lutte informatique défensive les plus performants et les plus souples disposeront *a fortiori* de capacités offensives et de moyens de cyberespionnage considérables. Même si cette possibilité de double usage et l'écart entre les capacités offensives et défensives existent également dans le domaine des armements traditionnels, la notion de dissuasion et la facilité relative avec laquelle il est possible de déterminer l'origine de l'attaque excluant (pas complètement) toute probabilité d'attaque classique.

Interactions entre guerre de l'information et guerre classique

La mise en œuvre généralisée des nouvelles techniques de l'information renforce et multiplie les possibilités de combat des armements et des techniques militaires conventionnels. Les techniques de l'information rendent en effet possibles des modifications qualitatives dans les domaines militaire, de la reconnaissance ainsi que des communications. Grâce à ces techniques, il est possible d'accroître de manière spectaculaire le débit de traitement de volumes considérables de données et de prendre des décisions opérationnelles complexes, ce qui permet de recourir à des méthodes radicalement nouvelles de contrôle des troupes et des armements tant au niveau stratégique qu'au niveau tactique. Les nouvelles technologies de l'information renforcent considérablement les capacités de combat des installations de guerre électronique et donnent naissance à de nouveaux types d'armements, notamment à des armes informatiques conçues pour nuire à l'infrastructure informatique, militaire et civile d'un adversaire en pénétrant dans ses réseaux informatiques.

Pour les forces armées, la révolution informatique et technique permet d'accroître considérablement les capacités de combat des troupes, non seulement en transformant les formes et les méthodes des différents types de guerres, mais aussi en modifiant le modèle classique de combat militaire et d'escalade des conflits. D'après des experts des Etats-Unis, en ciblant de manière sélective des armes informatiques sur les infrastructures informatiques essentielles, militaires ou civiles, d'un adversaire, on pourrait mettre fin à un conflit avant même l'ouverture d'hostilités classiques entre les parties, étant donné qu'une escalade des agressions informatiques aurait des conséquences catastrophiques. La possession d'armes informatiques confère une supériorité indéniable sur les pays qui en sont privés. Les variables informatiques et politiques de la confrontation entre les puissances l'emporteront inévitablement, à terme, sur les variables nucléaires. Par contre, tous les pays, et en particulier les pays les plus développés, sont vulnérables aux armes informatiques. Ces armes, tout comme les armes nucléaires, peuvent constituer un facteur de pression politique et de dissuasion.

La guerre de l'information, loin de se résumer à une simple réalité virtuelle de jeux informatiques, constitue un outil tangible permettant d'emporter la victoire lors d'un conflit militaire ou politique. Il ne fait aucun doute que comme les armes informatiques sont devenues une composante essentielle de la puissance militaire d'un pays, de nombreux pays, en particulier les Etats-Unis et la Chine, se préparent activement et en permanence à la guerre de l'information.

Caractéristiques des armes informatiques

Lorsqu'il s'agit de formuler un modèle de sécurité de l'information, l'un des problèmes consiste à définir et à déterminer ce que l'on entend par "arme informatique". Quelles sont les particularités des armes informatiques? A quel niveau (le cas échéant) un cyberconflit doit-il être considéré comme un conflit armé? Du fait qu'il n'existe aucun consensus international sur ces questions, il est impossible d'engager des négociations constructives sur la sécurité informatique mondiale. On pourrait définir une "arme informatique" comme une arme capables de nuire à des infrastructures informatiques militaires et civiles[98]. L'inconvénient de cette définition est que tous les types d'armements, y compris les armements conventionnels, peuvent entrer dans la catégorie des armes informatiques, s'ils sont capables d'endommager des éléments d'une infrastructure de l'information. Ainsi, est-il important de savoir quel dispositif a rendu inopérationnel le système de contrôle d'une économie nationale (code de programme, impulsion électronique intensive ou impact direct d'un explosif conventionnel)? On pourrait aussi faire valoir que les armes informatiques s'entendent de tous les moyens de destruction utilisant les TIC.

Lorsqu'on aborde la question des cyberconflits, il faut éviter de réduire les obstacles à la guerre en adoptant des définitions qui englobent les activités habituellement menées en temps de paix. Quelles sont les caractéristiques particulières des armes informatiques? A quel stade faut-il considérer un cyberconflit comme un conflit armé? Il serait peu judicieux, voire dangereux pour la stabilité internationale, de traiter comme des "conflits armés" les conflits qui ne font peser aucune menace réelle sur la vie humaine ou la liberté de la société. En outre, comme la quasi-totalité des systèmes

---

98 "Tout moyen ou dispositif, ou toute combinaison de capacités et de techniques, qui, s'il est affecté à l'usage auquel il est destiné, est susceptible de compromettre l'intégrité ou la disponibilité de données, d'un programme ou d'informations dans un ordinateur ou un système de traitement informatique". Graham H. Todd, "Armed Attack In Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition", Air Force Law Review, Vol. 64, 2009, 65 – 102, http://lawlib.wlu.edu/CLJC/index.aspx?mainid=418&issuedate=2010-03-23&homepage=no.

d'armements perfectionnés utilisent les TIC, il est extrêmement difficile, pour ne pas dire impossible, de dissocier les armes informatiques de la gamme complète des armements. Sachant que la guerre de l'information est un phénomène qui a toujours existé dans l'histoire des guerres, il est très difficile de formuler une définition précise, en raison même de ces différents niveaux de complexité théorique. Ainsi, dans quelle catégorie faut-il classer la fourniture délibérée de renseignements erronés, ou encore l'espionnage ou l'interception de flux d'information? Les points de vues sur ces activités seraient fortement influencés si elles étaient menées à bien pendant une guerre cybernétique.

Les caractéristiques opérationnelles importantes des armes informatiques sont 1) leur coût relativement modique et leur accessibilité; 2) leur possibilité d'évolution latente, d'accumulation et de mise en œuvre; et 3) leur extraterritorialité intrinsèque et le caractère anonyme de leur impact. Autant de caractéristiques qui permettent aux armes informatiques de se propager de manière incontrôlée et en font un problème de portée mondiale lorsqu'elles sont aux mains de régimes autoritaires. Du fait que ces armes informatiques représentent une grave menace pour la paix et la stabilité internationales, la communauté internationale doit suivre de près les menaces contre les infrastructures nationales et mondiales de sécurité de l'information en prenant des mesures concrètes en vue de les neutraliser. Les TIC, qui font partie intégrante de l'infrastructure des sociétés modernes, figurent donc au nombre des divers instruments qu'un pays peut utiliser pour lutter contre ses ennemis.

Un grand nombre de pays prennent actuellement des mesures pour contrer les menaces qui pèsent sur la sécurité de l'information. L'efficacité de ces mesures, aussi rigoureuses soient-elles, est cependant amoindrie par le caractère transnational de la menace et l'anonymat des agresseurs. En pareils cas, aucun pays ne peut s'estimer à l'abri s'il tente de faire cavalier seul pour lutter contre ces menaces informatiques. Ce n'est qu'en mettant en place un système international de sécurité informatique et en œuvrant de manière concertée que l'on pourra remédier à la prolifération des armes informatiques et réduire les menaces que présentent la guerre de l'information, le terrorisme informatique et la cybercriminalité.

On peut affirmer sans ambigüité que les logiciels conçus exclusivement pour détruire des infrastructures de l'information (virus, signets, etc.), sont des "armes informatiques". La plupart des moyens de lutte armée perfectionnés, lorsqu'ils font usage des TIC, sont polyvalents, c'est-à-dire qu'ils sont destinés non seulement à détruire des infrastructures de l'information, mais aussi à effectuer d'autres opérations de combats. Les pays possédant des systèmes d'armements et des moyens de reconnaissance, de communication, de navigation et de commande aussi perfectionnés, qui reposent tous sur l'utilisation à grande échelle des TIC, détiennent

incontestablement un avantage décisif sur le plan militaire. Il y a peu de chances, dès lors, qu'ils concluent un jour des accords qui viendraient limiter ces avantages stratégiques.

En conséquence, la question même de l'interdiction ou de la réduction de la production, de la prolifération et de l'utilisation d'armes informatiques portera sans doute uniquement sur les armes à usage unique visant exclusivement à détruire des composantes de l'infrastructure de l'information, par exemple celles fondées sur des codes de programme, c'est-à-dire les différents virus et moyens de les propager. Malheureusement, la grande majorité des TIC modernes, qui peuvent être utilisées à des fins militaires, terroristes et criminelles, sont conçues par des industries civiles, de sorte qu'il est très difficile de contrôler leur développement et leur prolifération.

Les instruments utilisés aux fins des cyberconflits et de la guerre de l'information font peser de réelles menaces, en particulier pour les pays développés, dont toutes les activités essentielles sont déterminées par des infrastructures de l'information complexes[99]. Ce n'est qu'en déployant des efforts concertés pour sécuriser les infrastructures essentielles de l'information au niveau national que la communauté internationale parviendra à contrer la menace que constitue l'utilisation des technologies de l'information à des fins malveillantes. En instaurant un consensus sur les systèmes informatiques de ce type, il sera possible d'arrêter des stratégies de dissuasion plus efficaces et de prendre des mesures de protection mieux adaptées, assorties du droit de recourir à des mesures de rétorsion, au cas où des actes de malveillance informatique auraient des conséquences directes, graves et inacceptables. Toutefois, la plus grande prudence est de mise, même dans ce domaine. Il ne serait pas justifié, au seul motif qu'une agression informatique a été commise, d'engager une guerre classique et il serait peu judicieux de donner aux gouvernements des arguments pour agir dans ce sens de leur propre initiative.

Limiter les cyberconflits

Les fortes disparités qui peuvent exister entre les techniques informatiques offensives et défensives font que des utilisateurs finals peuvent lancer des "cyberguerres"

---

99 La décision des forces armées des Etats-Unis de ne pas lancer de cyberattaque contre les systèmes financiers iraquiens est traitée dans la publication Information Warfare and Cyberwar: Capabilities and Related Policy Issues, Congressional Research Service, RL31787, 19 juillet 2004, pages 5-6, www.fas.org/irp/crs/RL31787.pdf. Ce rapport du service CRS décrit également le cadre dans lequel l'armée américaine lutte contre la guerre électronique et explique la place que celle-ci occupe dans la stratégie et les programmes militaires à long terme en matière de guerre de l'information.

personnelles contre l'infrastructure essentielle de l'information d'une société presque aussi efficacement que des Etats-nations. En conséquence, le régime juridique et politique visant à décourager et à limiter les cyberconflits entre les nations sera lié dans la pratique aux cadres juridiques et de procédure destinés à décourager et à lutter contre le cyberterrorisme et la cybercriminalité.

Dans le contexte de la société de l'information, la notion de dissuasion par le biais de sanctions civiles ou pénales peut être viable sur le plan de la criminalité ou du "cyberactivisme"[100], à condition que l'on assure un degré d'homogénéité suffisant au niveau international entre les codes pénals. Malheureusement, lorsqu'il est question de cyberattaques de la part d'Etats-nations, le principe de dissuasion apparu pendant la guerre froide perd de son utilité, étant donné qu'une contre-offensive de même nature risque de nuire à la connectivité sociale et physique sur le plan international, à un point qui serait inacceptable tant pour les parties tierces que pour les auteurs de la contre-offensive. Dans le cyberespace, les effets de ces dommages collatéraux peuvent se faire sentir à l'échelle mondiale, comme on l'a vu à plusieurs reprises avec la propagation rapide de logiciels malveillants tels que les virus informatiques. Dans le cas intermédiaire du cyberterrorisme, le comportement qu'ont eu récemment les Etats-Unis à l'égard des "combattants illégaux" dans leur "guerre contre le terrorisme" laisse penser que le modèle de dissuasion fondé sur des sanctions civiles ou pénales a là aussi échoué.

Même si les difficultés liées à la dissuasion encouragent la recherche de moyens de défense technologique ultra-perfectionnés contre les cyberattaques, l'histoire des autres types d'armements montre que le fond même d'un problème sociopolitique doit être traité en dernier ressort au niveau sociopolitique. Sur le plan politique, les graves conséquences potentielles d'un cyberconflit international appellent une attention immédiate. Etant donné que les technologies peuvent avoir un double usage, il est impossible de recourir à un système de contrôle international comparable à celui utilisé pour réglementer les techniques nucléaires. On ne peut qu'espérer (et œuvrer dans ce sens) que sera créé un cadre juridique transnational qui définira les règles et les sanctions applicables en cas de cyberconflits, qui feront l'objet d'un ensemble d'accords contraignants structurés et négociés au niveau international. De

---

100 Par "activisme informatique" on entend le fait d'élaborer ou d'utiliser un code informatique (piratage informatique) pour attaquer un réseau TIC-cible, en vue de promouvoir une idéologie politique ou un objectif social. Les activistes informatiques décrivent souvent leur action comme des actes de protestation ou de désobéissance civile. Voir par exemple, http://thehacktivist.com/hacktivism.php.

telles règles devront préciser les obligations incombant aux Etats signataires s'agissant du contrôle des organisations ou des réseaux non gouvernementaux opérant à l'intérieur de leurs frontières.

Bien que les attaques cyberterroristes ou de cyberespionnage relèvent généralement de la législation civile et pénale générale, certaines caractéristiques de ces agressions pourraient justifier l'adoption d'une législation spéciale, qui donnerait lieu à des considérations particulières du point de vue juridictionnel. Ces caractéristiques sont les suivantes: 1) préjudice important à connotation politique; 2) difficultés accrues pour identifier, arrêter et poursuivre les auteurs des infractions; et 3) existence de motivations politiques importantes destinées à déstabiliser la société, en violation des principes communément admis en matière de droit pénal et de droit des conflits armés. Un autre argument milite en faveur d'un traitement spécial en matière de cyberterrorisme, à savoir "qu'en général, une intervention spéciale peut être justifiée lorsque le terrorisme émane d'un groupe capable de s'organiser collectivement de manière durable, d'exécuter des projets et des opérations complexes et d'agir en marge de toute vie normale, ou disposant de moyens d'intimidation de la société, pour qu'elle tolère sa présence"[101]. Les cyberconflits prolongés menés à des fins terroristes ou militaires, exigent parfois une action internationale concertée visant à limiter ou à contrôler l'usage de la force.

Pour qu'il soit efficace, un système de contrôle devra également codifier les mesures susceptibles d'être prises pour lutter contre les agresseurs autres que des Etats, à condition que l'on puisse les identifier. En cas d'actes terroristes provenant du pays victime de l'agression, il est possible de prendre des mesures contre l'auteur de l'agression dans le contexte du droit pénal en vigueur dans le pays, et notamment dans le cadre des lois antiterroristes. Si l'agression est lancée par des Etats neutres ou coopératifs, il existe plusieurs solutions possibles: 1) extradition vers l'Etat victime de l'attaque; 2) poursuites au niveau national dans un pays neutre à partir duquel l'attaque a été perpétrée; ou 3) extradition vers un pays tiers qui revendique le principe de compétence universelle et le respect des principes généralement admis en matière d'application correcte de la loi. La solution à retenir dépendra de diverses considérations et devra concilier la participation de l'Etat d'origine, l'apparence de justice et les mesures propres à encourager le rejet des méthodes terroristes par la communauté internationale.

---

101 Clive Walker, "Cyber-Terrorism: Legal Principle and the Law in the United Kingdom", Penn State Law Review, Vol. 110, 2006, 625-65, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109113#%23.

Lorsque des attaques informatiques sont lancées depuis des Etats peu scrupuleux ou peu enclins à coopérer, il y a peu de chances que l'on puisse avoir recours aux circuits de coopération classiques pour mener une enquête, arrêter et poursuivre les auteurs de l'attaque ou, le cas échéant, procéder à leur extradition. Le principal problème est de déterminer si le ou les auteurs de l'agression seront poursuivis dans l'Etat victime des attaques, dans un Etat tiers neutre ou devant la Cour pénale internationale. De telles affaires posent alors naturellement la question de l'intervention par la force ou de l'application de sanctions internationales et sont analogues à celles qui se posent en cas de terrorisme par des moyens classiques. Les solutions qui s'offrent aux pays victimes de telles attaques sont les suivantes:

1. mesures de rétorsion à l'encontre du pays concerné;
2. intrusion illicite et arrestation[102] des auteurs présumés des agressions; et
3. respect approprié de la souveraineté par le biais de la participation d'un Etat tiers agissant comme intermédiaire.

Si l'on devait concevoir un système dans lequel certains types d'opérations seraient interdits dans le cyberespace, par analogie avec les Conventions de Genève sur les conflits armés classiques, on pourrait fort bien envisager une juridiction universelle à laquelle participerait un groupe international. Toutefois, on s'engagerait ainsi sur le terrain glissant des arguments concernant le non-droit sur l'Internet. A noter que la Convention du Conseil de l'Europe sur la cybercriminalité n'identifie, et par conséquent n'autorise, aucun motif justifiant la recherche de preuves transfrontières sur les réseaux informatiques, même en cas d'opérations de poursuite.

Conclusion

Il est admis que: 1) la plupart des entreprises, des gouvernements et des services publics des pays sont fortement tributaires de l'ordinateur et de l'Internet; 2) que, bien que l'Internet soit par nature résistant du point de vue de la connectivité, les ordinateurs qui lui sont reliés sont beaucoup plus vulnérables aux attaques; 3) l'acquisition de moyens d'attaque relativement puissants nécessite de nos jours assez peu d'investissements; et 4) il est difficile d'identifier avec certitude l'origine d'une attaque.

---

102 En vertu de la législation des Etats-Unis, le fait de traiter le cas d'un suspect dans une juridiction territoriale ne constitue pas un argument de défense face à l'accusation.

S'agissant des législations sur la guerre classique, la plupart des pays pourraient adopter un certain nombre de principes généraux afin d'instaurer un ordre harmonieux dans le cyberespace.

1. Les cyberattaques ciblant des infrastructures essentielles ne constituent pas des armes d'attaque légitimes même en cas de guerre classique (par analogie avec les armes biologiques ou chimiques).
2. Etant donné que l'espionnage sur Internet financé par les gouvernements se généralise, il est de plus en plus difficile d'identifier les intrusions et les désordres imputables au crime organisé, à des organisations sous-nationales et à des pirates informatiques, ce qui entrave la poursuite en justice de ces groupes en application des législations sur la cybercriminalité.
3. Même si l'espionnage informatique à petite échelle de la part des gouvernements peut être toléré, aucun acte de sabotage ne saurait être admis. La "concurrence" entre les Etats à un niveau relativement faible stimule le progrès technique et les pays ont tout intérêt à savoir que la sécurité des systèmes militaires étrangers est assurée contre des agresseurs potentiels.
4. L'espionnage de sociétés étrangères privées de la part d'un gouvernement a des conséquences difficiles à déterminer, mais sans doute relativement limitées dans la réalité. Toutefois, il suscite un élan nationaliste malsain au sein de la population, envoie des messages négatifs aux entreprises et tend à créer un pouvoir économique en marge de la concurrence, notamment si cet espionnage est effectué en faveur d'une entreprise privée du pays considéré.
5. Etant donné qu'il est très difficile de déterminer l'origine d'une attaque et de savoir si elle a été financée ou non par un gouvernement, les entités non gouvernementales déstabilisatrices peuvent être à même de provoquer un conflit national.

Etant donné qu'il est parfois impossible de vérifier que les accords officiels sont respectés, on pourrait peut-être, dans le cadre du dialogue international, établir des règles relatives aux preuves nécessaires pour veiller à ce que soient observés les principes de loyauté. Dans cette optique, les affirmations quant à l'avantage économique ou à la dynamique politique fondamental semblent supposer une dynamique de "Guerre froide" qui saperait les objectifs mêmes que l'on chercherait à atteindre dans le cadre d'un accord international[103]. Chose plus importante encore: si

---

103 Voir l'article "A Concept of Cyber peace" de Henning Wegener cité dans cet ouvrage.

ces affirmations sont vraies, aucun accord de l'ONU ne parviendrait à stopper ce processus.

Pour promouvoir l'objectif consistant à réduire le nombre de cyberconflits, il faut engager une réflexion théorique sur les questions suivantes, pour faciliter les discussions politiques au sein des instances internationales:

1. théorie de la dynamique offensive/défensive de la sécurité informatique;
2. dynamiques offensive/défensive du développement de la sécurité informatique sous l'angle des retours sur investissement;
3. obstacles créés par certains systèmes de sécurité robustes pour les opérations (traitement informatique, stockage des données, gestion des systèmes, durée de l'interface humaine);
4. incitations et éléments de dissuasion pour les cyberdélinquants s'agissant de la criminalité transfrontières;
5. incidences de l'espionnage informatique sur les secteurs public et privé.

5.2 Pour une géocyberstabilité

Par Jody R. Westby

Le rythme auquel la cybercriminalité se développe est impossible à suivre. Chaque jour, des personnes mal intentionnées utilisent des botnets pour se procurer des informations confidentielles et privées et mener des attaques par déni de service distribué contre les systèmes de gouvernements et d'entreprises. Selon le rapport *Unsecured Economies: Protecting Vital Information* publié par McAfee en 2009, les entreprises consultées auraient subi des pertes en termes de propriété intellectuelle s'élevant à 4,6 milliards USD au total en 2008 et dépensé environ 600 millions USD pour réparer les dommages liés à la violation des données. A partir de ces chiffres, McAfee a estimé par projection les pertes subies par les entreprises à l'échelle mondiale à plus de mille milliards USD en 2008. Quant aux particuliers, ils doivent mettre à jour en permanence les logiciels d'exploitation et les programmes de protection contre les virus qu'ils utilisent, ce qui n'empêche toutefois pas qu'un grand nombre de leurs systèmes soient infectés et utilisés dans le cadre d'attaques.

Les pays sont conscients que leurs systèmes et ceux de leurs entreprises sont précieux et que leur sécurité nationale et économique est menacée. Ils se sont donc lancés dans l'élaboration de stratégies de cyberguerre et dans la mise en place de cybercommandements dotés de moyens offensifs et défensifs. Certes, de telles mesures sont opportunes et souhaitables, mais le manque de dialogue concernant la cyberpaix, et plus encore le maintien d'un niveau acceptable de géocyberstabilité, est manifeste. Comme il est indiqué dans l'introduction, l'auteur définit la notion de "géo-cyber" comme la relation entre l'Internet et la géographie, la démographie, l'économie et la politique d'un pays et sa politique étrangère. Elle définit la "géocyberstabilité" comme la capacité de tous les pays d'utiliser l'Internet au service de l'économie, de la politique et de la démographie, en s'abstenant de toute activité qui pourrait causer des souffrances et des dégâts inutiles[104].

Cette réticence des pays à entamer des discussions sur le "minimum de communications essentielles" nécessaire pour préserver les fonctions vitales de la société et empêcher les souffrances et dégâts inutiles causés par les cyberattaques est

---

104 Présenté pour la première fois à la Conférence du ANSER Institute of Homeland Security, "Homeland Security 2005: Charting the Path Ahead", University of Maryland, exposé de Jody Westby, "A Shift in Geo-Cyber Stability and Security", 6-7 mai 2002.

peut-être en partie due au flou général qui entoure la question de savoir comment une telle question pourrait être traitée dans le cadre juridique international actuel.

Le droit des conflits armés

Tout au long de l'histoire moderne, le droit international des conflits armés a été actualisé pour être adapté aux atrocités de la guerre et aux nouvelles méthodes de combat. Il est aujourd'hui urgent de poursuivre son adaptation pour qu'il corresponde à la réalité des cybermoyens car il est probable que les actions de cybercombat soit ne respectent pas de nombreuses dispositions du droit des conflits armés existant, soit ne relèvent pas du champ d'application de ce droit pris dans son ensemble.

Très complets, les cadres juridiques fondamentaux régissant les conflits armés ont en grande partie été élaborés au cours du siècle dernier. Les principaux pertinents pour les cyberconflits sont les suivants:

- la Charte des Nations Unies[105];
- le Traité de l'Atlantique Nord[106];
- les Conventions de Genève de 1949[107];
- le Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I)[108];
- les Conventions de La Haye (1899 et 1907)[109];
- la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination[110].

---

105 Charte des Nations Unies: www.un.org/en/documents/charter/index.shtml.

106 Traité de l'Atlantique Nord: www.nato.int/cps/en/natolive/official_texts_17120.htm.

107 Conventions de Genève de 1949: www.icrc.org/web/eng/siteeng0.nsf/html/genevaconventions.

108 Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977, www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (ci-après "Protocole I").

109 Convention concernant les lois et coutumes de la guerre sur terre (La Haye II), 29 juillet 1899, http://avalon.law.yale.edu/19th_century/hague02.asp; Convention concernant les lois et coutumes de la guerre sur terre (La Haye IV), 18 octobre 1907: http://avalon.law.yale.edu/20th_century/hague04.asp.

Les principes fondamentaux énoncés dans ces textes peuvent être simplifiés. Le droit des conflits armés régit la conduite des hostilités armées et les forces militaires doivent s'y conformer lorsqu'elles planifient et mènent leurs opérations. Il s'applique aux opérations militaires ainsi qu'aux activités connexes et vise à empêcher les souffrances et les dégâts superflus en temps de guerre. Des dispositions spéciales protègent les civils, les prisonniers, les blessés et les malades, ainsi que les naufragés.

De quelle manière les actions militaires peuvent-elles être menées?

Trois principes fondamentaux régissent *la façon* dont les actions militaires peuvent être conduites: la nécessité, la distinction et la proportionnalité.

Nécessité: Le principe de nécessité oblige les forces belligérantes à ne mener que les actions qui sont nécessaires pour atteindre des objectifs militaires légitimes. Les installations, les équipements et les forces militaires peuvent être pris pour cibles à condition que cela permette d'obtenir la soumission partielle ou totale de l'ennemi.

Distinction: Le principe de distinction impose aux militaires de faire une distinction entre cibles licites et cibles illicites, comme les civils, les biens de caractère civil et les blessés. Les cibles civiles doivent être séparées des cibles militaires dans toute la mesure du possible. Une attaque est considérée sans discrimination dès lors qu'elle frappe à la fois des cibles militaires et des cibles/populations civiles.

Proportionnalité: Le principe de proportionnalité interdit l'emploi d'une force excessive par rapport à celle nécessaire pour atteindre des objectifs militaires. Ce principe consiste à comparer l'avantage militaire obtenu grâce à l'attaque et les dommages causés et suppose un équilibre entre l'avantage militaire direct anticipé et les pertes et dommages civils attendus.

Qui peut conduire un conflit armé?

Seuls les *combattants licites* peuvent participer à un conflit armé. On appelle combattants licites les personnes autorisées par une autorité publique à prendre part aux hostilités. Ces combattants peuvent être une force irrégulière, mais ils doivent avoir à leur tête une personne responsable pour ses subordonnés, avoir un signe

---

110 Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination: www.icrc.org/web/eng/siteeng0.nsf/html/p0811 (ci-après "Convention sur les armes produisant des effets traumatiques excessifs").

distinctif fixe et reconnaissable à distance (par exemple un uniforme ou une couleur), porter les armes ouvertement et se conformer dans leurs opérations au droit des conflits armés.

On appelle *combattants illicites* les personnes qui participent directement aux hostilités sans y être autorisées par une autorité publique ou dans le cadre du droit international. Les civils qui s'en prennent aux forces armées, les pirates et les terroristes sont par exemple des combattants illicites.

On appelle *non-combattants* les personnes qui ne sont pas autorisées par une autorité publique à participer à des hostilités, mais y sont impliquées. Il s'agit par exemple des aumôniers, du personnel civil accompagnant les forces armées et du personnel médical. Les non-combattants ne font pas nécessairement l'objet d'attaques directes, mais courent néanmoins le risque d'être tués au cours d'une attaque directe. Lorsque le statut d'un combattant n'est pas connu, les Conventions de Genève s'appliquent jusqu'à ce que ce statut soit établi.

Les cibles potentielles

Les *cibles militaires* sont les cibles qui, par leur nature, leur emplacement, leur destination ou leur utilisation apportent une contribution effective à la capacité militaire d'un ennemi et dont la destruction totale ou partielle ou la neutralisation au moment de l'attaque contribue à atteindre des objectifs militaires légitimes.

Les *cibles protégées* sont les cibles protégées par les Conventions de Genève, comme les hôpitaux, les véhicules transportant des blessés ou des malades, les sites religieux ou culturels et les zones de sécurité. Toutefois, l'une quelconque de ces cibles peut être attaquée dès lors qu'elle est utilisée à des fins militaires. Par exemple, une église servant de base à une armée pour ses opérations devient une cible militaire légitime[111].

Dans le cybercontexte, ces principes soulèvent un certain nombre de questions sans réponse:

- Qu'est-ce qu'un acte de cyberconflit armé?
- Les infrastructures essentielles peuvent-elles être prises pour cibles?

---

111 *Voir* Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace,* Aegis Research Corp., Falls Church, VA, 2000; *Le droit des conflits armés: les connaissances de base,* Comité international de la Croix-Rouge, juin 2002, www.icrc.org.

- Des infrastructures essentielles qui appuient des cibles protégées par les Conventions de Genève peuvent-elles être prises pour cibles?
- Est-il nécessaire d'attaquer des infrastructures essentielles pour atteindre des objectifs militaires?
- Comment les participants à des hostilités peuvent-ils faire la distinction entre cibles militaires et cibles protégées?
- Les dégâts causés aux infrastructures essentielles sont-ils proportionnels aux objectifs militaires?
- Qu'est-ce que la force excessive dans le cyberespace?
- Comment identifie-t-on des cybersoldats?
- Comment détermine-t-on si des tiers agissent pour le compte d'un Etat-nation?

Le droit existant ne donne aucune réponse claire à ces questions. Par exemple, aux Etats-Unis, peut-on considérer que les réseaux de communication du secteur privé sont une cible militaire légitime entrant dans le cadre du principe de nécessité militaire au motif que 90% des communications du gouvernement américain se font sur des réseaux commerciaux (Internet, téléphonie, cellulaire et satellite)[112]? Nul doute que les entreprises et les actionnaires auxquels appartiennent ces réseaux réfuteraient un tel raisonnement, de même que les hôpitaux dont le fonctionnement dépend entièrement de ces réseaux. Ils considèreraient vraisemblablement qu'il s'agit d'une attaque visant une cible protégée.

Si le droit des conflits armés autorise l'emploi de forces irrégulières, les gouvernements peuvent-ils engager des botmasters et utiliser leurs botnets comme combattants licites dans des cyberconflits? Certes, des forces irrégulières peuvent être autorisées à prendre part aux hostilités, mais les botnets ne sont pas reconnaissables à distance et ne portent pas ouvertement les armes. A l'évidence, les robots qui les composent ne portent ni emblème, ni signe distinctif. Ils peuvent même être impossibles à détecter puisqu'ils utilisent des pages web, des réseaux entre homologues, des liens malveillants, des sites de réseaux sociaux et des spams pour diffuser leurs logiciels malveillants. Un ordinateur personnel agissant comme un robot dans le cadre d'une attaque lancée à la demande d'un Etat-nation peut appartenir à

---

112 *The Insider Threat to U.S. Government Information Systems*, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99, www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf.

un civil innocent qui ne sait pas que son ordinateur a été impliqué. S'ils sont arrêtés, ces botmasters peuvent-ils être jugés comme des criminels de guerre? Qu'en est-il des propriétaires des ordinateurs?

Les Conventions V et XIII de La Haye énoncent les droits et devoirs des puissances neutres en cas de guerre sur terre ou de guerre maritime, mais aucune de leurs dispositions ne traite du cyberespace. Les belligérants ont interdiction de faire passer à travers le territoire d'une puissance neutre des troupes ou des convois, ou de commettre un acte d'hostilité quel qu'il soit dans les eaux territoriales d'un pays neutre, mais qu'en est-il du fait de passer par les réseaux d'un pays neutre? Un pays doit-il obtenir la permission d'un pays neutre pour lancer une cyberattaque qui transiterait par les réseaux de ce pays? Avec la commutation par paquets, comment un pays peut-il même savoir quels réseaux seront utilisés? Un pays peut-il utiliser un botnet comme force irrégulière si celui-ci fait appel à des ordinateurs situés dans un pays neutre?

La Charte des Nations Unies, les Conventions de Genève et de La Haye, ainsi que le Traité de l'Atlantique Nord ne traitent pas des cyberconflits. La Charte des Nations Unies et le Traité de l'Atlantique Nord utilisent des expressions telles que "intégrité territoriale", "l'emploi de la force armée", "au moyen des forces aériennes, navales ou terrestres" et "agression armée" qui ne sont pas adaptées aux cyberscénarios et, semble-t-il, inscrivent ce type de conflits en dehors du champ d'application du droit international. Les conflits estonien et géorgien sont un parfait exemple des conséquences que peut avoir un cyberconflit et de la confusion dans laquelle les ripostes sont menées en raison de l'incertitude concernant la règle de droit[113].

Arguments en faveur de la géocyberstabilité

Les paragraphes qui précèdent ne traitent que de quelques-unes des incertitudes juridiques relatives aux cyberconflits. Un examen du droit des conflits armés fait apparaître une volonté tout au long de l'histoire de moderniser les textes pour qu'ils tiennent compte des nouvelles technologies, comme les armes navales et les

---

113 Pour un examen plus approfondi des conflits estonien et géorgien et des questions relatives à la riposte et au cadre juridique, voir Jody R. Westby, The Path to Cyber Stability", *Rights and Responsibiliites in Cyberspace: Balancing the Need for Security and Liberty",* EastWest Institute et World Federation of Scientists, 2010, www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

aéronefs[114]. Ces instruments pourraient donc être modifiés pour s'appliquer aux cyberconflits.

La première grande question qui se pose toutefois est celle de savoir quel niveau d'activité devrait être autorisé. Pour l'auteur, quatre principes devraient être appliqués en cas de cyberconflit:

1. *Une certaine partie des infrastructures essentielles devrait être protégée en vue d'empêcher des destructions, des dommages et des souffrances inutiles et d'assurer un minimum de communications essentielles.*

   Les infrastructures essentielles protégées seraient celles qui sous-tendent, par exemple, les hôpitaux et les établissements médicaux, les logements assistés, les systèmes financiers, les systèmes maintenant les personnes en vie et les appareils médicaux essentiels, les chaînes d'approvisionnement, les transports, les émissions d'information, les établissements d'éducation, les églises et centres religieux, les premiers secours et les entités chargées de l'application de la loi. Cette liste ne se veut pas exhaustive mais donne plutôt des exemples des types de systèmes qui permettent d'aider les populations civiles innocentes, y compris les plus jeunes, les infirmes et les blessés, et les personnes âgées. Les parties prenantes devraient, par leur contribution, aider les diplomates à définir les contours sacrés des infrastructures essentielles.

   Justification: Le droit des conflits armés en vigueur corrobore ce concept. Comme il est noté dans les *Règles essentielles des Conventions de Genève et de leurs Protocoles additionnels:*

   > Dans tout conflit armé, le droit des Parties au conflit de choisir des méthodes ou moyens de guerre n'est pas illimité. De ce principe découlent deux règles fondamentales. La première interdit d'employer des armes, des projectiles et des matières ainsi que des méthodes de guerre de nature à causer des maux superflus. La

---

114 Voir par exemple "Protection des populations civiles et des personnes civiles en temps de guerre", tiré de "Règles essentielles des Conventions de Genève et de leurs Protocoles additionnels", Comité international de la Croix-Rouge, 31 décembre 1988, www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV (ci-après "Protection des populations civiles") ("l'essor extraordinaire de l'arme aérienne (…) exigeait que les règles existantes du droit des conflits armés soient non seulement réaffirmées, mais aussi précisées et développées. Tel est l'objet du Titre IV du Protocole I additionnel aux Conventions"); la Convention II a été ajoutée afin de tenir compte de l'utilisation de la marine en temps de guerre et de définir le traitement appliqué aux blessés, aux malades et aux naufragés des forces armées sur mer.

> seconde impose aux Parties au conflit, en vue d'assurer le respect et la protection de la population civile et des biens de caractère civil, de faire en tout temps la distinction entre la population civile et les combattants, ainsi qu'entre les biens de caractère civil et les objectifs militaires et, par conséquent, de ne diriger leurs opérations que contre des objectifs militaires[115].

Les préjudices et les dommages qui découleraient de la destruction ou de la mise hors service de systèmes d'infrastructures essentielles sont superflus et entraîneraient des souffrances et des épreuves extrêmes comme celles que le droit des conflits armés vise à empêcher. De surcroît, pour ces réseaux desservant de grandes populations, une telle attaque provoquerait des préjudices et des dommages d'une très grande ampleur qui ne seraient pas proportionnels à l'avantage militaire attendu.

La Convention IV de Genève contient de nombreuses dispositions venant appuyer le principe proposé. Elle traite précisément de la protection des populations civiles et en particulier protège les blessés, les malades, les infirmes et les femmes enceintes (Article 16). Pendant les hostilités, toute Partie pourra proposer la création de zones neutralisées dans les zones de conflit dans le but de protéger les blessés et les malades, combattants ou non-combattants, ainsi que les civils qui séjournent dans ces zones mais qui ne participent pas aux hostilités et ne se livrent à aucun travail de caractère militaire (Article 15). Les hôpitaux civils qui donnent des soins aux blessés, aux malades, aux infirmes et aux femmes en couches ne pourront, en aucune circonstance, être l'objet d'attaques (Article 18). L'entretien, la pratique de la religion et l'éducation des enfants de moins de quinze ans devenus orphelins ou séparés de leurs parents devront être facilités (Article 24). Il est interdit de détruire des biens mobiliers ou immobiliers appartenant individuellement ou collectivement à des personnes privées, à des pays ou à des collectivités publiques, à des organisations sociales ou coopératives (Article 53).

Le Protocole I de la Convention de Genève complète la Convention IV et élargit la protection des populations civiles en temps de guerre. Ses Articles 48 à 59 sont particulièrement intéressants. Est considérée comme civile toute personne qui n'est pas membre des forces armées (Article 50). La

---

115 "Protection des populations civiles et des personnes civiles en temps de guerre", tiré de "Règles essentielles des Conventions de Genève et de leurs Protocoles additionnels", Comité international de la Croix-Rouge, 31 décembre 1988, www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV.

population civile et les personnes civiles jouissent d'une protection générale contre les dangers résultant d'opérations militaires, ne doivent pas être l'objet d'attaques, ni subir des actes visant à répandre la terreur, ni faire l'objet d'attaques sans discrimination qui ne sont pas dirigées contre un objectif militaire déterminé (sont dites sans discrimination les attaques dont on attend qu'elles causent incidemment des pertes en vies humaines dans la population civile, des blessures ou des dommages aux biens de caractère civil qui seraient excessifs par rapport à l'objectif militaire) (Article 51). Les biens de caractère civil ne doivent être l'objet ni d'attaques ni de représailles; en cas de doute, les biens seront réputés civils (Article 52). Aucun acte d'hostilité ne sera commis contre les monuments historiques, les œuvres d'art ou les lieux de culte (Article 53). Les attaques contre les biens indispensables à la survie de la population civile (tels que les denrées alimentaires, les zones agricoles, les récoltes, le bétail, les installations et réserves d'eau potable et les ouvrages d'irrigation) sont interdites (Article 54). Les ouvrages d'art ou installations contenant des éléments dangereux, comme les barrages, les digues et les centrales nucléaires, ne seront pas l'objet d'attaques, même s'ils constituent des objectifs militaires, lorsque de telles attaques provoqueraient "la libération de (…) forces [dangereuses] et, en conséquence, [causeraient] des pertes sévères dans la population civile" (Article 56). On veillera constamment à épargner la population (Article 57). Ceux qui préparent une attaque doivent, d'une part, prendre toutes les précautions pour vérifier que les objectifs attaqués ne sont ni des personnes civiles, ni des biens de caractère civil, et ne bénéficient pas d'une protection spéciale et, d'autre part, prendre toutes les précautions pratiquement possibles pour éviter et réduire au minimum les pertes en vies humaines dans la population civile (Article 57). Il est interdit d'attaquer des localités non défendues (pas d'opérations ni de personnel militaires dans la zone) (Article 59).

En outre, le droit des conflits armés contient de nombreuses dispositions qui ont été ajoutées au fil des ans dans le but d'interdire l'utilisation de technologies qui produisent des effets traumatiques excessifs ou frappent sans discrimination. Déjà en 1899, des déclarations à la Convention de la Haye avaient été adoptées à l'effet d'interdire le lancement de projectiles et d'explosifs du haut de ballons "ou par d'autres modes analogues nouveaux[116]", l'emploi de projectiles qui ont pour effet de répandre des gaz

---

116 Déclaration relative à l'interdiction de lancer des projectiles et des explosifs du haut de ballons (La Haye IV), 29 juillet 1899, http://avalon.law.yale.edu/19th_century/hague994.asp.

asphyxiants ou délétères[117], et l'emploi de balles qui s'épanouissent ou s'aplatissent facilement dans le corps humain[118]. Adoptée en 2001, la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination interdit un grand nombre d'armes particulièrement dangereuses et nuisibles, à savoir celles susmentionnées, déjà interdites depuis 1899, ainsi que les mines, les pièges, les armes incendiaires, les armes à laser aveuglantes et les restes explosifs de guerre[119]. Cette Convention pourrait être modifiée de sorte qu'elle s'applique aux cyberattaques visant des infrastructures essentielles définies.

2. *L'utilisation de botnets et d'autres cyberforces irrégulières devrait être interdite.*

Justification: Pour la victime, au début d'une attaque, ces combattants ne peuvent être distingués d'un autre attaquant quel qu'il soit; la victime ne sait pas si la personne qui attaque son système se trouve à l'intérieur, est un hacker isolé ou un acteur mal intentionné, une organisation criminelle à la pointe de la technologie, un terroriste ou un Etat-nation. Il est difficile de repérer et d'identifier les activités cybercriminelles et il n'est pas toujours possible d'en retrouver les auteurs, même lorsque cette tâche est confiée à des enquêteurs et chercheurs expérimentés. En outre, il est impossible de distinguer un cybersoldat tiers car celui-ci ne peut pas porter de signe distinctif et ne peut en aucun cas être reconnaissable à distance. Par conséquent, les cyberforces irrégulières ne respectent pas l'une des règles fondamentales des conflits armés.

---

117 Déclaration concernant l'interdiction de l'emploi de projectiles qui ont pour but unique de répandre des gaz asphyxiants ou délétères, Conférence de La Haye, 29 juillet 1899, http://avalon.law.yale.edu/19th_century/dec99-02.asp.

118 Déclaration concernant l'interdiction de l'emploi de balles qui s'épanouissent ou s'aplatissent facilement dans le corps humain, Conférence de La Haye, 29 juillet 1899, http://avalon.law.yale.edu/19th_century/dec99-03.asp.

119 Convention sur les armes produisant des effets traumatiques excessifs.

3. *Les pays doivent respecter la neutralité des autres pays et ne doivent pas utiliser les infrastructures essentielles des pays neutres pour acheminer leurs attaques quelles qu'elles soient (Conventions V et XIII de La Haye).*

   Ce principe est conforme aux Conventions de La Haye qui limitent le passage de troupes ou de convois d'approvisionnement ou de munitions sur le territoire ou dans les eaux territoriales d'un pays neutre. De nombreuses infrastructures essentielles, comme les réseaux électriques, peuvent être détruites par des surcharges. Ainsi, le fait d'autoriser un pays à mener des cyberattaques qui pourraient transiter par les réseaux d'un grand nombre d'autres nations sans que celles-ci en aient connaissance est tout simplement en contradiction avec l'histoire et l'intention du droit des conflits armés. Le principe proposé imposerait aux pays d'obtenir la permission des autres pays avant de lancer une cyberattaque, ce qui aurait également pour effet de dissuader un Etat de se lancer dans un cyberconflit.

4. *Les pays doivent s'aider mutuellement lorsqu'ils enquêtent sur des activités cybercriminelles.*

   Il est indispensable que les fournisseurs de service Internet et les gouvernements coopèrent dans les enquêtes portant sur des activités cybercriminelles pour garantir un certain niveau de géocyberstabilité. Certes, il peut sembler paradoxal de demander l'assistance d'un pays neutre dans une enquête, même en temps de guerre, mais au départ, toutes les cyberattaques se ressemblent. Seule une enquête permettra à la victime de découvrir l'identité de celui qui l'attaque. Il est fondamental que les pays qui veulent être connectés à l'Internet, ainsi que les fournisseurs sur leur territoire, aient l'obligation d'apporter leur assistance dans les enquêtes sur les cyberdélits. Si un pays était autorisé à refuser une telle assistance au motif qu'il est neutre, tous les cybercriminels auraient tout le loisir de piller les pays prenant part aux hostilités. Inversement, un pays neutre pourrait dans la pratique aider et encourager les criminels ou le pays agresseur en refusant d'apporter son assistance. En cas de cyberattaque, ce n'est que par l'assistance qu'un pays peut rester véritablement neutre.

Instaurer la géocyberstabilité

L'Internet a créé une cyberplanète qui ne reconnaît aucune des frontières traditionnelles et échappe en grande partie au contrôle des Etats. Il représente un armement d'un type nouveau qui expose les populations civiles, en particulier les personnes très jeunes, âgées, malades, fragiles ou handicapées, à des dangers inconnus jusqu'alors. Par ailleurs, l'Internet bouleverse radicalement le droit des

conflits armés car, en cas de cyberconflit, ce seront vraisemblablement davantage les populations civiles que les troupes militaires qui seront prises pour cibles et touchées. Dans la plupart des pays, le secteur privé détient et exploite les infrastructures essentielles. Par conséquent, attaquer les infrastructures essentielles reviendra à attaquer les populations civiles et les réseaux qui précisément permettent à ces populations de vivre et d'assurer leur subsistance. L'urgence de la nécessité de moderniser le droit des conflits armés pour que celui-ci tienne compte de cette nouvelle menace ne saurait être ignorée car il est trop facile d'interpréter *l'absence* de cadre juridique comme une approbation juridique des attaques.

Certains experts dans les domaines du droit et de la sécurité plaident en faveur d'une législation ou d'un traité de grande envergure sur le cyberespace. Cela n'a pas de sens. Le droit des conflits armés s'est adapté à mesure que les technologies utilisées dans la marine, l'aéronavale et dans d'autres domaine ont évolué, et reste un ensemble de textes juridiques cohérent, mais lui aussi en constante évolution. En outre, des considérations d'ordre pragmatique sont à prendre en compte. Les traités posent problème en ce qu'ils nécessitent de longues discussions multilatérales lors de la phase de rédaction, puis sont ouverts à la signature. Les signataires doivent ensuite ratifier le traité et le transposer dans le droit national. En règle générale, un certain nombre de signataires doivent ratifier le traité pour que celui-ci entre en vigueur, et même une fois cette condition remplie, le traité n'est effectif que pour les pays qui l'ont ratifié et transposé. Toute cette procédure prend du temps, ce qui profite aux acteurs malveillants et aux cybercriminels.

En revanche, les instruments existants, comme la Charte des Nations Unies, le Traité de l'Atlantique Nord, les Conventions de Genève et les Conventions de La Haye, peuvent tous être modifiés *et* présentent l'avantage d'avoir déjà été ratifiés et transposés dans le droit national.

Dans le cyberespace, où chaque minute compte, la meilleure solution est la plus rapide. Les Etats-nations doivent œuvrer de concert, avec l'aide des parties prenantes, pour modifier le droit international des conflits armés en vigueur comme suit:

1. La Charte des Nations Unies devrait être modifiée de sorte qu'elle tienne compte des cyberconflits et précise que le terme "intégrité territoriale" inclut les infrastructures essentielles, la cyberdisponibilité, la cyberintégrité et la cyberconfidentialité. Plus précisément, l'Article 42 devrait être modifié pour que le Conseil de sécurité puisse entreprendre des cyberactions.
2. Le Traité de l'Atlantique Nord devrait être modifié de sorte qu'il autorise une défense collective au titre de l'Article 5. Le terme "attaque armée" utilisé

dans l'article 6.1 devrait être élargi pour ne pas se limiter aux "territoires" et aux "forces, navires ou aéronefs" et englober également les cyberattaques.

3. Les Conventions de La Haye devraient être modifiées de manière à rendre l'utilisation de forces irrégulières dans les cybercombats illégale et à interdire l'utilisation des réseaux d'un pays neutre pour acheminer des cyberattaques.

4. Les Conventions de Genève devraient être modifiées de manière à rendre illégales les attaques visant les infrastructures essentielles qui rendraient difficile un minimum de communications essentielles et mettraient en danger les populations civiles.

Un seul domaine nécessite un nouvel accord. Chaque pays doit accepter individuellement de coopérer et de participer aux enquêtes concernant les activités cybercriminelles dont on pense qu'elles ont transité par ses réseaux. Les pays non signataires d'un tel accord ne devraient avoir aucun recours en vertu du droit international si les communications en provenance de son territoire sont bloquées par d'autres pays.

C'est de cette manière que les Etats-nations et les populations pourront avoir confiance dans les TIC et continuer à les intégrer dans leur vie et leur société sans craindre de devenir une cible dans le cadre d'un cyberconflit. C'est aussi ainsi que s'ouvrira un dialogue constructif entre les nations, lesquelles, pour la première fois, viendront à la table des discussions avec une position commune.

6 Cyberpaix

La notion de cyberpaix

Par Henning Wegener

Cet ouvrage a été placé sous le signe de la cyberpaix, par opposition volontaire aux notions négatives que sont la cyberguerre, le cyberterrorisme et la cybercriminalité. Opter pour le côté positif de l'antinomie guerre/paix c'est changer radicalement de perspective et d'échelle de priorités: on met ainsi en lumière les avantages et les possibilités qu'offre la société de l'information et on définit un objectif à cette fin en renforçant la connotation négative de la cyberguerre et des maux qui lui sont associés et en insufflant une dynamique en faveur d'une culture mondiale de la cybersécurité.

Cette tentative d'ôter toute légitimité à la cyberguerre en inversant la perspective ne fait nullement abstraction du fait que les infrastructures numériques sont aujourd'hui omniprésentes et seront inévitablement utilisées également à des fins hostiles, non pacifiques. La priorité essentielle est alors de maîtriser de telles utilisations et de limiter le plus strictement possible toute application belliqueuse des TIC. Etant donné que le terme même de "cyberguerre" renvoie à des schémas de pensée militaires et incite à concevoir la cyberdéfense avant tout en termes d'opérations et de techniques militaires ("représailles"), nous essaierons dans le présent chapitre de combattre cet automatisme mental et de plaider en faveur d'un comportement pacifique dans le cyberespace. Cet exercice ne saurait être qu'une ébauche des fondements théoriques de la cyberpaix qui devra être complétée au fil du temps. De nombreuses autres parties de cet ouvrage y contribuent déjà.

Depuis plusieurs années, que ce soit dans des réunions publiques ou des publications, la cyberpaix est au cœur des travaux[120] de la World Federation of Scientists. L'UIT pour sa part, en particulier par l'intermédiaire de son Secrétaire général, a récemment contribué à concrétiser davantage cette notion[121], mais manifestement le terme a déjà été utilisé auparavant, quoique dans une acception moins générale. L'utilisation la plus

---

120 Voir les différentes références sous "publications" et "activités" à l'adresse www.unibw.de/infosecuret, plus précisément le compte rendu in extenso d'une conférence tenue en décembre 2008 intitulée "The Global Internet Crisis: The Quest for Cyber Peace".

121 "Les Nations Unies ont proposé un accord international pour prévenir la cyberguerre" 31 janvier 2010, www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a.

intéressante du terme, quoique spécifique et limitée, et en l'occurrence spécifique aux enfants, date de 2007 lors de la promotion en Egypte d'une initiative relative à la cyberpaix dans le cadre du Mouvement international Suzanne Moubarak des femmes pour la paix (SMWIPM)[122], qui faisait directement référence à la Déclaration et au Programme d'action des Nations Unies sur une culture de la paix. Cette initiative vise à donner aux jeunes de tous les pays, grâce au renforcement des capacités dans le domaine des TIC, les moyens de vivre dans un monde en ligne sécurisé et à encourager l'esprit d'innovation. Le terme de cyberpaix apparaît aussi occasionnellement, à défaut d'être consacré et défini, dans les activités de la communauté de recherche sur la paix.

Aux fins du présent article, le terme de cyberpaix s'entend dans une acception beaucoup plus large que celle du SMWIPM, et désigne un principe fondamental, celui de l'établissement d'un "ordre universel du cyberespace". Si l'emploi de ce terme a davantage à voir avec la politique et cherche à orienter l'esprit vers les bons choix justes, son acception devrait rester relativement large. Sa définition ne saurait être figée, être plutôt intuitive et englober toujours plus d'éléments.

Pourtant, une définition élémentaire s'impose. Toute définition devrait partir de la notion générale de paix, comprise comme un état de tranquillité totale, l'absence de désordres, de troubles ou de violence, – l'absence non seulement de violence ou d'utilisation de la force "directe" mais aussi de contraintes indirectes. La paix suppose la primauté de principes juridiques et de principes moraux généraux, l'existence de possibilités et de procédures pour le règlement des conflits, une durabilité et une stabilité.

C'est l'Assemblée générale des Nations Unies qui la première a essayé de donner tout son sens au concept de paix – et de culture de la paix. Dans sa "Déclaration et son Programme d'action sur une culture de la paix" d'octobre 1999[123] elle établit une liste des éléments et des conditions indispensables à l'avènement de la paix et indique la voie à suivre pour y parvenir durablement, grâce à une culture de la paix. Rappelant l'Acte constitutif de l'Organisation des Nations Unies pour l'éducation, la science et la culture qui énonce que "les guerres prenant naissance dans l'esprit des hommes, c'est dans l'esprit des hommes que doivent être élevées les défenses de la paix" cette

---

122 Mouvement international Suzanne Moubarak des femmes pour la paix, Initiative sur la cyberpaix, http://smwipm.cyber peaceinitiative.org/.

123 "Déclaration sur une culture de la paix", UNESCO, A/Res/53/243, www.unesco.org/cpp/uk/declarations/2000.htm.

Résolution décrit en détail les différents éléments en jeu et fixe des mesures à prendre pour la décennie, jusqu'en 2010.

Au nombre des éléments indispensables à la paix et à une culture de la paix, il faut citer non seulement le non-recours à la force, la promotion et la pratique de la non-violence mais aussi un ensemble commun de valeurs et de modes de comportement, un ordre et un cadre juridique internationaux, des processus participatifs dynamiques et positifs et le respect des droits de l'homme (entre autres l'adhésion aux principes de liberté, de justice, de démocratie, de tolérance, de solidarité, de coopération, de pluralisme, de diversité culturelle, de dialogue et de compréhension, de promotion de résolution des conflits). Outre les éléments éthiques de la paix, qui ont été amplement soulignés, il est essentiel, lorsqu'il s'agit du cyberespace, d'ajouter à cette énumération le respect et la promotion du droit de chacun à la liberté d'expression, d'opinion et d'information ainsi que l'accès à l'information. Ces références n'ont bien sûr qu'un caractère indicatif et la Résolution, dans son ensemble, doit être examinée avec soin. L'UIT a récemment formulé cinq principes en faveur de la cyberpaix qui définissent des mesures et des obligations spécifiques garantissant paix et stabilité dans le cyberespace. Le lecteur se reportera à cette liste de la plus haute importance.

La World Federation of Scientists a, pour sa part, entrepris de traduire plus en détail, dans sa "Déclaration d'Erice sur les principes régissant la cyberstabilité et la cyberpaix" d'aout 2009[124], les principes généraux contenus dans ces documents ainsi que d'autres valeurs consacrées par les Nations Unies et se rapportant au cyberenvironnement. La Déclaration prouve que cyberstabilité et cyberpaix sont indissociables. Concise, elle est axée sur les éléments opérationnels essentiels de la cyberpaix à savoir:

1. Tous les gouvernements devraient reconnaître que le droit international garantit aux individus la libre circulation des informations et des idées; ces garanties s'appliquent aussi au cyberespace. Il ne devrait y avoir de restrictions que si cela est nécessaire et elles devraient être assorties d'une procédure d'examen juridique
2. Tous les pays devraient œuvrer ensemble à l'élaboration d'un code de conduite commun dans le cyberespace et d'un cadre juridique mondial harmonisé, y compris des procédures d'assistance et de coopération en

---

124 "Déclaration d'Erice sur les principales régissant la cyberstabilité et la cyberpaix", World Federation of Scientists, août 2009, www.ewi.info/system/files/**Erice**.pdf.

matière d'enquête, respectueuses de la vie privée et des droits de l'homme. Tous les gouvernements, les fournisseurs de services et les utilisateurs devraient concourir aux efforts déployés pour sanctionner les cybercriminels en vertu du droit international.

3. Tous les utilisateurs, les fournisseurs de services et les gouvernements devraient œuvrer pour faire en sorte qu'aucune utilisation du cyberespace ne donne lieu à l'exploitation des utilisateurs, en particulier des jeunes et des personnes sans défense, à travers des actes de violence ou des actes dégradants.
4. Les gouvernements, les organisations et le secteur privé, y compris les particuliers, devraient mettre en œuvre durablement des programmes de sécurité détaillés reposant sur de bonnes pratiques et des normes internationalement reconnues et faisant appel à des technologies permettant de renforcer la protection de la vie privée et la sécurité.
5. Les concepteurs de logiciels et de matériels devraient s'efforcer de développer des technologies sûres, axées sur la robustesse et invulnérables.
6. Les gouvernements devraient activement participer aux efforts des Nations Unies pour promouvoir la cybersécurité et la cyberpaix au niveau mondial et pour éviter de porter les conflits dans le cyberespace.

Au-delà de ces principes et en particulier du dernier principe transparaît la ferme intention de maîtriser les risques de conflit dans le cyberespace. De fait, compte tenu de la croissance alarmante des moyens offensifs de cyberguerre, la recherche de la paix dans le cyberespace doit mettre tout particulièrement l'accent sur la nature belliqueuse des activités des agresseurs, qu'il s'agisse d'Etats ou d'individus.

Ces problèmes sont traités en détail dans d'autres parties de cet ouvrage. Toutefois quelques déclarations de principe s'imposent dans le contexte actuel pour clarifier la notion de cyberpaix. Le cyberespace est encore trop souvent un espace de non-droit, permissif, dénué de directives ou de sanctions qui semblerait autoriser des actions en l'absence de tout cadre juridique. D'où l'appel lancé en faveur de l'élaboration de codes de conduite communs reprenant tous les domaines d'activité virtuels. Depuis 2001, la World Federation of Scientists a appelé à travailler à l'élaboration d'une loi

universelle du cyberespace, de préférence sous les auspices des Nations Unies[125]. Cet appel est plus pertinent que jamais dans le domaine des utilisations militaires offensives du cyberespace.

La complexité de cette tâche ainsi que des obstacles juridiques, et peut-être avant tout politiques, sur cette voie est évidente. Comme on l'a déjà fait observer dans d'autres parties de cet ouvrage, le droit classique de la guerre et des conflits armés est ambigu, voire d'une utilité très limitée et ne comporte aucune définition en la matière. Les limites que l'on impose traditionnellement à l'action offensive dans les principaux textes du droit international, par exemple la Charte des Nations Unies ou le traité de l'OTAN, sont ici largement inefficaces. On trouve dans l'ensemble des Conventions de Genève et dans certaines résolutions de l'Assemblée générale des Nations Unies, par exemple dans le domaine de la criminalité internationale organisée, du terrorisme ou du comportement dans l'espace extra-atmosphérique au mieux des analogies vagues et incomplètes[126]. "La maîtrise des armements" ou la distinction entre les utilisations légitimes et les utilisations "illicites" des TIC ou entre acte offensif et acte défensif est floue étant donné que les technologies sont identiques et que le problème de la "double utilisation", qui nuit à la maîtrise des armements, prend ici un caractère permanent. De plus, le problème que pose l'établissement de la responsabilité – localisation et suivi de l'agresseur – de façon fiable et dans des délais raisonnables, qui rend déjà complexe la poursuite de "simples" cybercriminels, est accru dans le domaine militaire par le fait que vraisemblablement un agresseur ayant des visées belliqueuses aura recours le plus possible à des techniques d'évasion et de dissimulation sophistiquées. La vérification, élément essentiel de la maîtrise des armements, est pratiquement impossible. La dissuasion dans son acception classique est vouée à l'échec lorsque les conditions préalables essentielles (établissement de la responsabilité, localisation de l'origine de l'attaque, intensité de la riposte) ne sont pas

---

125 *Voir Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Rapport et Recommandations du Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists 19 novembre 2003, Document soumis au Sommet mondial sur la société de l'information, www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf.

126 Ténues mais en aucun cas non significatives. *Voir* Sergei Komov, Sergei Korotkov, Igor Dylewski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law", *ICTs and International Security*, United Nations Institute for Disarmament Research, 2007, www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?fecvnodeid=128420&dom=1&groupot593=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&fecvid=21&ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&v21=128420&lng=en&id=47166.

réunies. Il est donc logique que la littérature préconise souvent qu'il faut faire le pari de la cyberdéfense (y compris en l'élargissant aux alliés) plutôt que celui de la cyberdissuasion[127].

Toutefois, si l'on aspire véritablement à la cyberpaix, il est essentiel d'élaborer un cadre juridique pour définir ce que constitue une rupture de la paix et les Etats ne devraient pas se focaliser sur les imperfections inhérentes à un tel cadre. Dans cette optique, le Secrétaire général de l'UIT, s'appuyant sur les cinq principes de l'Union, a proposé que les pays s'engagent à ne pas lancer en premier une cyberattaque à l'encontre d'un autre pays ("non-recours en premier") et à ne pas héberger de cyberterroristes ou d'agresseurs dans leur pays en toute impunité[128]. Les Etats pourraient aussi être encouragés à conclure bilatéralement ou multilatéralement des pactes de non-agression dans le cyberespace. On pourrait également envisager qu'ils s'engagent mutuellement à ne pas attaquer des infrastructures nationales essentielles (en particulier des infrastructures à vocation humanitaire ou qui répondent à des besoins humains essentiels, lesquelles seraient déjà en partie protégées par le droit international actuellement en vigueur) et qu'ils confirment l'inviolabilité des réseaux de données transfrontières. Une avancée dynamique et courageuse consisterait, dans le cadre d'un instrument international, à priver de toute légitimité l'utilisation de cyberarmes et de stratégies offensives.

Soyons réalistes, les stratégies et principes qui sont conçus pour promouvoir la cyberpaix n'auront pas, selon toute vraisemblance, l'adhésion spontanée de nombreux pays qui ont déjà beaucoup investi et continuent d'investir dans un potentiel de cyberguerre en mettant à profit le vide juridique qui existe actuellement dans le domaine du cyberespace. En effet, les rapports actuels sur la "militarisation" systématique du cyberespace, la création de cybercommandements, l'élaboration de cyberstratégies offensives etc. ne sont pas pour nous rassurer. Cela étant, il ne faut pas sous-estimer les conséquences morales de contre-mesures multilatérales. La légitimité est la pierre angulaire de l'action étatique et le simple fait de limiter l'action ou de convenir de critères pourrait, avec le temps, être source de dynamisme et de motivation. Pour pouvoir contribuer à la stabilité dans le cyberespace et au respect des droits fondamentaux, la cyberpaix doit être assortie de mesures de mise en œuvre énergiques.

---

127 Voir par exemple, Martin C. Libicki "Cyber deterrence and Cyberwar", Santa Monica, 2009, p. 158 et. seq.

128 Voir Chapitre VII.

Il existe un puissant argument à l'appui de cette thèse. Le fonctionnement et la stabilité de la structure de réseaux mondiaux interdépendants inspirant la confiance constituent un bien public commun. Il est difficile de contrôler des cyberattaques massives même contre une partie du système et leurs conséquences pourraient être incalculables[129], tant il est vrai que des réactions en chaîne surviennent même après des événements mineurs. Bien au-delà des seules parties au conflit, ces cyberattaques pourraient modifier radicalement les équations de puissance, la géostabilité de l'ensemble de l'environnement numérique dont la société est tributaire. L'intérêt de maintenir le bon fonctionnement des réseaux transnationaux et des structures de l'information est un intérêt partagé par tous les acteurs internationaux.

Il est aisé de comprendre qu'une cyberaction offensive non provoquée, et en fait une cyberattaque, est incompatible avec les principes de la cyberpaix.

Mais l'heure de vérité pour la cyberpaix c'est de définir et d'évaluer la réaction à des cyberattaques attendues ou réelles en cas de véritable cyberconflit, de savoir si et quand une cyberattaque est réputée être ou non une attaque armée: il est généralement admis que le principe fondamental de droit international du droit à l'autodéfense, décrivant le fait légitime de se protéger ou de faire face à une agression, prévaut. Comme on l'a dit à maintes reprises dans cet ouvrage, qualifier un acte hostile d'"attaque armée" est, selon les termes de la Charte des Nations Unies, du traité de l'OTAN et du droit international général, la condition indispensable pour légitimer une défense individuelle ou collective par des moyens militaires. On peut bien entendu avancer l'argument qu'une cyberattaque menée à l'encontre d'un autre Etat ou qui a des conséquences dans un autre Etat est une "attaque armée" de ce type ou son équivalent, du moins lorsque cette attaque cause des destructions massives ou des pertes de vies humaines[130].

---

129 "La communauté international doit être consciente du fait que le moindre petit accrochage dans le cyberespace pourrait déclencher un cyberconflit grave susceptible de provoquer un conflit régional classique qui aurait des retombées internationales. Quote from John Bumgarner, Chief Technology Officer, US Cyber Consequences Unit, *Jane's Defence Weekly*, 29 Sept. 2010, www.jdw.janes.com (par la suite "Jane's").

130 Lorsque cet article a été écrit, les pays membres de l'OTAN, en préparation à une réunion au sommet des Etats parties au Traité de Washington (20 novembre 2010) réfléchissaient à des décisions collectives concernant les nouvelles menaces, y compris les cyberattaques. Si des attaques de ce type étaient classées dans la catégorie des mesures déclenchant une défense collective, les dispositions de l'article 4 (consultations mutuelles) et de l'article 5 (assistance mutuelle en prenant telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée) s'appliqueraient.

Cela pourrait constituer la base juridique d'une action collective, y compris par des moyens militaires. Mais la définition et l'opportunité d'une mesure de représailles militaires dans un environnement de technologies numériques nécessite une nouvelle réflexion approfondie et, en dernière analyse, une politique de retenue délibérée.

Les différences entre un cyberconflit et une guerre classique sont frappantes et vont bien au-delà des différences manifestes qui existent dans les "armes" utilisées. Pour résumer les arguments avancés dans de nombreuses autres parties de cet ouvrage, y compris dans ce chapitre, la première distinction réside dans le fait qu'il est difficile d'identifier avec certitude les auteurs des cyberattaques, ce qui fait peser une incertitude sur la cible des éventuelles mesures de rétorsion ou représailles – en d'autres termes qui ces mesures peuvent elles légitimement frapper? Deuxième distinction, du fait de l'omniprésence et de l'interdépendance des réseaux et des systèmes numériques, l'impossibilité de prévoir les conséquences de contre-mesures électroniques et, par voie de conséquence, la difficulté de mesurer l'effet d'escalade de toute contre-mesure de ce type. Troisième distinction, un cyberconflit peut être soit une attaque coordonnée et donc dévastatrice soit prendre la forme pernicieuse de menaces répétées de portée limitée (cyberespionnage, création de réseaux zombies non reconnus, etc.) pouvant, à des degrés divers, aboutir à une désintégration importante des infrastructures. Autre distinction, dans le cas d'un conflit entre Etats, le nombre d'acteurs possibles est infini; les enseignements de la guerre froide de la seconde moitié du siècle passé, le fonctionnement de l'équilibre militaro-nucléaire entre deux puissances fondé sur la dissuasion et la retenue ne peuvent tout simplement pas être transposés dans le cas d'un scénario où s'affrontent de multiples acteurs. Enfin, comme cela a déjà été souligné, il est de l'intérêt de tous de maintenir une infrastructure mondiale de l'information opérationnelle.

Toutes ces différences et bien d'autres doivent guider notre réflexion quant aux ripostes à apporter aux agressions. Suivant la notion de cyberpaix, la priorité doit être donnée au maintien et au rétablissement rapide d'un environnement stable et pacifique, ce qui met clairement l'accent sur la défense.

L'autodéfense préventive est la clé des ripostes menées dans un esprit de paix A cet égard, il convient de reconnaître la responsabilité partagée qu'ont tous les acteurs du numérique de se doter de réseaux et de systèmes sécurisés, une exigence qui est consacrée dans la Déclaration d'Erice. La coopération entre gouvernements et entreprises est toute aussi importante que la coopération internationale. Le maître mot ici est robustesse: non seulement la qualité des systèmes mais aussi leur gestion doivent contribuer à leur solidité et à leur invulnérabilité. Les parties prenantes devraient avoir une connaissance parfaite de l'état de leurs réseaux, identifier les ressources stratégiques et se préoccuper de leurs failles possibles (surveillance en

temps réel de la totalité du réseau, mise en place de zones de sécurité, segmentation des réseaux, garantie de la sécurité énergétique). Des systèmes et des logiciels robustes, respectant rigoureusement les normes et protocoles nationaux et de l'UIT en matière de sécurité devraient par conséquent être disponibles en grand nombre. Des infrastructures IT solides découragent en effet les attaques et contribuent à un environnement pacifique. Une défense sans faille est un élément essentiel de la cyberstabilité car elle dissuade les attaques, contribue à un climat de confiance et rassure les opérateurs.

La robustesse, dans sa définition générale, englobe plusieurs éléments: la capacité d'autoréparation des systèmes, l'existence de systèmes d'alerte, les redondances intégrées, mais aussi des comportements professionnels, par exemple le fait de réfléchir aux domaines dans lesquels les parties prenantes peuvent coopérer en vue de l'instauration d'un environnement pacifique et un partage accru de l'information. Il faut mettre l'accent sur l'action positive et inciter à agir en ce sens. Les Etats qui réfléchissent à d'éventuels scénarios de prévention des cyberconflits ou qui souhaitent mettre en place de tels scénarios pourraient aussi envisager d'œuvrer dans le domaine de la réglementation, par exemple conclure des accords de non-agression dans le cyberespace, élaborer des dispositions de transparence afin de neutraliser des images ennemies, surveiller les actes malveillants et mieux partager l'information afin d'identifier plus facilement les agresseurs en cas de conflit. Plusieurs de ces propositions figurent déjà dans le programme du Secrétaire général de l'UIT précédemment évoqué. Le tout nouveau mécanisme d'alerte (Centre d'alerte mondial (GRC), le Network Early Warning System (NEWS) ou ESCAPE) sont d'une utilité évidente car ils permettent des ripostes non violentes. Les cadres de coopération internationaux devraient utiliser les réseaux CERT de plus en plus étendus.

Il faut toutefois prévoir des scénarios de cyberconflits graves dans lesquels une simple défense passive ne suffit pas et où le droit à l'autodéfense prévu dans le droit international doit être invoqué activement. Du point de vue de la cyberpaix, il est là encore inutile de faire de simples analogies avec le droit classique des conflits armés, au risque sinon de créer un état d'esprit favorisant des scénarios de guerre de représailles et une logique militaire d'anéantissement des biens de l'ennemi. Recourir à des règles d'engagement héritées du passé pourrait être dangereux. La cyberpaix n'exige pas de renoncer totalement à toute contre-offensive ou à des mesures de représailles mais nuance grandement les scénarios applicables.

La retenue est le mot clé de l'élaboration des ripostes. Elle suppose une analyse rigoureuse et constante des menaces et des risques afin de prévenir des conséquences incontrôlables: neutralisation de vastes cyberréseaux; concentration sur des ripostes de non-escalade bien réfléchies; temporisation et opportunité de la riposte pour qu'il

soit plus facile d'identifier l'auteur de l'attaque, activation des mécanismes de redondance et alliances de défense mutuelles; stricte application des principes de proportionnalité et de nécessité légitimant l'autodéfense; protection scrupuleuse des infrastructures humanitaires ou sociales indispensables.

Même s'il est peut être exagéré d'affirmer que, pour riposter à des cyberattaques, la défense est toujours la meilleure offensive, il semble que, dans le cas de la cyberpaix, il faille, parallèlement aux limites strictes imposées aux représailles, privilégier une autodéfense globale à l'offensive[131]. Ce principe serait compatible avec une déligitimisation systématique des "cyberarmes" et des cyberstratégies offensives au niveau des Etats comme cela a été discuté plus haut.

131 "Clausewitz ne pouvait pas prévoir que la meilleure offensive au XXIe siècle serait une cyberdéfense forte" Jane's.

7 Quelle riposte internationale face à la menace d'une cyberguerre?

Par Hamadoun I. Touré

7.1 Politiques et approches nationales

Les pays dans le monde réagissent différemment à la nouvelle menace que constitue une cyberguerre. Si certains Etats commencent tout juste à s'intéresser à la question de la cybersécurité[132], la plupart des gouvernements reconnaissent à tout le moins qu'il est nécessaire de procéder à une réaffectation des ressources et de revoir, à un niveau ou un autre, les stratégies nationales relatives à la cybersécurité. De nombreux pays augmentent actuellement leurs moyens financiers, leurs activités de recherche ainsi que leurs ressources tactiques et diplomatiques dans le but d'améliorer leur cybersécurité[133]. Certains pays essaient d'isoler certains réseaux, de ne pas les relier à d'autres systèmes afin de protéger des structures et des systèmes d'information essentiels contre d'éventuelles attaques[134]. Les différentes approches adoptées par les Etats sont évaluées dans les paragraphes qui suivent

a) Intégrer les cybercapacités dans une stratégie de guerre conventionnelle

Certains pays appliquent une méthode de guerre classique en matière de cybertactique et renforcent leurs cyberarmes offensives ainsi que leurs cybercapacités défensives. Ils voient dans les cyberarmes des "multiplicateurs de puissance", qu'ils utiliseront surtout dans le cadre d'opérations militaires plus classiques pour augmenter sensiblement leur potentiel de combat[135]. Internet est récemment devenu

---

132 Par exemple, la République sudafricaine n'a que récemment (février 2010) fait part de son intention de commencer à élaborer une politique nationale coordonnée en matière de cybersécurité. "Notice of Intention to Make South African Cybersecurity Policy", République sudafricaine, Government Gazette, No. 32963, 19 février 2010.

133 "Cyberwar: Sabotaging the System – 60 Minutes – CBS News", 8 Nov. 2009, www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml (indiquant que le Congrès américain a alloué 17 milliards USD aux initiatives offensives ou défensives dans le domaine de la cybersécurité).

134 David Eshel, "Israel Adds Cyber-Attack to IDF", *Military.com,* 10 février 2010, www.military.com/features/0,15240,210486,00.html (hereinafter "Eshel").

135 Kevin Coleman, "Russia's Cyber Forces", DefenseTech, 27 mai 2008, http://defensetech.org/2008/05/27/russias-cyber-forces/.

un vecteur important d'échange d'informations et de propagande pendant des conflits armés. De nombreux pays estiment que le sabotage de l'information sur Internet est une forme d'agression militaire qui sape le moral de la population et sont donc prêts à riposter à des cyberattaques par la force militaire[136]. Des incidents récents comme la fuite de documents militaires classifiés montrent pourquoi les Etats s'inquiètent des conséquences que des cybervulnérabilités pourraient avoir sur le soutien et le moral de la population.[137]. Certains fonctionnaires de l'Etat ont indiqué dans le passé qu'ils considéreraient les tactiques de guerre de l'information comme des actions militaires, qu'elles causent ou non des pertes en vies humaines, et qu'une riposte militaire pourrait donc être justifiée[138].

b) Faire des cybertactiques une ressource nationale

En réaffectant leurs ressources, en prévoyant des moyens financiers et en procédant à une planification stratégique, de nombreux pays font de leur infrastructure numérique et des TIC une ressource nationale ou un bien stratégique. Certains en ont même fait une nouvelle politique nationale[139]. Des pays ont réaffecté des ressources budgétaires à des programmes sur le cyberespace et ont alloué des sommes considérables à la

---

136 Gregory Asmolov, "Russia: New Military Doctrine and Information Security", Global Voices, 23 février 2010, http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/ (décrivant la doctrine militaire actualisée de la Russie selon laquelle la guerre de l'information est considérée comme une agression militaire).

137 *Voir par exemple*, Jo Biddle, "AFP: Huge leak of secret files sows new Afghan war doubts", 27 juillet 2010, www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg.

138 *Cyberwarfare*, Congressional Research Service, RL30735, mise à jour 19 juin2001, www.fas.org/irp/**crs**/RL30735.pdf (citant un responsable militaire russe qui a exclu la possibilité que la guerre de l'information soit classé comme non militaire) (hereinafter "CRS Cyberwarfare"). *Voir également* Peter Beaumont, "Les Etats-Unis nomment le premier général en matière de cyberguerre", *Guardian.co.uk*, 23 mai 2010, www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/ (faisant observer que les Etats-Unis ont également indiqué qu'ils pourraient envisager d'utiliser une tactique militaire classique pour riposter à des cyberattaques) (hereinafter "Cyber General").

139 Président Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure", La Maison blanche, 29 mai 2009, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (précisant que désormais l'infrastructure du pays serait considérée comme "un bien national stratégique" et que sa protection serait considérée comme une "priorité nationale en matière de sécurité").

recherche et développement de moyens de cyberguerre[140]. Pour lutter contre les nouvelles cybermenaces, plusieurs gouvernements ont élaboré et commencé à mettre en œuvre des plans nationaux intégrés, à mobiliser plusieurs secteurs et à réaménager radicalement leurs ressources et leurs stratégies[141]. Cette transformation peut prendre plusieurs formes: formation (ou recyclage) des militaires, réorganisation des services de renseignement chargés essentiellement de collecter des informations scientifiques et technologiques sensibles, de réaliser des simulations de cyberguerre et de conduire des exercices militaires tout en accordant une attention particulière aux applications des technologies de l'information[142]. Plusieurs pays ont lancé des concours au niveau national pour identifier et recruter les meilleurs cybercerveaux parmi leurs citoyens[143]. Les industries nationales sont aussi poussées à améliorer leurs capacités technologiques pour soutenir la nouvelle stratégie militaire. Certains gouvernements s'emploient aussi à constituer un groupe de pirates informatiques civils privés sur lequel ils pourraient compter en cas de besoin[144]. Il peut s'agir d'individus très férus de technologies ou même d'anciens pirates informatiques illégaux qui ont été recrutés et formés pour mettre leurs compétences au service de la sécurité nationale[145]. Certains pays vont jusqu'à utiliser des "mandataires", de louer les services de pirates informatiques ou de spécialistes d'autres pays qui travaillent pour leur compte[146]. Tous ces changements prouvent qu'il y a une rupture avec les stratégies de réaction aux cybermenaces au profit d'une tactique de guerre de

---

140 Iran (estimating Iran's cyberwarfare budget at around USD 76 million).

141 Gurmeet Kanwal, "China's Emerging Cyber War Doctrine", at 20, Journal of Defense Studies, 2009, disponible à l'adresse: www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf (examinant la politique chinoise en matière de guerre de l'information et l'acupuncture). [Hereinafter "Kanwal"].

142 Cyberwarfare: An Analysis of the Means and Motivations of Selected Nation States, Dartmouth College, Institute for Security, Technology, and Society, novembre 2004 at 2, www.ists.dartmouth.edu/docs/execsum.pdf (hereinafter "Selected Nations").

143 *Voir par exemple,* Richard Westcott, "UK Seeks Next Generation of Cybersecurity Specialists", *BBC News*, 26 July 2010, www.bbc.co.uk/news/technology-10742588.

144 Kanwal at 20.

145 Gordon Corera, "Cyber-security strategy launched", *BBC News,* 25 juin 2009, http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm?ad=1 (hereinafter "Corera"); Tom Gjelten, "Cyberwarrior Shortage Threatens U.S. Security", National Public Radio, 19 juillet 2010, www.npr.org/templates/story/story.php?storyId=128574055.

146 Eshel.

l'information plus proactive dans le but d'être efficace dans un environnement hautement technologique[147].

c) Créer des cyberunités militaires

Plusieurs pays ont réagi à la nouvelle menace d'une cyberguerre en affectant en affectant un grand nombre de miliaires à la tâche des combats virtuels[148]. Ce changement de politique se traduit par la constitution d'équipes de guerre virtuelle spécialisées dans la cybersécurité qui pourraient être intégrées dans d'autres unités de renseignement[149], voire la création d'entités entièrement nouvelles dans la structure militaire qui s'occuperaient des activités dans le cyberespace[150]. Ces nouvelles formations militaires entendent intégrer et préparer les ressources miliaires en vue d'opérations tout azimut dans le cyberespace[151]. Leur première tâche est souvent de protéger les réseaux militaires et de conduire des opérations militaires dans le cyberespace mais elles peuvent également être en charge de la sécurisation des réseaux privés et d'une grande partie des nombreuses opérations militaires[152].

d) Utiliser les cybertactiques pour être à égalité

En perfectionnant leurs tactiques de guerre électronique et de guerre de l'information, certains pays espèrent faire jeu égal avec les Etats qui comptent sur les systèmes logiciels et informatiques pour mobiliser leurs forces armées conventionnelles. Une

---

147 Kanwal at 20.

148 Certains pays ont fait état de leurs redéploiements massifs de personnel. *Voir* Cyber General (indiquant que les Etats-Unis ont réaffecté 30 000 militaires au cybercombat). Toutefois les informations concernant les stratégies de nombreux pays sont difficilement accessibles. Voir Robert McMillan, "Black Hat Talk on China's `Cyber Army´ Pulled After Pressure", *InfoWorld,* 15 July 2010, www.infoworld.com/print/130362.

149 Eshel.

150 Par exemple les Etats-Unis ont annoncé en 2009 la création d'une nouvelle unité cybermilitaire. Cyber General. Le Royaume-Uni a lui aussi annoncé la création d'un centre opérationnel de cybersécurité dans le cadre de sa stratégie de cybersécurité. Corera.

151 Voir "U.S. Cyber Command Fact Sheet", U.S. Department of Defense, 25 mai 2010, www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

152 Siobhan Gorman, "U.S. Backs Talks on Cyberwarfare", The Wall Street Journal, 4 juin 2010, http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html (notant que 90% de la puissance militaire des Etats-Unis est assurée par le secteur privé, selon des militaires américains), (hereinafter "Gorman").

telle transition suppose d'investir dans de nouveaux systèmes de commande automatisés ainsi que dans de nouveaux matériels – câbles en fibres optiques, satellites, systèmes de radiocommunications numériques haute fréquence – et de mettre davantage l'accent sur les systèmes de surveillance spatiale, aérienne, navale et au sol[153]. Certains gouvernements utilisent déjà les TIC et font appel à des militaires très férus de technologie pour surveiller leurs frontières nationales[154]. Les nouvelles cyberstratégies risquent de dépendre encore plus de ces ressources et des systèmes automatisés qui leur sont associés, pour la sécurisation des frontières. Parmi d'autres tactiques, on peut citer les opérations de commande et contrôle qui visent à perturber les flux d'informations de l'ennemi et qui ciblent les infrastructures TIC ennemies dans le but d'endommager et de détruire matériels, réseaux ou données stratégiques[155]. Il s'agit avant tout d'exploiter les points faibles des adversaires potentiels, c'est-à-dire leur dépendance vis-à-vis du cyberespace et des nouvelles technologies. Les pays disposant des moyens les plus importants en matière de cyberguerre ou de guerre conventionnelle risquent en fait d'être très fragilisés car la technologie même qui les rend forts est vulnérable à de nouvelles formes d'attaque comme les bombes logiques ou le piratage[156]. En exploitant l'asymétrie potentielle des opérations menées dans le cyberespace, certains pays espèrent neutraliser les capacités militaires de leurs adversaires[157].

e) Eduquer des citoyens et les sensibiliser aux problèmes liés à la cybersécurité

De l'avis de nombreux gouvernements, éduquer et sensibiliser les citoyens est une méthode très efficace de cyberdéfense[158]. En effet, les bases de données d'information hébergées par des entités publiques ou privées ainsi que les campagnes de sensibilisation qui sont organisées au niveau national contribuent à mieux

---

153 Kanwal at 16.

154 Kanwal at 14.

155 Kanwal at 18.

156 Radical Change ("les Etats-Unis étant le pays qui dépend le plus de l'Internet et qui est le plus automatisé c'est aussi le plus vulnérable aux cyberattaques").

157 Kanwal at 18; CRS Cyberwarfare at 11.

158 *Voir par exemple* Selected Nations at 5 (préconisant des efforts systématiques et soutenus pour changer la façon dont le peuple américain voit la sécurité des réseaux afin d'améliorer la cybersécurité dans le pays).

sensibiliser les citoyens à la base[159]. Ces programmes, qui s'adressent à des particuliers ou à de petites entreprises, visent à leur apprendre comment protéger leurs informations et leurs systèmes contre des cyberdélits, comme l'usurpation d'identité ou le piratage. Dans la plupart des cas, l'accès illégal au système informatique n'est qu'une première étape, laquelle est essentielle et le piratage d'ordinateurs ou de systèmes individuels peut être le préalable à des délits plus graves qui affectent la sécurité nationale, par exemple l'espionnage de données ou des attaques de déni de service. Pour ces "délits", lorsqu'ils sont dirigés contre des ressources nationales ou des entités gouvernementales stratégiques, il est plus judicieux de parler de cyberattaques ou de cyberguerre. Des pirates informatiques essaient déjà régulièrement d'infiltrer les gouvernements, les entreprises privées et les systèmes de défense nationaux, avec un succès non négligeable[160]. L'espionnage de données ou l'accès à des informations sensibles peuvent se faire à la fois par des moyens techniques ou par "manipulation des structures sociales" ("social engineering") tactique qui consiste à duper les personnes et les amener, sous de faux prétextes, à donner accès à des systèmes qui sont par ailleurs sécurisés[161]. Par conséquent, le fait d'éduquer les citoyens sur l'utilisation de moyens de subversion psychologique ou de moyens techniques, par exemple le fait de laisser des clés de mémoire infectées dans des lieux publics peut contribuer à protéger les ressources nationales[162].

---

159 Par exemple le National Computer Board de Maurice qui est rattaché au Ministère des technologies de l'information et de la communication supervise un portail de sensibilisation à la cybersécurité disponible à l'adresse: www.gov.mu/portal/sites/ncbnew/main.jsp, et les Etats-Unis consacrent chaque année en octobre un mois à la sensibilisation au problème de la cybersécurité. Les partenariats public/privé tels que la National Cybersecurity Alliance, éduquent également les utilisateurs et les gestionnaires des infrastructures numériques en leur apprenant à construire des systèmes et des mécanismes de protection résistants. Voir "About Us", The National Cybersecurity Alliance, www.staysafeonline.org/content/about-us.

160 *Voir par exemple*, Understanding at 20 (donnant les cibles célèbres de diverses attaques de piratage dont le Pentagone, le gouvernement allemand, Google, Ebay et la NASA). **ITU - this citation has not been listed before. Need full citation**.

161 *Voir également* at 23–24.

162 Par exemple, en 2008, le commandement central des Etats-Unis a été infiltré par une clé publique infectée *Voir* Fifth Domain.

f) Pays moins connectés et pays en développement

De nombreux pays dépendent beaucoup des TIC et de l'Internet pour leurs infrastructures et leurs services essentiels, tandis que d'autres ne sont pas aussi tributaires ou connectés et utilisent les réseaux intranets nationaux ou d'autres ressources que les TIC. Toutefois, il semble que ces pays, eux aussi, augmentent leurs moyens en ligne même si ces avancées se limitent aux utilisations militaires ou gouvernementales[163]. Les pays qui sont entrés dans le monde en ligne plus récemment sont peut-être moins vulnérables aux cyberattaques car leurs systèmes publics partagent moins de connexions avec le reste du cyberespace[164]. Pourtant, même les pays en développement qui ne possèdent pas encore l'infrastructure qui leur permettrait de bénéficier de tous les avantages rendus possibles par les TIC restent dépendants de l'Internet et d'autres technologies mobiles ou numériques pour certains de leurs besoins essentiels[165]. Ils sont donc eux aussi concernés par l'avenir de la cybersécurité.

7.2 Réactions internationales récentes

Aujourd'hui, les efforts déployés au niveau international pour faire face à la menace d'une cyberguerre sont beaucoup moins nombreux que les stratégies nationales, même si des initiatives ont été lancées au niveau multilatéral. Des tentatives ont été faites au niveau bilatéral mais elles sont bien loin d'une stratégie globale susceptible d'améliorer la cybersécurité et de garantir la paix dans le cyberespace étant donné qu'elles ne font intervenir qu'un très petit nombre des acteurs concernés dans l'équation de la cyberpaix. Certains pays ont lancé un appel pour que soit élaboré un traité visant à limiter l'utilisation des cyberarmes, contrairement à d'autres pour qui un tel traité est soit inutile, soit prématuré[166]. Ces propositions sont bien sûr un pas fait dans la direction d'une collaboration internationale, mais elles sont là aussi bien loin d'une approche véritablement globale et d'une stratégie claire pour aller de

---

163 Martyn Williams, "North Korea Moves Quietly Onto the Internet", *Computerworld*, 10 juin 2010, www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet.

164 Corera.

165 Voir par exemple "Economic and Social Council Opens General Segment of 2010 Session", at 3, ECOSOC/6444, 16 juillet 2010, www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm (examinant la question de l'argent électronique ou le système d'argent électronique utilisé dans les pays africains) (hereinafter "ECOSOC 2010").

166 Gorman.

l'avant, une stratégie impliquant toutes les parties prenantes intéressées. Certaines réactions internationales récentes sont décrites dans les paragraphes qui suivent mais la liste n'est pas exhaustive.

a) Office des Nations Unies contre la drogue et le crime (ONUDC) – Congrès des Nations Unies pour la prévention du crime et la justice pénale (UNCPCJ)

En avril 2010, le douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale a élaboré un ensemble de déclarations qui comprenaient une disposition appelant à la création d'un Groupe d'experts intergouvernementaux qui serait chargé d'étudier le problème de la cybercriminalité et les solutions que l'on pourrait y apporter au niveau international[167]. Au cours de la 19ème session de la Commission pour la prévention du crime et la justice pénale, les Etats Membres ont élaboré une recommandation en la matière demandant que la Commission crée un Groupe d'experts intergouvernementaux à composition non limitée[168]. Même s'il n'est pas arrivé à un consensus quant à l'élaboration d'un nouveau traité sur la cybercriminalité, le Congrès a conclu des accords sur l'assistance technique et le renforcement des capacités qui constituent déjà une bonne base de discussion pour les mesures à prendre[169].

b) Conseil économique et social des Nations Unies (ECOSOC)

Le Conseil économique et social des Nations Unies (ECOSOC) a ouvert sa session de 2010 sur une communication consacrée aux problèmes liés à la cybersécurité ainsi qu'aux menaces et aux possibilités liées à l'utilisation toujours croissante de l'Internet. Entre autres choses, le Conseil a insisté sur la nécessité de prendre des mesures au niveau international dans les domaines de l'échange d'informations, des bonnes pratiques, de la formation et de la recherche. Les membres du panel ont par ailleurs

---

167 "Projet de Déclaration du Salvador sur des stratégies globales pour les défis mondiaux: systèmes de prévention du crime et de justice criminelle et élaboration de tels systèmes dans un monde en pleine évolution" Déclaration 42, 12ème Congrès des Nations Unies pour la prévention du crime et la justice pénale, 18 avril 2010, www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529031A_CONF213_L6_REV2_E.pdf.

168 "Rapport du 12ème Congrès des nations Unies pour la prévention du crime et la justice pénale", UNODC, Salvador, Brésil, 12-19 avril 2010, www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf.

169 "Résumé des résultats concernant la cybercriminalité: 12ème Congrès des Nations Unies pour la prévention du crime et la justice pénale ", Projet relatif à la cybersécurité, 26 avril 2010, www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/2079_UNCC_cyberoutcome.pdf.

indiqué que les Nations Unies devaient faire front commun face au problème de la cybersécurité et qu'il fallait renforcer non seulement la coopération entre les pays, mais aussi la collaboration entre les Etats et le secteur privé afin de garantir la cybersécurité[170]. Ils ont prévenu que la dimension internationale et les graves conséquences d'une cyberguerre réelle exigent une réponse coordonnée et que les solutions ad hoc ou un renforcement des défenses ne suffisent plus aujourd'hui[171].

c) Organisation du Traité de l'Atlantique Nord (OTAN)

L'OTAN a mis en œuvre sa propre politique de cyberdéfense en 2008 afin de protéger ses ressources technologiques et celles de ses Etats Membres[172]. Dans le cadre de cette politique, l'Alliance à créé une Autorité de gestion de la cyberdéfense, une Capacité d'intervention en cas d'incident informatique, qui prévoit l'envoi d'Equipes de réaction rapide (RRT) dans les différents pays membres et un Centre d'excellence pour la cyberdéfense en coopération[173]. Situé en Estonie, ce Centre regroupe des experts qui mènent des travaux de recherche et proposent une formation dans le domaine de la cybersécurité. Parmi les pays qui ont financé ce centre, on compte l'Estonie, la Lettonie, la Lituanie, l'Allemagne, l'Italie, la République slovaque, et l'Espagne[174].

En outre, l'OTAN a également organisé des exercices de cyberdéfense dans le cadre desquels des équipes des Etats Membres apprennent à défendre des réseaux informatiques virtuels contre des cyberattaques. Ces exercices sont destinés à mieux faire comprendre ce qu'est le cyberenvironnement international et à renforcer la coopération internationale pour faire face aux incidents techniques[175]. L'OTAN a également signé avec l'Estonie, les Etats-Unis, le Royaume-Uni, la Turquie et la Slovaquie des mémorandums d'accord concernant la cybersécurité [176].

---

170 ECOSOC 2010.

171 *Id.* (examinant le système d'argent numérique ou d'argent électronique utilisé dans les pays africains).

172 "Se défendre contre des cyberattaques", OTAN www.nato.int/cps/en/natolive/topics_49193.htm.

173 "OTAN 2020", www.nato.int/cps/en/natolive/official_texts_63654.htm?selectedLocale=en.

174 Centre d'excellence pour la cyberdéfense en coopération, www.ccdcoe.org/.

175 "Exercices de défense pour améliorer les compétences en matière de lutte contre les cyberattaques", NATO-News, 10 mai 2010, www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news_63177.htm.

176 "L'OTAN et l'Estonie ont conclu un accord de cyberdéfense", NATO-News, 23 avril 2010, www.nato.int/cps/en/natolive/news_62894.htm.

d) Conseil de l'Europe – Convention de Budapest sur la cybercriminalité

La Convention sur la cybercriminalité du Conseil de l'Europe[177] contient des dispositions juridiques types concernant certains cyberdélits que les pays peuvent adopter et adapter à leurs besoins spécifiques. Elle apporte certaines solutions juridiques pour des délits comme l'accès illégal (piratage) ou l'interception illégale mais elle ne prévoit rien pour certaines des formes les plus menaçantes de cyberintrusions comme l'espionnage ou le sabotage de données. Même si la Convention contribue à encourager la coopération internationale en érigeant en infraction pénale les principaux cyberdélits, son pouvoir normatif est limité par le fait que le rédacteur s'est efforcé de ne pas enfreindre d'autres législations nationales potentiellement conflictuelles. Des différences culturelles et juridiques importantes ralentissent l'élaboration d'un droit unifié, voire la rendent tout à fait impossible[178]. Trente pays seulement ont ratifié le Traité depuis son ouverture à la signature en novembre 2001, un seul de ces pays étant un pays non européen[179].

Des dispositions juridiques comme celles qui sont contenues dans la Convention sont un moyen de faire face à certaines des menaces qui pèsent sur la cybersécurité aux niveaux national ou international. Toutefois les dispositions de la Convention ne traitent pas directement de la question d'une cyberguerre entre pays. La menace de sanctions peut certes décourager certains cyberdélinquants en puissance mais ce type de législation ne va peut être pas assez loin pour dissuader des agresseurs qui sont persuadés qu'ils peuvent échapper à toute détection, identification ou poursuite.

e) Accords bilatéraux sur la cybersécurité

Des Etats, à titre individuel, essaient de nouer des relations avec d'autres pays dans le domaine de la cybersécurité. Le Ministère indien des communications et des technologies de l'information a noué des liens de collaboration en signant avec de nombreux autres pays des mémorandums d'accord ou en lançant des programmes de développement ou de partage de l'information. L'Inde et la Corée du sud ont signé en 2004 une déclaration commune de coopération bilatérale dans le domaine des

---

177 Convention sur la cybercriminalité CETS N° 185, Conseil de l'Europe http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last visited on 10 Aug. 2010 (hereinafter "Convention").

178 "National Security Threats in Cyberspace", American Bar Association, Standing Committee on Law and National Security and National Strategy Forum, septembre 2009 at 13, www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (hereinafter "Workshop").

179 Convention.

technologies de l'information et l'Equipe indienne d'intervention en cas d'incident informatique a également signé un mémorandum d'accord avec le Centre national de cybersécurité de la Corée en vue de mettre en place une collaboration officielle, entre autres, dans le domaine de la cybersécurité[180]. L'Inde a par ailleurs conclu un certain nombre d'autres accords bilatéraux concernant les technologies de l'information et un petit nombre d'accords portant spécifiquement sur la cybersécurité et la cybercriminalité[181].

Le Maroc et la Malaisie ont également signé un mémorandum d'accord sur la cybersécurité lors de la Conférence régionale sur la cybersécurité qui s'est tenue au Maroc au début de cette année[182]. Dans le cadre de ce mémorandum d'accord, les ministres des deux pays chargés de la cybersécurité ont noué des liens de coopération dans divers domaines, notamment la protection des infrastructures essentielles de l'information, l'élaboration de cadres pour la cybersécurité, le renforcement des capacités, la formation et la sensibilisation. Ces formes de collaboration peuvent bien sûr améliorer la cybersécurité d'un pays, mais elles ne suffisent pas pour protéger un pays quelconque contre une cyberguerre mondiale. Il faut donc mettre en place une structure globale plus complète dans le domaine de la cybersécurité pour garantir le maintien de la paix entre toutes les nations.

f) Union internationale des télécommunications (Commission d'études 17 de l'UIT-T) – Normes mondiales

Pour faire face au problème grandissant de la cybersécurité, en particulier en ce qui concerne les réseaux intelligents, l'UIT a créé un Groupe d'action sur les réseaux intelligents chargé de collecter les informations et les idées qui pourraient être utiles pour l'élaboration de Recommandations sur les réseaux intelligents sous l'angle des télécommunications[183]. Les groupes d'action sont un instrument de l'UIT qui enrichit

---

180 "Coopération bilatérale: Asie", Département indien des technologies de l'information, gouvernement de l'Inde, Ministère des communications et des technologies de l'information www.mit.gov.in/content/bilateral-cooperation (hereinafter "Cooperation").

181 Par exemple, la coopération de l'Inde avec Brunei, la Malaisie, la France et l'Australie est axée sur la sécurité de l'information et/ou la cybercriminalité alors que d'autres relations sont centrées sur le développement des ressources et des moyens. Cooperation.

182 "La Malaisie et le Maroc sont désormais partenaires dans le domaine de la cybersécurité", CyberSecurity Malaysia, 24 janvier. 2010, www.cybersecurity.my/data/content_files/44/632.pdf?.diff=1265036362.

183 Pour plus d'informations sur les groupes d'action voir le site www.itu.int/ITU-T/focusgroups/smart/.

le programme de travail des commissions d'études en ce sens qu'ils offrent un autre environnement de travail pour élaborer rapidement des spécifications dans un domaine particulier[184]. Ils sont aujourd'hui largement utilisés pour répondre aux besoins en constante évolution de l'industrie et tout à fait adaptés à l'évolution rapide des technologies comme celles des réseaux intelligents. Le Groupe d'action sur les réseaux intelligents (FG Smart) qui regroupe des représentants de différents Etats Membres collaborera avec les organismes qui, à l'échelle mondiale, s'intéressent à ces réseaux (par exemple des instituts de recherche, des forums, des établissements universitaires). Pour atteindre son objectif, à savoir élaborer des recommandations définissant des normes pour les réseaux intelligents, le Groupe d'action tiendra à jour une liste évolutive des organismes de normalisation s'occupant des réseaux intelligents, recueillera les points de vue et évaluera les propositions concernant ces réseaux, fournira la terminologie nécessaire, collectera les nouvelles idées, définira d'éventuels domaines d'étude pour ces réseaux et déterminera enfin l'incidence éventuelle de la normalisation dans des domaines tels que la sécurité, la confidentialité des données et l'interopérabilité[185]. Le Groupe aura ainsi une approche pluridisciplinaire des problèmes de plus en plus nombreux et en constante évolution que pose la cybersécurité pour ce qui est des réseaux intelligents.

En outre, à travers ses liens avec le Secteur de la normalisation des télécommunications (UIT-T) de l'UIT, l'une des organisations de normalisation les plus reconnues pour ce qui est des télécommunications, le Groupe d'action sera une source d'informations fiables et unifiées, ayant la réputation d'élaborer des normes de qualité et consensuelles. Le lien avec l'UIT-T contribuera à mieux faire connaître, au besoin, les produits du Groupe d'action, à travers les Recommandations, les Suppléments, les Manuels de l'UIT-T, etc. Faisant partie de l'UIT-T, ce Groupe d'action pourra mieux faire accepter ses spécifications sur de nombreux marchés mondiaux, en particulier dans les pays en développement et dans les régions autres que celles qui participent plus activement aux activités du forum.

---

184 Groupes d'action de l'UIT-T, voir le site: www.itu.int/ITU-T/focusgroups/.

185 Mandat du Groupe d'action de l'UIT-T sur les réseaux intelligents disponible à l'adresse: www.itu.int/ITU-T/focusgroups/smart/tor.html.

7.3 Nécessité d'un cadre international

a) Non-viabilité de la dissuasion

Chaque nouveau domaine d'activité apporte de nouveaux problèmes. Tout comme les questions d'attribution, d'efficacité d'utilisation ou de résolution des conflits se sont posées dans le passé et continuent de se poser aujourd'hui sur les théâtres d'opérations terrestres, maritimes, aériennes ou spatiales, le cyberespace fait naître de nouvelles difficultés et de nouvelles incertitudes. La cybersécurité est un problème qui concerne toute personne qui est connectée et en raison de la dépendance croissante vis-à-vis des TIC pour l'infrastructure sociale de base, ce problème touche aujourd'hui même ceux qui ne sont pas connectés. Les attaques lancées contre l'infrastructure de l'information et les services Internet peuvent aujourd'hui causer des préjudices graves à la société. En raison des caractéristiques propres d'une cyberguerre et des problèmes spécifiques qu'elle pose, les stratégies de maintien de la paix qui ont fait leurs preuves dans le passé risquent de plus être efficaces.

Pendant longtemps, les pays ont misé sur la dissuasion pour assurer le maintien de la paix et de la sécurité face à des armes qui pouvaient causer des destructions massives. Or, l'efficacité de la dissuasion dépend de certaines circonstances et hypothèses dont bon nombre ne s'appliquent pas dans le cyberespace[186]. La dissuasion nécessite généralement la présence de quatre grands éléments: l'identification de l'auteur de l'attaque (savoir qui vous a attaqué); l'origine de l'attaque (savoir d'où est partie l'agression); la riposte à l'attaque (pouvoir riposter si l'on est attaqué le premier); et la transparence (l'ennemi connaît votre capacité et votre intention de riposter massivement par la force)[187]. Le cyberespace et la cyberguerre posent de nouveaux problèmes qui remettent en cause l'hypothèse de base, à savoir l'existence de ces quatre éléments lorsque des pays construisent leurs arsenaux militaires défensifs. Les TIC multiplient les façons dont un agresseur peut masquer son identité ou l'emplacement où il se trouve; les agresseurs peuvent utiliser des "mandataires" ou des services, par exemple des terminaux Internet publics, des réseaux hertziens ou des services mobiles à prépaiement qui ne nécessitent pas d'authentification. Les technologies de cryptage qui sont techniquement essentielles pour garantir la

---

186 Radical Change (citant l'ancien conseiller américain à la défense Richard Clarke qui affirmait que, "la force qui a empêché la guerre nucléaire – la dissuasion – ne fonctionne pas pour la cyberguerre").

187 Tang Lan etZhang Xin, "Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, The U.S., Russia, India, and Norway,* EastWest Institute, avril 2010 at 1, www.ewi.info/system/files/CyberDeterrenceWeb.pdf.

confidentialité, l'intégrité et la disponibilité des données peuvent aussi être utilisées pour masquer les identités ou, à tout le moins, ralentir la progression d'une enquête sur l'origine d'une cyberattaque. Les processus et les politiques techniques qui limitent la rétention de données concernant le trafic Internet contribuent aussi à régler ce problème de l'identité et de la localisation de l'attaquant.

Le risque d'exercer des représailles contre la mauvaise cible ainsi que l'incertitude qui entoure les dommages collatéraux d'une cybercontre-attaque - qui pourrait facilement nuire à un allié ou une partie neutre – limite encore plus la capacité des Etats à riposter à une attaque[188]. Si les agresseurs estiment qu'ils peuvent conserver leur anonymat ou ne croient pas que leurs victimes vont riposter par la force militaire de peur de violer les normes internationales, la menace de représailles est alors très peu efficace. En ripostant par la force à une cyberattaque où la force militaire conventionnelle n'a pas été utilisée et qui vise plus à exploiter qu'à détruire, une victime exerçant des représailles court le risque que la communauté internationale interprète son acte comme un acte d'agression non justifié[189]. Le fait de miser sur une stratégie de dissuasion incite aussi les pays à afficher des postures agressives les unes vis-à-vis des autres et à inventer de nouvelles menaces de représailles dans différents domaines pour compenser les éventuelles asymétries, ce qui compromet les avantages d'une intégration plus poussée et accroît les tensions entre pays[190]. De toutes ces façons, les caractéristiques fondamentales du cyberespace nuisent à l'efficacité de la dissuasion en tant qu'approche de la cyberpaix.

Le cadre même des approches juridique existantes n'est peut-être plus adapté pour gérer les risques liés à la cybersécurité. Par exemple, en vertu du droit international en vigueur, par exemple dans l'Article 51 de la Charte des Nations Unies, un Etat peut exercer son droit de légitime défense lorsqu'il est l'objet d'une agression armée. Dans le cas d'un cyberconflit, de nouvelles questions surgissent: quand une cyberattaque peut elle être assimilée à une agression armée et, alors, la responsabilité de l'attaque peut elle être attribuée à un Etat[191]. La doctrine reconnue de la "responsabilité de l'Etat" apporte, semble-t-il, quelques éléments de réponse à cette dernière

---

188 James A Lewis, "Cross-Domain Deterrence and Credible Threats", Center for Strategic and International Studies, juillet 2010, http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf.

189 *Id*.

190 *Id.*

191 Workshop at 14.

interrogation; selon cette doctrine en effet, chaque Etat doit agir pour empêcher que son territoire ne soit utilisé pour perpétrer de telles agressions à l'encontre d'autres Etats et s'il refuse de prendre des mesures préventives, il peut être tenu responsable de ces agressions. Toutefois, comme nous l'avons vu lors de notre réflexion préliminaire sur les cyberattaques, il devient extraordinairement difficile de répondre à ce type de question pratique dans le cyberespace: en effet, certaines attaques n'ont pas d'origine géographique (comme c'est le cas avec les "botnets" – réseaux zombies), elles peuvent traverser plusieurs frontières, être le fait de coalitions relevant de plusieurs juridictions ou d'un "mandataire" qui ne fait qu'agir pour le compte du véritable agresseur. Parfois, les Etats eux-mêmes ne sont pas en mesure de découvrir ou de vérifier quels agresseurs agissent dans les limites de leur propre territoire. Et, même dans le cas où un Etat pourrait déterminer l'identité de l'attaquant qui opère sur son territoire géographique, la nature même du cyberespace fait qu'il est impossible pour une seule et même entité d'exercer un plein contrôle[192]. Par conséquent, non seulement la question de l'origine de l'attaque mais aussi celle du contrôle deviennent inévitablement troubles.

b) Nécessité d'un cadre international

Etant donné que les normes et les instruments juridiques internationaux existants ne sont pas parfaitement adaptés pour traiter les nouveaux problèmes que pose la cybersécurité, des discussions et une collaboration mondiales sont aujourd'hui nécessaires. L'évolution de la technologie elle-même – avec les chevauchements de plus en plus nombreux entre juridictions nationales, les TIC, les ressources et les systèmes en ligne – rend encore plus cruciale l'adoption d'un nouvel ensemble de stratégies et la mise en place d'une coopération internationale pour garantir le maintien de la paix dans le cyberespace[193].

Des cyberattaques peuvent être lancées n'importe où dans le monde et frapper n'importe quel pays; ces menaces ont donc par nature une dimension internationale et exigent une coopération internationale, une assistance en matière d'enquête ainsi que l'adoption de dispositions matérielles et de procédure communes pour y faire face. Par ailleurs, il est largement admis que la coopération internationale est une des conditions indispensables à la cybersécurité mondiale. En 2003 et 2005, les pays réunis lors du Sommet mondial sur la société de l'information (SMSI) ont convenu de la nécessité de disposer d'outils efficaces aux niveaux national et international pour

---

192 *Id.*

193 *Id.*

promouvoir la coopération internationale dans le domaine de la cybersécurité[194]. Cette collaboration internationale devrait être dictée non seulement par un désir mutuel de paix mais aussi par les intérêts bien compris de chaque pays. Chaque pays étant aujourd'hui tributaire plus que jamais de la technologie pour le commerce, les opérations financières, les soins de santé, les services d'urgence, la distribution des produits alimentaires, la perte de réseaux vitaux paralyserait rapidement n'importe lequel d'entre eux et personne n'est à l'abri d'une cyberattaque. La prééminence des TIC et l'interconnectivité des nouvelles technologies préfigurent un nouvel ordre mondial qui justifie une collaboration sur ces nouvelles questions pour garantir la stabilité.

Il est essentiel que les pays harmonisent leurs cadres juridiques pour lutter contre la cybercriminalité et promouvoir une coopération internationale dynamique et multiforme. Les Etats devraient définir un cadre juridique et réglementaire commun et prévoir un système de mise à jour régulière des législations compte tenu de la nature évolutive des menaces sécuritaires. Certains groupes se sont déjà prononcés en faveur de normes internationales et de cybernormes pour améliorer la cybersécurité au niveau international[195]. Quoi qu'il en soit, une stratégie efficace de cyberpaix doit être souple, modulable pour pouvoir s'adapter à la rapidité des progrès technologiques, à l'essor des TIC et aux problèmes de sécurité inhérents. Les pays doivent également s'entendre sur des procédures et des méthodes pour déterminer l'origine d'une attaque et l'identité de son auteur afin de régler le problème des cyberattaques anonymes et des imbroglios internationaux qu'elles menacent de créer. Les propositions d'élaboration d'un accord international faisant obligation à chaque pays de contrôler son propre cyberespace sont une tentative pour résoudre le problème de l'établissement de l'identité de l'agresseur; le fait de lier responsabilité et origine géographique risque d'esquiver le processus délicat de l'identification, avec certitude, de l'auteur d'une cyberattaque[196]. Toutefois, ces propositions laissent sans solution le

---

194 SMSI: Agenda de Tunis pour la société de l'information, paragraphe 40, Sommet mondial de la société de l'information, WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 novembre 2005, www.itu.int/wsis/docs2/tunis/off/6rev1.html (ci-après "Agenda de Tunis").

195 Des participants à un atelier, y compris des membres de l'American Bar Association Standing Committee on Law and National Security, de la McCormick Foundation et du National Strategy Forum ont réfléchi à la constitution d'un groupe international spécialisé dans la cybersécurité qui serait chargé d'élaborer des normes et des règles pour améliorer la cybersécurité. Workshop at 26.

196 Robert Mullins, "Pearl Harbor' post struck a nerve", *NetworkWorld*, 11 mars 2010, www.networkworld.com/community/node/58450 (citant l'ancien conseiller spécial à la sécurité du président américain Richard Clarke lors d'une récente réunion-débat sur la cybersécurité).

problème de l'identification des "mandataires" et celui de la détermination de l'origine géographique d'une attaque. Compte tenu des lacunes des approches classiques et des approches existantes en matière de sécurité internationale, il est clair que la communauté mondiale doit adopter une nouvelle stratégie pour faire face aux problèmes liés à la cybersécurité et pour garantir une cyberpaix durable.

7.4 Propositions de principes internationaux dans le cyberespace

Pour élaborer des principes directeurs relatifs à la cyberpaix, nous devons prendre en considération les caractéristiques spécifiques du cyberespace et les difficultés qui en découlent. Nous pouvons toutefois toujours nous inspirer d'autres initiatives entreprises pour lutter contre des menaces internationales, par exemple la Convention contre la criminalité transnationale organisée, pour étayer notre propos. Comme la criminalité transnationale organisée, les cyberattaques ne connaissent pas les frontières nationales et empruntent des réseaux complexes qui doublent les systèmes exploités à des fins pacifiques et productives. La Convention illustre l'idée partagée selon laquelle la solution à ces problèmes transnationaux répandus passe par une coopération internationale étroite et l'adoption de nouveaux cadres, une assistance mutuelle en matière juridique et dans le domaine du développement, un partage de l'information et une coopération en vue de respecter la loi[197].

Certains éléments indispensables à un plan de cyberpaix existent déjà dans des principes juridiques bien établis et des normes adoptées au niveau international. En particulier, l'Article 19 de la Déclaration universelle des droits de l'homme énonce le 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 considération de frontières les informations et les idées, par quelque moyen d'expression que ce soit[198]. Dans sa Déclaration de principes de Genève de 2003, le Sommet mondial sur la société de l'information (SMSI) a réaffirmé l'idée que la liberté de communiquer est un fondement essentiel de la société de l'information[199]. La

---

197 Convention contre la criminalité transnationale organisée par l'Office des Nations Unies contre la drogue et le crime, 2004, www.unodc.org/unodc/en/treaties/CTOC/index.html.

198 Déclaration universelle des droits de l'homme, Article 19, Assemblée générale des nations Unies, Résolution. 217A (III), U.N. GAOR, U.N. Doc. A/810, 1948, www.un.org/en/documents/udhr/index.shtml#a19.

199 Déclaration de principes de Genève, paragraphe 4, Sommet mondial sur la société de l'information 2003: www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

Déclaration ajoute que la communication est un processus social fondamental et un besoin essentiel de l'être humain et la base de toute organisation sociale. Par conséquent, tout un chacun devrait avoir un accès équitable aux technologies de l'information et de la communication. Les Nations Unies se sont engagées à mettre cet accès à la disposition de tous et à pleinement exploiter le potentiel de la révolution numérique en ce sens[200].

Bien qu'il existe de nombreuses différences entre la technologie nucléaire et les TIC, ces initiatives de collaboration internationale pour le maintien de la paix nucléaire, en raison de similarités importantes, sont riches d'enseignements pour l'élaboration d'une stratégie de cyberpaix. Tout comme le cyberespace et les TIC, l'énergie nucléaire et la technologie nucléaire ont un certain nombre d'utilisations pacifiques et d'utilisations militaires. Elles peuvent causer des dommages considérables si elles sont utilisées pendant une attaque. Par ailleurs, elles pourraient être utilisées contre n'importe quel pays mais tous les pays subiraient les conséquences d'une telle attaque[201]. Consciente du fait que la menace d'une attaque nucléaire est, par essence, mondiale, la communauté internationale a cherché à mettre en place une stratégie de collaboration multilatérale qui prévoit l'élaboration d'une approche commune et la prise d'un engagement commun en faveur de la sécurité nucléaire[202]. Des traités comme le Traité de non-prolifération des armes nucléaires (TNP) sont une réponse efficace au problème de la préservation des utilisations pacifiques de matériels qui peuvent avoir des effets dévastateurs et qui ne connaissent pas les frontières nationales. Dans le cadre du TNP, la responsabilité concernant les matières nucléaires est basée sur la juridiction nationale ou les activités "exercées sous le contrôle [d'un Etat] en quelque lieu que ce soit"[203]. Lors du Sommet 2010 sur la sécurité nucléaire, 47 pays se sont engagés de nouveau à sécuriser les matières nucléaires sous leur contrôle, à continuer de renforcer la sécurité en fonction de l'évolution de la situation et de partager les bonnes pratiques et des solutions concrètes pour la sécurité[204].

---

200 "Ban urges greater use of digital technology to improve living conditions", UN News Centre, 17 May 2010, www.un.org/apps/news/story.asp?NewsID=34716.

201 National Statement of the United States, 2010 Nuclear Security Summit, 13 avril 2010, www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states (hereinafter "National Statement of the United States").

202 *Id.*

203 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), Art. 3, 1970, www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglish_Text.pdf (hereinafter "NPT").

204 National Statement of the United States.

Le TNP met en avant les avantages des applications pacifiques de la technologie nucléaire et l'importance de rendre ces avantages accessibles à tous les Etats, y compris les pays en développement[205]. Le Traité souligne l'importance d'une coopération internationale, de tous les Etats, y compris l'échange d'informations et de renseignements en vue du développement plus poussé des utilisations de l'énergie atomique à des fins pacifiques[206]. Par ailleurs, en vertu de l'Article 3 du TNP, les signataires s'engagent à accepter des garanties qui sont destinées à empêcher que l'énergie nucléaire ne soit détournée de ses utilisations pacifiques vers des armes nucléaires ou d'autres dispositifs explosifs nucléaires[207]. L'Agence internationale de l'énergie atomique, reconnue pour son expérience, ses compétences, et sa capacité à faciliter les discussions dans un cadre neutre, est chargée de superviser la négociation et la conclusion d'un accord entre Etats qui définira un tel système de garanties[208]. Parmi d'autres initiatives de collaboration pour garantir la paix nucléaire, on peut citer l'Initiative mondiale de lutte contre le terrorisme nucléaire, partenariat international regroupant des pays qui se sont engagés à œuvrer individuellement ou collectivement pour mettre en œuvre un ensemble de principes communs de sécurité nucléaire[209]. Ces principes sont notamment les suivants: développer et améliorer les mesures de gestion, de contrôle et de sécurité des substances nucléaires et des installations nucléaires civiles, améliorer les capacités de détection et de contrôle des Etats membres, ne pas héberger de terroristes, améliorer les capacités d'intervention et d'investigation des membres en cas d'attaque et promouvoir le partage de l'information[210].

Les initiatives internationales en faveur de la paix prises dans d'autres secteurs nouveaux, semble-t-il, innombrables prônent une large coopération internationale. Par exemple, la Déclaration des principes juridiques régissant les activités des Etats en matière d'exploration et d'utilisation de l'espace extra-atmosphérique comprend, entre autres principes directeurs, celui selon lequel, en ce qui concerne l'exploration

---

205 TNP, Préambule et Article 5.

206 *Id.* Préambule

207 *Id Article*. 3.

208 *Id.*

209 "The Global Initiative to Combat Nuclear Terrorism", Département d'Etat des Etats-Unis www.state.gov/t/isn/c18406.htm.

210 "Déclaration de principes", The Global Initiative to Combat Nuclear Terrorism, Département d'Etat des Etats-Unis, www.state.gov/documents/organization/141995.pdf.

et l'utilisation de l'espace extra-atmosphérique, tous les Etats devront se fonder sur les principes de la coopération et de l'assistance mutuelle[211].

Conscient du risque croissant qu'une cyberattaque pourrait être lancée n'importe où et toucher n'importe quel pays, le Secrétaire général de l'UIT propose cinq principes directeurs pour l'établissement et le maintien de la paix dans le nouveau cybermonde. Ces principes incarnent et promeuvent les valeurs et la culture que l'Union internationale des télécommunications défend depuis toujours en tant qu'organisation internationale de tout premier plan en matière de normalisation et de réglementation. Le Règlement des télécommunications internationales (RTI) de l'UIT qui fait autorité n'est qu'un exemple de cette tradition qui consiste à encourager le développement harmonieux et le bon fonctionnement des télécommunications et l'accès universel à ces technologies. Le RTI a été conçu comme un nouveau cadre réglementaire pour répondre aux problèmes que posait le nouveau paysage des télécommunications à la fin des années 80[212]. Elaboré pour encourager l'efficacité et le développement dans un contexte de collaboration, de coopération et d'équité d'accès, il illustre bien la tradition qui est celle de l'UIT. Il reflète également la volonté primordiale de l'institution de protéger le droit de communiquer tout en évitant de porter atteinte aux installations.

Les cinq principes proposés par le Secrétaire général de l'UIT en matière de cyberpaix intègrent eux aussi ces valeurs essentielles tout en définissant des mesures et des obligations bien précises qui garantiront la paix et la stabilité dans le cyberespace. Ces principes sont les suivants:

1. Tout gouvernement devrait s'engager à donner à ses citoyens l'accès aux communications.
2. Tout gouvernement devrait s'engager à protéger ses citoyens dans le cyberespace.
3. Tout pays s'engagera à ne pas héberger de terroristes/criminels sur son propre territoire.

---

211 Déclaration de principes juridiques régissant les activités des Etats en matière d'exploration et d'utilisation pacifique de l'espace extra-atmosphérique ("Traité sur l'espace extra-atmosphérique"), Principe 6, 1967, www.oosa.unvienna.org/oosa/SpaceLaw/lpos.html.

212 "Règlement des télécommunications internationales: Actes finals de la Conférence administrative mondiale télégraphique et téléphonique" Union internationale des télécommunications, 1989, www.itu.int/osg/spu/intset/itu-t/mel88/mel-88-e.pdf.

4. Chaque pays devrait s'engager à ne pas être le premier à lancer une cyberattaque contre un autre pays.
5. Chaque pays doit s'engager à collaborer avec les autres pays dans un cadre international de coopération afin de garantir le maintien de la paix dans le cyberespace.

8 Programme mondial cybersécurité de l'UIT

Par Hamadoun I. Touré

L'UIT constitue une instance mondiale unique pour débattre de la cybersécurité. L'institution joue en effet un rôle majeur dans le domaine des télécommunications, de la sécurité de l'information et de la normalisation, à divers titres et ce depuis sa fondation en 1865, il y a près de 145 ans. Consciente que la cybersécurité est un problème important qui nécessite une action multi-parties prenantes coordonnée, l'Union œuvre à la réalisation de cet objectif. Elle s'engage actuellement pour la cybersécurité à travers toute une série d'activités, par exemple à la normalisation ou à l'assistance technique aux pays en développement adaptée à leurs besoins spécifiques. Reconnaissant sa longue expérience, ses capacités et ses compétences techniques, les dirigeants et les gouvernements du monde entier ont désigné l'UIT comme seul coordonnateur pour la grande orientation C5 du SMSI "Etablir la confiance et la sécurité dans l'utilisation des TIC"[213]. Ainsi, les chefs d'Etat et d'autres dirigeants participant au SMSI, ainsi que des Etats Membres de l'UIT ont chargé l'Union de prendre des mesures concrètes en vue de limiter les menaces et les risques liés à la société de l'information. La Résolution 140 (Rév. Antalya 2006) de la Conférence de plénipotentiaires de l'UIT relative au rôle de l'UIT dans la mise en œuvre des résultats du Sommet mondial sur la société de l'information a chargé le Secrétaire général de l'UIT de prendre toutes les mesures nécessaires pour que l'UIT s'acquitte de son rôle.

En mai 2007, le Secrétaire général a lancé le Programme mondial cybersécurité (GCA), cadre dans lequel toutes les parties prenantes peuvent coordonner une réponse internationale aux menaces croissantes qui pèsent sur la cybersécurité. Le GCA est fondé sur la coopération internationale et cherche à mobiliser toutes les parties prenantes concernées dans un effort concerté pour établir la confiance et la sécurité dans la société de l'information. Très récemment, à la Conférence de plénipotentiaires de 2010, les Etats Membres ont confirmé les travaux de l'UIT dans ce domaine en consacrant le GCA comme cadre de coopération international (Résolution 130, Rév. Guadalajara, 2010). Cette Résolution charge le Secrétaire général de continuer à examiner et améliorer les progrès réalisés. En particulier, les Etats Membres ont noté le renforcement du rôle de l'UIT dans l'établissement de la confiance et de la sécurité dans l'utilisation des TIC, ainsi que l'initiative mondiale de

213 Agenda de Tunis.

l'Union prise en collaboration avec IMPACT (Partenariat international multilatéral contre les cybermenaces) et le Forum FIRST (Forum des équipes d'intervention et de sécurité en cas d'incident). Il a également été décidé dans le cadre de cette Résolution de continuer à donner un rang de priorité élevé aux travaux de l'UIT concernant la sécurité des réseaux d'information et de communication.

Le Programme mondial cybersécurité comporte sept buts stratégiques notamment:

a) élaborer des stratégies en vue d'établir une législation type en matière de cybercriminalité qui soit applicable à l'échelle mondiale et compatible avec les dispositions réglementaires en vigueur aux niveaux national et régional;

b) élaborer des stratégies mondiales en vue de créer des structures organisationnelles et des politiques appropriées aux niveaux national et régional dans le domaine de la cybercriminalité;

c) concevoir une stratégie en vue de mettre en place des critères de sécurité et des mécanismes d'accréditation minimaux et mondialement acceptés pour les applications et les systèmes matériels et logiciels;

d) élaborer des stratégies en vue de créer un cadre mondial de veille, d'alerte et d'intervention en cas d'incident qui garantisse la coordination transfrontière des initiatives existantes et des initiatives nouvelles;

e) concevoir des stratégies mondiales en vue de créer et d'entériner un système générique et universel d'identité numérique ainsi que les structures organisationnelles nécessaires pour faire en sorte que les justificatifs numériques soient reconnus au-delà des frontières géographiques;

f) mettre au point une stratégie mondiale visant à faciliter le renforcement des capacités humaines et institutionnelles pour perfectionner les connaissances et le savoir-faire à tous les niveaux et dans tous les domaines susmentionnés;

g) présenter des propositions relatives à un cadre pour une stratégie mondiale multi-parties prenantes de coopération, de dialogue et de coordination au niveau international dans tous les domaines susmentionnés.

Afin d'atteindre ces objectifs, le Programme mondial cybersécurité repose sur cinq grands axes.

1. Cadre juridique

La cybercriminalité organisée est en hausse car l'Internet s'est révélé être un secteur d'activité lucratif à faible risque, ce qui s'explique par le fait qu'il reste des lacunes dans les législations nationales et régionales d'où la difficulté de traquer efficacement les criminels. Selon cet axe du GCA, il s'agit d'élaborer des stratégies pour mettre en

place une législation type sur la cybercriminalité qui soit applicable dans le monde entier et compatible avec d'autres dispositions règlementaires. L'UIT, en s'appuyant sur ses diverses ressources en matière de législation sur la cybercriminalité, aide les Etats Membres à comprendre les aspects juridiques de la cybersécurité afin qu'ils harmonisent leurs cadres juridiques.

2. Mesures techniques et de procédure

Ces mesures visent à corriger les failles des produits logiciels, l'objectif étant de définir des mécanismes, des protocoles et des normes d'accréditation mondialement acceptés. L'UIT, et plus particulièrement le Secteur de la normalisation (UIT-T) et le Secteur des radiocommunications (UIT-R), occupent une position unique en ce qui concerne la normalisation des TIC et jouent également un rôle essentiel pour remédier aux failles de sécurité des protocoles. Afin d'identifier les cybermenaces et de définir les contre-mesures à prendre pour en atténuer les risques, l'UIT cherche à sécuriser les services de communication, à améliorer les spécifications de sécurité pour les communications mobiles de bout en bout et s'occupe des spécifications de sécurité pour les services sur le web et les protocoles d'application. Les groupes d'action et les commissions d'études de l'UIT, par exemple le Groupe d'action sur les réseaux intelligents récemment constitué, sont des mécanismes efficaces pour atteindre ces objectifs.

3. Structures organisationnelles

Le monde a pris conscience du fait que les systèmes de veille, d'alerte et d'intervention en cas d'incident jouent un rôle déterminant pour faire face à des cyberattaques, au même titre que la libre circulation des informations, la collaboration et la coordination au sein des structures organisationnelles de chaque pays et entre elles. L'objectif est donc de mettre en place des structures organisationnelles et des stratégies qui contribuent à prévenir et à détecter les attaques lancées contre des infrastructures de l'information essentielles et à réagir à de telles attaques. Dans cette optique, l'UIT travaille actuellement avec ses Etats Membres dans le but de déterminer leurs besoins spécifiques en matière de cybersécurité et de les aider à créer des équipes nationales d'intervention en cas d'incident informatique (CIRT). Dans le cadre de la collaboration avec le partenariat IMPACT (Partenariat international multilatéral contre les cybermenaces), le Centre d'alerte mondial (GRC) joue un rôle déterminant dans la réalisation des objectifs du GCA.

L'UIT et IMPACT ont officiellement conclu un mémorandum d'accord qui fait du siège moderne d'IMPACT à Cyberjaya (Malaisie) le siège physique du GCA. Cette collaboration fournit aux 192 Etats Membres de l'UIT les compétences techniques, les

moyens et les ressources dont ils ont besoin pour répondre de façon efficace aux cybermenaces les plus graves qui surgissent dans le monde. Du fait des synergies étroites qui existent entre les cinq axes de travail du GCA et les services et infrastructures fournis par IMPACT, ce Partenariat s'inscrit dans la logique du combat contre les cybermenaces. Près de 60 pays y ont déjà souscrit[214]. IMPACT fournit des ressources d'intervention en cas d'urgence pour faciliter l'identification des cybermenaces et le partage des ressources afin d'aider les Etats Membres[215]. Le Centre d'alerte mondial (GRC) est doté d'un centre de crise, d'équipements de communication et d'information très modernes, d'un centre de sécurité opérationnel parfaitement fonctionnel, sept jours sur sept, d'un centre de données sécurisé totalement redondant, d'installations pour les personnes travaillant en équipes, d'un centre de radiodiffusion sur place et d'une salle de projection pour les hautes personnalités. Le GRC joue donc un rôle déterminant dans la réalisation de l'objectif du GCA, à savoir mettre en place des mesures techniques pour lutter contre les nouvelles cybermenaces en constante évolution. Les deux grandes nouveautés du GRC sont le système NEWS (Network Early Warning System) et le système ESCAPE (Electronically Secure Collaboration Application Platform for Experts). Le programme NEWS aide les pays membres à identifier rapidement les cybermenaces et donne des indications essentielles sur les mesures à prendre pour en atténuer les effets. Le programme ESCAPE est l'un des outils et des systèmes spécialisés auquel les Etats Membres auront accès. ESCAPE est un outil électronique qui permet à des cyberexperts habilités de différents pays de regrouper leurs ressources et de collaborer à distance dans un environnement de confiance sécurisé. Le programme ESCAPE, qui permet de mobiliser à bref délai ressources et compétences de nombreux pays, aidera les différents pays et la communauté mondiale à réagir immédiatement aux cybermenaces, en particulier pendant les situations de crise.

Les objectifs et les ressources fournis dans le cadre de cette collaboration non seulement reprennent les cinq axes du GCA mais aussi s'inspirent des principes proposés pour la cyberpaix. Les ressources auxquelles les Etats Membres peuvent avoir accès dans le cadre d'IMPACT aideront chaque pays à protéger ses propres

---

214 "Partenariat international multilatéral contre les cybermenaces", Union internationale des télécommunications, www.itu.int/ITU-D/cyb/cybersecurity/impact.html.

215 Lettre d'information de l'UIT envoyée à tous les Etats Membres "Déploiement des capacités en matière dedcybersécurité - IMPACT Global Response Centre", www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf.

citoyens contre des cyberattaques, leur garantissant un accès permanent aux communications via Internet ou d'autres applications TIC. En rejoignant le partenariat IMPACT et en contribuant au partage des ressources et aux discussions avec les autres membres, chaque pays s'emploiera activement à mettre en œuvre le cinquième principe, à savoir l'engagement de collaborer dans un cadre international à la réalisation de la cyberpaix. Le Partenariat IMPACT offre également des bourses d'étude aux pays en développement membres qui remplissent les conditions requises. Ces bourses leur permettent d'assister à des cours de formation axés sur la constitution d'un pool de ressources et de connaissances que les stagiaires pourront ensuite mettre à profit avec d'autres pays pour renforcer les capacités et les compétences dans le domaine de la sécurité au niveau national. Ces bourses d'étude amélioreront aussi les moyens dont dispose chaque pays pour sécuriser ses propres ressources TIC et garantir l'accès de ces ressources à leurs citoyens.

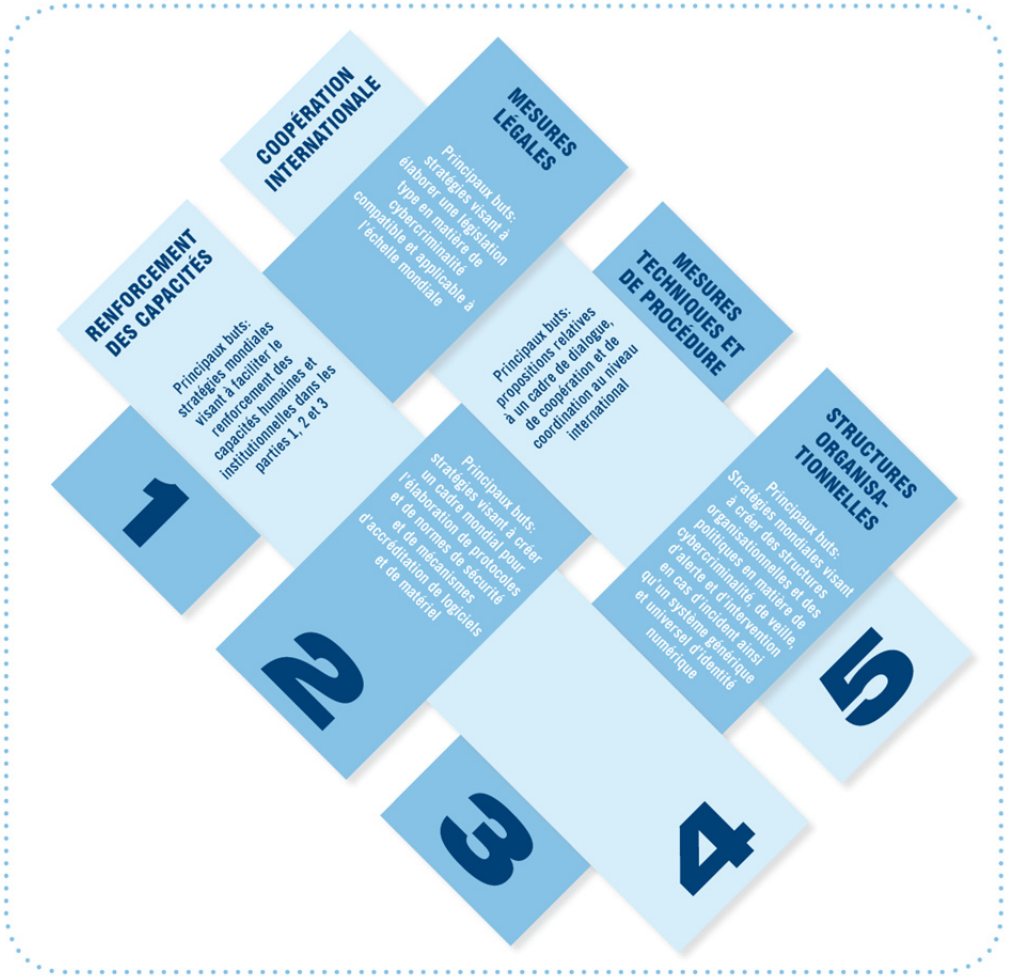
4. Renforcement des capacités

Cet axe de travail du GCA concerne l'élaboration de stratégies visant à enrichir les connaissances et les compétences techniques pour que le problème de la cybersécurité soit en bonne place dans l'agenda politique de chaque pays. Il faut encourager le renforcement des capacités afin de développer une culture de la cybersécurité durable et proactive. Saisir et bien comprendre les dangers qui peuvent exister dans le cyberespace est fondamental si l'on veut que les utilisateurs finals bénéficient des avantages des TIC en toute sécurité. Dans le droit fil de son mandat, qui consiste notamment à aider les Etats Membres à renforcer leurs capacités dans le domaine de la cybersécurité, l'UIT s'emploie à faciliter la mise en œuvre et la diffusion d'ouvrages sur les capacités de cybersécurité, par exemple le Guide UIT sur la cybersécurité, les ressources UIT dans le domaine de la cybercriminalité et le kit pratique d'atténuation des effets des réseaux zombies.

5. Coopération internationale

La cybersécurité ayant comme l'Internet une dimension mondiale, le cinquième axe du GCA concerne les stratégies de coopération, de dialogue et de coordination internationales. La collaboration avec IMPACT constitue un progrès important dans cette direction et fournit aux Etats Membres et à des tiers une instance où ils peuvent examiner les politiques et partager les informations. Le mandat qu'un grand nombre d'Etats Membres ont confié à l'UIT dans le cadre de la grande orientation C5 du SMSI est directement renforcé. La Déclaration de principes du SMSI dispose que renforcer le climat de confiance, notamment grâce à la sécurité de l'information et à la sécurité des réseaux, aux procédures d'authentification et à la protection de la vie privée et du consommateur est un préalable au développement de la société de l'information et à

l'établissement de la confiance parmi les utilisateurs des TIC. Une culture globale de la cybersécurité doit être encouragée, développée et mise en œuvre, en coopération avec tous les partenaires et tous les organismes internationaux compétents. La collaboration avec IMPACT ainsi que le RTI et les groupes d'action de l'UIT, renforcent les bases de cette confiance et contribuent à la réalisation de ces objectifs, grâce à l'adoption d'une approche globale et à l'existence d'un lieu où tous les membres de la communauté mondiale peuvent se réunir.



Programme mondial Cybersécurité: Dispositif en cinq parties

Conclusion

Les menaces liées au cyberdéveloppement et à la dépendance accrue vis-à-vis des TIC sont sérieuses mais leurs avantages potentiels sont beaucoup plus séduisants. Il est vrai que certains des risques d'une cyberguerre sont déjà devenus bien réels, mais nous avons aussi profité des avantages du cyberespace et, demain, les possibilités seront infinies. Au fur et à mesure que nous progressons, nous devons déterminer clairement comment nous pouvons continuer d'accroître dépendance, développement et intégration cybernétique tout en protégeant nos ressources, en créant un environnement stable propice à la poursuite du développement harmonieux des infrastructures et des nouvelles technologies et au maintien d'une paix durable. Les approches existantes, pour un grand nombre d'entre elles, sont positives mais elles restent insuffisantes et n'apportent pas nécessairement la meilleure solution. Si nous travaillons ensemble, nous avons toutes les chances d'atteindre ces objectifs et d'éviter la catastrophe que représente un cyberconflit. L'UIT œuvre déjà efficacement à la réalisation de cet objectif, de diverses manières, et mobilise ses ressources et son influence pour encourager l'appui et la participation multilatéraux nécessaires.

9 Déclaration d'Erice sur les principes régissant la cyberstabilité et la cyberpaix

Par World Federation of Scientists

Déclaration d'Erice sur les principes régissant la cyberstabilité et la cyberpaix

L'humanité, grâce à l'utilisation des technologies modernes de l'information et de la communication (TIC) a désormais les moyens de développer les ressources économiques dans l'intérêt de tous les pays, d'enrichir les capacités intellectuelles de leurs citoyens et de développer leur culture et leur confiance dans d'autres sociétés. C'est là une victoire sans précédent de la science. Internet, comme la science elle-même est, par essence, international et universel. Internet, et les outils d'information qui lui sont associés, représente le vecteur incontournable du discours scientifique aux niveaux national et mondial et permet à tous de bénéficier des avantages d'une science en libre accès, sans considération de confidentialité et de frontières

Au XXIème siècle, l'Internet et les autres réseaux interconnectés (cyberespace) sont devenus indispensables au bien-être de l'humanité ainsi qu'à l'indépendance politique et à l'intégrité territoriale des Etats.

Le monde est tellement interconnecté, les risques et les menaces sont si complexes et si diffus que le danger est de ne pas pouvoir maîtriser leur développement exponentiel compte tenu des moyens dont on dispose pour y faire face. Des Etats ou des personnes sans scrupules ont aujourd'hui la possibilité de désorganiser en profondeur la vie et la société dans tous les pays; la cybercriminalité – et son corollaire les cyberconflits – menacent l'existence pacifique de l'humanité et l'utilisation du cyberespace à des fins bénéfiques.

Les systèmes et réseaux d'information et de communication sont le fondement de la sécurité nationale et économique de tous les pays et constituent le système nerveux central pour les capacités d'intervention, les activités des secteurs privé et public, les services personnels, la santé publique et l'épanouissement personnel.

Les infrastructures et les systèmes d'information deviennent indispensables dans le domaine de la santé, de la sécurité et du bien-être de l'être humain, en particulier pour les personnes âgées, les personnes handicapées, les infirmes et les très jeunes enfants. Le chaos dans le cyberespace pourrait causer des souffrances et des destructions inutiles.

Les TIC concourent aux valeurs des droits de l'homme garantis en vertu du droit international, y compris la Déclaration universelle des droits de l'homme (Articles 12, 18 et 19) et la Charte internationale des droits civils et politiques (Articles 17, 18 et 19). Le chaos dans le cyberespace a) porte atteinte au droit de chaque individu, au respect de sa vie privée, de sa famille, de son foyer, et au droit de correspondance sans ingérence ni attaque, b) nuit au droit d'exercer la liberté de la pensée, de conscience et de religion, c) restreint le droit à la liberté d'opinion et d'expression et d) limite le droit de recevoir et de diffuser des informations et des idées à des médias, quels qu'ils soient, sans considération de frontières.

Les TIC peuvent être un bien ou un mal et donc être un instrument de paix ou de guerre. Tirer parti des avantages de l'ère de l'information suppose que les réseaux et les systèmes d'information soient stables, fiables, disponibles et dignes de confiance. Assurer l'intégrité, la sécurité et la stabilité du cyberespace en général nécessite l'adoption de mesures concertées au niveau international.

Nous nous prononçons donc en faveur des principes suivants pour parvenir à une cyberstabilité et cyberpaix durables:

1. Tous les gouvernements devraient reconnaitre que le droit international garantit aux individus la libre circulation de l'information et des idées; ces garanties s'appliquent également au cyberespace. Il ne devrait y avoir de restrictions que si cela est nécessaire et elles devraient être assorties d'un processus d'examen juridique.
2. Tous les pays devraient œuvrer ensemble à l'élaboration d'un code de cyberconduite commun et d'un cadre juridique mondial harmonisé, y compris des procédures d'assistance et de coopération en matière d'enquête, respectueuses de la vie privée et des droits de l'homme. Tous les gouvernements, les fournisseurs de services et les utilisateurs devraient appuyer les efforts déployés pour sanctionner les cybercriminels en vertu du droit international.
3. Tous les utilisateurs, les fournisseurs de services et les gouvernements devraient œuvrer pour faire en sorte qu'aucune utilisation du cyberespace ne donne lieu à l'exploitation des utilisateurs, en particulier des jeunes et des personnes sans défense, à travers des actes de violence ou des actes dégradants.
4. Les gouvernements, les organisations et le secteur privé, y compris les particuliers, devraient mettre en œuvre durablement des programmes de sécurité complets reposant sur de bonnes pratiques et des normes

internationalement reconnues et faisant appel à des technologies permettant de renforcer la protection de la vie privée et la sécurité.

5. Les concepteurs de logiciels et de matériels devraient s'efforcer de développer des technologies sûres, robustes et invulnérables.

6. Les gouvernements devraient activement participer aux efforts déployés par les Nations Unies en faveur de la cybersécurité et de la cyberpaix au niveau mondial et pour éviter de porter les conflits dans le cyberespace.

La Déclaration d'Erice sur les principes régissant la cyberstabilité et la cyberpaix a été élaborée par le Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists (WFS) à Genève et a été adoptée en plénière par la WFS à l'occasion de la 42ème session des séminaires internationaux sur les urgences planétaires à Erice (Sicile) le 20 août 2009.

10 Conclusion

Par Jody R. Westby

A ce jour, étonnamment, bien peu a été fait pour tenter de parvenir à la cyberpaix. Le Groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists a été le premier à parler de cyberpaix dans le cadre d'un programme décisif qu'il a présenté à l'Académie pontificale des sciences du Vatican en décembre 2008. Par la suite, le PMP a rédigé en 2009 la Déclaration d'Erice sur les principes régissant la cyberstabilité et la cyberpaix. Cette déclaration a été adoptée par la WFS et diffusée à chaque Etat Membre des Nations Unies. Les notions et les principes énoncés dans cette publication reflètent la constatation pessimiste du PMP selon laquelle le monde va droit au cyberchaos tandis que la quête de la cyberpaix entraînera un renforcement de la stabilité au niveau mondial.

Les statistiques et les scénarios qui sont présentés ici montrent qu'il est urgent de parvenir à une maîtrise des cyberdélits et des cyberconflits. L'Internet est le lieu par excellence pour comettre un délit car il est difficile d'établir l'identité de l'auteur d'un cyberdélit et il est rare que les cyberdélinquants se fassent prendre ou soient poursuivis. Il est à craindre aussi que l'Internet devienne l'arme par excellence. En pouvant accéder facilement aux données les plus sensibles et aux infrastructures essentielles, le plus petit des pays peut s'attaquer à des pays qui ont de très gros budgets de défense. Les pays en développement ont montré aux pays développés comment construire une infrastructure TIC de façon non linéaire en utilisant les technologies satellitaires et les technologies hertziennes. De même, les pays se rendent compte que les exploits dans le cyberespace constituent une option non linéaire intéressante pour promouvoir leurs intérêts nationaux et leurs intérêts de sécurité économique.

Pourquoi la maîtrise des cyberconflits ou la cyberpaix ne sont-elles pas à l'ordre du jour? Au lieu de cela, les dirigeants militaires dans le monde ne pensent qu'à annoncer la création de cybercommandements et leur intention de développer leurs capacités d'attaque, de défense ou d'exploitation des réseaux. Lorsque les pays se sont trouvés confrontés aux armes nucléaires, ils ont réclamé haut et fort une maîtrise et une non-prolifération des armes nucléaires. Les pays du monde entier ont fait front commun pour stopper un danger mondial qui menaçait l'humanité. Comme l'ont démontré les attaques qui ont frappé l'Estonie et la Géorgie, lorsqu'un pays victime est face aux insuffisances du cadre juridique international, aux incertitudes de la diplomatie, à des limites techniques et à l'impossibilité d'assurer la traçabilité des communications, la notion de cyberpaix devient séduisante.

S'il est vrai que de nombreuses organisations multinationales travaillent sur divers aspects de la cybercriminalité et/ou des cyberconflits, seule l'UIT a adopté un point de vue global et présenté un programme destiné à régler les grands problèmes tout en s'appuyant sur les efforts déployés par d'autres organisations. Il faut féliciter le Secrétaire général pour son leadership, sa vision et son courage pour aborder de front un problème d'une telle ampleur. Nous espérons sincèrement que d'autres organisations appuieront cette initiative et s'en inspireront et que les dirigeants s'attelleront à l'élaboration d'un code de conduite dans le cyberespace et d'un cadre juridique promouvant la géocyberstabilité.

Nous sommes à un moment crucial où le mauvais côté de l'Internet risque de faire oublier les énormes avantages des TIC et de bouleverser l'ordre mondial. Dès aujourd'hui, il faut œuvrer à la cyberpaix.

Contact:
Division de la stratégie institutionnelle
Union internationale des télécommunications
Place des Nations – 1211 Genève 20
Suisse
E-mail: strategy@itu.int
www.itu.int/cybersecurity

Imprimé en Suisse
Genève, janvier 2011