Déni de responsabilité

Les articles publiés dans le Forum du désarmement n'engagent que leurs auteurs.
Ils ne reflètent pas nécessairement les vues ou les opinions de l'Organisation des Nations Unies,
de l'UNIDIR, de son personnel ou des États ou institutions qui apportent leur concours à l'Institut.

Printed at United Nations, Geneva GE.07-01858—September 2007—4,440 UNIDIR/DF/2007/3 ISSN 1020-7287

TABLE DES MATIÈRES

NOTE DE LA RÉDACTRICE EN CHEF

Les technologies de l'information et de la communication sont imbriquées dans tous les aspects de nos vies : notre capacité à communiquer avec des internautes du monde entier en temps réel, les infrastructures qui fournissent nos foyers en électricité et nos bureaux en téléphonie, et les connexions de nos réseaux de défense et de sécurité nationale. Si la connectivité mondiale et le développement des technologies de l'information et de la communication ont eu des effets positifs indéniables, notre dépendance à l'égard de ces technologies et leur omniprésence ont créé de nouvelles faiblesses.

Le risque de voir des cyberguerres, le cyberterrorisme ou des attaques contre les infrastructures essentielles de l'information profiter de ces failles inquiète de plus en plus. Les différents acteurs engagés ou concernés par ces questions (qu'il s'agisse de gouvernements, du secteur privé, de particuliers, de criminels, et même de terroristes) ne sont pas vraiment d'accord sur la terminologie ou les définitions. À cela viennent s'ajouter les différences d'interprétations sur la question de savoir si le cadre juridique international existant convient face aux actes de guerre de l'information ou de cyberterrorisme. Un Groupe d'experts gouvernementaux des Nations Unies devrait se réunir en 2009 afin « de poursuivre l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des mesures de coopération qui pourraient être prises pour y parer » (résolution 60/45 de l'Assemblée générale) – poursuivant les efforts initiaux du Groupe d'experts gouvernementaux de 2005 chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale.

Ce numéro du *Forum du désarmement* se concentre sur les menaces civiles et militaires que représente l'utilisation des technologies de l'information et de la communication à des fins militaires, terroristes ou politiques contraires au maintien de la sécurité internationale et qui auraient des conséquences graves aux niveaux politique, social et économique. Afin d'encourager les débats, ce numéro présente une très large diversité de points de vue sur les questions de sécurité de l'information. Il évoque notamment les aspects juridiques du cyberespace et de la guerre de l'information s'agissant de la sécurité nationale et internationale ; le cyberespace et la gouvernance de l'Internet ; les risques qui pèsent sur les infrastructures essentielles de l'information ; et la façon qu'ont différentes instances régionales et internationales de traiter certains aspects de la sécurité de l'information.

Le prochain numéro du *Forum du désarmement* portera sur les questions de sécurité en Asie centrale. Après avoir été ignorée par beaucoup d'acteurs de la communauté internationale, l'Asie centrale se retrouve au cœur de nombreuses questions de sécurité et de développement. Si d'aucuns évoquent une reprise du Grand jeu, d'autres insistent sur les problèmes de sécurité très contemporains qui se posent à la région. Riche en ressources, l'Asie centrale est aussi une région d'États fragiles, de frontières contestées, de conflits autour des ressources et de menaces transrégionales.

Ce numéro consacré à l'Asie centrale examinera les intérêts régionaux en matière de sécurité, les problèmes de frontières et de ressources naturelles, les stocks d'armes légères, et les motifs d'instabilités internes et de conflit. Il étudiera les influences extérieures qui incitent les pays de l'Asie centrale à se faire concurrence ou à coopérer pour régler les problèmes de sécurité.

Du 17 mai au 4 juin 2007, l'équipe du projet sur « Le protocole pour l'évaluation des besoins de sécurité » s'est rendue au Ghana pour effectuer un essai préliminaire de techniques de génération de données, tester des idées de structure d'équipe sur le terrain et pour étudier divers aspects logistiques liés aux missions sur le terrain. Au Ghana, l'équipe du projet s'est entretenue avec du personnel des organismes des Nations Unies pour voir si, dans le cadre de leurs actions, ils évaluent (et si oui comment) la sécurité de la communauté (bénéficiaire). L'équipe est également allée dans la région nord du Ghana avec huit chercheurs locaux pour tester des techniques de génération de données envisagées pour le protocole pour l'évaluation des besoins de sécurité. L'objectif était d'étudier les pratiques, termes et concepts locaux concernant la sécurité dans un environnement d'après-conflit.

Les 4 et 5 juin 2007, l'UNIDIR, le Programme pour l'étude des organisations internationales et l'Appel de Genève ont organisé une conférence intitulée « Examen de critères et conditions pour encourager les acteurs non étatiques à respecter le droit humanitaire et le droit relatif aux droits de l'homme ». Les participants, qui représentaient des organismes des Nations Unies, le milieu universitaire et des ONG, se sont engagés dans des discussions très animées sur les questions juridiques liées à la participation des acteurs non étatiques dans les situations de conflit et d'après-conflit.

En janvier 2006, l'UNIDIR lançait un projet de recherche en plusieurs phases sur l'assistance internationale proposée aux États pour exécuter le Programme d'action des Nations Unies en vue de prévenir, combattre et éliminer le commerce illicite des armes légères. La première phase du projet a abouti à la publication d'un rapport qui fait le point sur l'assistance internationale au cours de la période 2001-2005. La deuxième phase comporte une série d'études de cas en Afrique de l'Est afin de créer un mécanisme qui favoriserait l'adéquation entre les ressources et les besoins. Le rapport sur ces études de cas est disponible sur le site web de l'UNIDIR (voir aussi, dans ce numéro, l'Actualité de l'UNIDIR, page 57).

Cette phase fut également l'occasion de concevoir un prototype pour un mécanisme en ligne qui permettra aux points de contact nationaux des pays concernés d'entrer leurs propres besoins d'assistance et aux donateurs et aux organismes d'exécution de repérer les possibilités de coopération dans des régions ou des zones thématiques précises. Le projet cherche à recueillir le plus de réactions possibles sur le prototype ainsi que des fonds pour la phase de développement.

Le Conseil consultatif du Secrétaire général pour les questions de désarmement, qui tient également lieu de Conseil d'administration de l'UNIDIR, s'est réuni à New York du 16 au 18 juillet 2007. C'était la première réunion du Conseil depuis la nomination du Secrétaire général Ban Ki-moon. Ce fut également l'occasion de saluer le nouveau Haut Représentant pour le désarmement, M. Sergio Duarte. Le Conseil consultatif s'est réuni sous la présidence avisée de l'Ambassadeur Lee Ho-jin de la République de Corée.

À l'occasion du dixième anniversaire de l'entrée en vigueur de la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction et de la création de l'Organisation pour l'interdiction des armes chimiques (OIAC), l'UNIDIR, l'OIAC, le Bureau des affaires de désarmement et les Conférences Pugwash sur la science et les problèmes internationaux ont organisé un séminaire à Genève, le 7 août 2007. Les participants ont retracé l'histoire des négociations de la Convention sur les armes chimiques, évoqué la pertinence de la Convention aujourd'hui et fait le point sur son application actuelle, en insistant tout particulièrement sur le régime de vérification. Une exposition présentant l'application de la Convention et l'action de l'OIAC était organisée en parallèle.

N'oubliez pas de consulter le blog du projet Disarmament Insight (voir l'Actualité de l'UNIDIR, page 57) – www.disarmamentinsight.blogspot.com.

Kerstin Vignard

COMMENTAIRE SPÉCIAL

Le siècle dernier a connu des avancées scientifiques et technologiques considérables. L'effet multiplicateur et les aspects positifs des inventions dans les domaines des technologies de l'information et de la communication sont de plus en plus évidents. Ces technologies facilitent la communication, ouvrent de nouveaux marchés, attirent les investissements et accélèrent le développement économique et social. À l'heure de la mondialisation, il est difficile d'imaginer un pays qui parvienne à la prospérité économique sans une infrastructure avancée de technologies de l'information et de la communication. La force de cette révolution repose sur le fait que ces technologies sont présentes dans tous les aspects de notre vie, qu'il s'agisse de la communication par e-mail ou par téléphone portable ou des systèmes de commandement et de contrôle des armées.

Ces technologies, qui offrent des avantages innombrables, peuvent aussi être utilisées à des fins malveillantes. Les questions de confidentialité, de cybercriminalité, de cyberterrorisme et d'utilisation des technologies de l'information à des fins militaires inquiètent de plus en plus.

Si la coopération et les discussions progressent au niveau international s'agissant des trois premiers sujets, la communauté internationale a plus de difficultés avec la question du lien entre la guerre et les technologies de l'information et de la communication. La révolution dans les affaires militaires repose sur les améliorations de ces technologies permettant aux forces militaires d'employer de nouvelles méthodes de commandement et de contrôle du personnel et de l'équipement aux niveaux stratégiques et tactiques. L'évolution des technologies de l'information et de la communication rend possible la mise au point de cyber-armes et les guerres électroniques. Cette évolution entraîne des changements dans la façon de mener une opération militaire et pourrait, par la suite, transformer le modèle de guerre classique, les batailles réelles entre belligérants étant remplacées par des attaques virtuelles ayant de graves conséquences dans la réalité. À mesure que les États découvrent les capacités – et les dangers – de la guerre de l'information, il n'est pas impossible qu'une course aux armements s'engage dans le cyberespace. Une telle course serait non seulement terriblement déstabilisante, mais confisquerait d'énormes ressources qui auraient pu être consacrées au développement durable et pacifique.

Une utilisation malveillante des technologies de l'information et de la communication représenterait des menaces universelles et transnationales qui toucheraient tous les aspects de l'existence des États, des sociétés, du secteur privé et des particuliers. Ce risque concerne toute l'humanité, mais deux grands problèmes empêchent toute coopération internationale dans ce domaine. Premièrement, il n'existe pas de définitions communément admises pour les expressions utilisées lors des débats, comme guerre de l'information, cybercriminalité, cyberterrorisme, armes de l'information, sécurité de l'information, pour n'en citer que quelques-unes. Deuxièmement, une question fondamentale se pose : le droit international actuel couvre-t-il correctement les aspects des technologies de l'information et de la communication ayant un rapport avec la sécurité ?

Il est de la responsabilité de la communauté internationale d'empêcher l'émergence de cette zone d'affrontement potentielle entre les États. Les Nations Unies ont relevé le défi en examinant, dans le cadre de l'Assemblée générale, la résolution annuelle sur « Les progrès de la téléinformatique dans le contexte de la sécurité internationale » introduite par la Fédération de Russie en 1998 (résolution 53/70 du 4 décembre 1998). La résolution fut adoptée par consensus chaque année jusqu'en 2005 ; au cours des deux dernières années, un État a voté contre.

La résolution souligne que la « téléinformatique risque d'être utilisée à des fins incompatibles avec le maintien de la stabilité et de la sécurité internationales » et de porter atteinte à l'intégrité de l'infrastructure des États, nuisant ainsi à leur sécurité dans les domaines tant civils que militaires. La résolution note également la nécessité de « prévenir l'utilisation illégale de la téléinformatique ou son emploi à des fins criminelles ou terroristes ».

La résolution demande aux États de collaborer à l'examen des dangers réels et des risques dans le domaine de la sécurité de l'information. Elle encourage aussi les mesures de coopération pouvant être prises pour parer à ces menaces et les principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux.

Le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, qui s'est réuni en 2004 et 2005, fut l'un des premiers à décrire l'ensemble des questions de sécurité de l'information qui sont d'une importance cruciale pour la communauté internationale.

L'intérêt pour cette question fut confirmé par la résolution 60/45, qui recommande la création en 2009 d'un groupe d'experts gouvernementaux pour « poursuivre l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des mesures de coopération qui pourraient être prises pour y parer », ainsi que l'étude des principes susceptibles de renforcer la sécurité des systèmes mondiaux dans le domaine de la téléinformatique.

J'apprécie profondément l'action de l'UNIDIR qui cherche constamment à favoriser les discussions et l'examen, au niveau international, des questions de désarmement. L'UNIDIR s'intéresse depuis longtemps à la sécurité des technologies de l'information et de la communication notamment depuis que l'Institut a organisé, en août 1999 à Genève, une rencontre internationale d'experts sur les progrès de la téléinformatique dans le contexte de la sécurité internationale. Cette occasion permit une meilleure compréhension des questions de sécurité internationale de l'information et des concepts connexes.

Je ne peux que me féliciter de la sortie de ce numéro du *Forum du désarmement* consacré à la question de la sécurité de l'information. Il sera particulièrement utile aux diplomates, aux scientifiques, aux entreprises, à la société civile et aux organisations internationales, ainsi qu'au Groupe d'experts gouvernementaux sur la sécurité de l'information au niveau international.

Andrey Krutskikh

Président, Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, 2004-2005

La sécurité de l'information au niveau international : description et aspects juridiques

A. A. Streltsov

Les technologies de l'information et de la communication, qui ont beaucoup progressé et sont largement utilisées dans tous les domaines de l'activité humaine, ont accéléré le développement post-industriel et l'apparition d'une société globale de l'information. Elles représentent aujourd'hui un facteur majeur de développement social. Les infrastructures mondiales de l'information ouvrent aux gens des possibilités sans précédent pour la communication, la socialisation et l'accès à l'information. Les particuliers, la société et l'État comptent sur la stabilité et la fiabilité des infrastructures de l'information.

Les technologies de l'information et de la communication pourraient toutefois représenter un moyen efficace, radicalement nouveau, pour perturber ou détruire l'industrie d'un pays, son économie, ses infrastructures sociales et l'administration publique. Elles pourraient devenir un moyen de combat capable d'atteindre des objectifs liés à la confrontation entre États aux niveaux tactique, opérationnel et stratégique[1]. Les technologies de l'information et de la communication acquièrent ainsi les caractéristiques d'une arme « destinée à vaincre l'ennemi dans un combat »[2]. Le pouvoir destructeur potentiel des armes dites de l'information va croître à mesure que les technologies de l'information et de la communication se développeront et que les infrastructures de l'information des sociétés évolueront. Les armes et l'équipement militaire étant de plus en plus associés aux technologies de l'information et de la communication, dont ils dépendront toujours plus, le pouvoir des armes dites de l'information s'en trouvera accru.

Ces préoccupations ne sont pas nouvelles et ne concernent pas un seul pays ni une seule région. Par exemple, la nécessité d'encourager les utilisations avantageuses des technologies de l'information et de la communication et de limiter les conséquences négatives fut exprimée, en 1998, par les Présidents de la Fédération de Russie et des États-Unis, dans la Déclaration conjointe sur les problèmes communs de sécurité au seuil du XXIe siècle, qui soulignait l'importance « de renforcer les aspects positifs et de réduire les effets négatifs de la révolution actuelle de la technologie de l'information — tâche capitale pour garantir dans l'avenir les intérêts de nos deux pays en matière de sécurité stratégique »[3].

Les premières initiatives internationales

Préoccupée par l'apparition de nouvelles menaces contre la paix et la sécurité, la Fédération de Russie défend, depuis près de dix ans au niveau international, la question de la sécurité de l'information. Le

A. A. Streltsov est docteur en ingénierie, docteur en droit, professeur, membre correspondant de l'Académie de cryptographie de la Fédération de Russie, expert des questions de sécurité de l'information. Il était membre de la délégation russe participant aux rencontres du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (2004-2005).

23 septembre 1998, le Ministre des affaires étrangères de la Fédération de Russie, I. S. Ivanov, soumit au Secrétaire général de l'ONU une lettre demandant la distribution d'un projet de résolution sur la sécurité de l'information. Une résolution intitulée « Les progrès de la téléinformatique dans le contexte de la sécurité internationale » fut ensuite adoptée par consensus lors de la cinquante-troisième session de l'Assemblée générale[4].

La résolution demandait aux États Membres de collaborer à l'examen, au niveau multilatéral, des dangers réels et des risques dans le domaine de la sécurité de l'information. Elle invitait aussi tous les États Membres à communiquer au Secrétaire général leurs vues et observations sur les questions suivantes :

- les problèmes généraux en matière de sécurité de l'information ;
- la définition des concepts fondamentaux en matière de sécurité de l'information, notamment les interférences illicites dans les systèmes télématiques ou l'utilisation illégale de ces systèmes ;
- et l'opportunité d'élaborer des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux et d'aider à combattre le terrorisme et la criminalité dans le domaine de l'information ;

Le Secrétaire général était prié de présenter un rapport à la cinquante-quatrième session de l'Assemblée générale.

Le Rapport du Secrétaire général reconnaissait que la sécurité de l'information au niveau international était un problème complexe qui revêtait de multiples aspects[5]. Fondé sur les réponses de l'Arabie saoudite, de l'Australie, du Bélarus, du Brunéi Darussalam, de Cuba, des États-Unis, de la Fédération de Russie, d'Oman, du Qatar et du Royaume-Uni, le rapport montrait les différentes priorités accordées par les États aux divers aspects de la question ainsi que les différentes initiatives prises au niveau national et, plus particulièrement, au niveau international.

Suite à cette première analyse des différentes positions, la Fédération de Russie proposa un nouveau projet de résolution à la cinquante-quatrième session de l'Assemblée générale[6], qui, pour la première fois, mettait directement l'accent sur le *potentiel militaire* des technologies de l'information et de la communication. Cette résolution fut adoptée sans être mise aux voix, le 1er décembre 1999.

En mai 2000, souhaitant faire progresser les débats sur la question, la Fédération de Russie soumit au Secrétariat de l'ONU un projet d'ensemble de principes concernant la sécurité de l'information au niveau international. Ces différents documents facilitèrent l'adoption, lors de la cinquante-cinquième session de l'Assemblée générale, d'une résolution notant l'intérêt d'une étude portant sur les « principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux »[7].

En 2001, les États Membres de l'ONU convinrent de créer un Groupe d'experts gouvernementaux, qui débuterait ses travaux en 2004 et serait chargé d'examiner les menaces qui existent ou pourraient exister dans le domaine de la sécurité de l'information au niveau international et des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux[8]. Une décision politique était ainsi prise, pour la première fois au niveau international, de passer de l'examen de la question à une action concrète.

En avril 2003, la Fédération de Russie remit au Secrétariat de l'ONU une nouvelle réponse intitulée « Questions liées aux travaux du Groupe d'experts gouvernementaux sur le problème de la sécurité de l'information » ; elle contenait la vision russe sur les questions de fond et sur les aspects organisationnels et pratiques des travaux du Groupe[9]. Elle précise, entre autres, qu'il conviendrait d'élaborer un instrument multilatéral mutuellement acceptable visant à renforcer le caractère universel d'un régime de sécurité de l'information au niveau international.

Le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale se réunit en 2004 et en 2005 ; il devait préparer un projet de rapport pour le Secrétaire général de l'ONU. Malgré l'ampleur des travaux menés, le Groupe ne parvint pas à un consensus sur un projet de rapport. La principale pierre d'achoppement était la question de savoir si le droit international humanitaire et le droit international réglementaient suffisamment les questions de sécurité dans le cadre des relations internationales en cas d'utilisation « hostile » des technologies de l'information et de la communication à des fins politico-militaires.

Les travaux du Groupe d'experts gouvernementaux ne furent toutefois pas vains ; ils permirent d'accroître l'importance accordée à ces questions au niveau international. Les échanges préliminaires entre les États sur les aspects les plus complexes de ces questions furent particulièrement fructueux. L'Assemblée générale des Nations Unies a décidé de continuer à étudier ce problème ce qui atteste de l'importance accordée à ces sujets[10]. Un nouveau groupe d'experts gouvernementaux doit débuter ses travaux en 2009.

Au cours des dix dernières années, différents aspects de la sécurité de l'information ont été examinés dans d'autres instances internationales et régionales, comme l'Union internationale des télécommunications, le Sommet mondial sur la société de l'information et le Conseil de l'Europe. Outre les résolutions mentionnées ci-dessus, l'Assemblée générale a examiné d'autres aspects de la question des technologies de l'information et de la communication, comme la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles[11].

La sécurité de l'information au niveau international

Avant d'examiner la question de savoir si les normes existantes du droit international sont suffisantes pour traiter les cas d'utilisation des technologies de l'information et de la communication à des fins hostiles, il convient de préciser de quoi il s'agit.

La sécurité de l'information concerne le risque de voir un État utiliser les technologies de l'information et de la communication pour influencer ou attaquer les technologies d'un autre État. L'utilisation des technologies de l'information et de la communication à des fins hostiles peut conduire à des situations constituant une menace pour la paix et la sécurité internationales[12]. Il convient d'examiner plus particulièrement les trois types d'actions décrits brièvement ci-dessous.

Les actes visant à affecter ou endommager les ressources informationnelles et les systèmes de télécommunications d'un autre État en utilisant des technologies de l'information et de la communication

Il s'agit :

- de moyens radioélectriques ou énergo-informationnels utilisant des impulsions électroniques pour neutraliser, provisoirement ou de manière définitive, les moyens et systèmes radioélectroniques ;
- de moyens permettant de neutraliser ou modifier l'algorithme de travail des programmes des technologies de l'information et de la communication ;
- de moyens d'agir afin d'interrompre ou désorganiser les flux d'information ou de communication en altérant la diffusion des signaux ;
- de moyens de désinformation ou la création, dans le domaine de la communication, d'une image virtuelle distincte de la réalité ou la déformant ;

- ou de moyens agissant sur les individus en vue de les désorienter ou de réprimer leur volonté ou visant à provoquer, dans la population, une déstabilisation temporaire.

L'utilisation délibérée de l'information afin d'affecter les structures de base d'un autre État

Il serait extrêmement dangereux d'utiliser les technologies de l'information et de la communication comme armes contre les installations, systèmes et institutions militaires et civils des États, et toute entrave à leur fonctionnement normal pourrait constituer une menace directe à la sécurité nationale.

Les intrusions dans les systèmes de gestion de la distribution d'énergie, par exemple, peuvent provoquer une paralysie complète de l'infrastructure d'un pays. Imaginez les effets écologiques catastrophiques d'une attaque contre une installation chimique, biologique ou énergétique, ou les conséquences catastrophiques d'une attaque impliquant une centrale nucléaire.

Les secteurs financier et bancaire sont également très exposés. Les transferts de fonds illégaux ou le pillage direct des ressources bancaires, l'« annulation » de comptes et le blocage, par des « attaques électroniques » des réseaux informatiques des banques centrales, peuvent, de toute évidence, non seulement créer des situations de crise dans ce domaine précis mais également entraîner l'effondrement de l'économie d'un pays et, partant, compromettre ses relations avec les autres pays.

La destruction de l'infrastructure des télécommunications au moyen de technologies de l'information et de la communication signifierait une paralysie des structures administratives et des organes décisionnels.

Toute attaque dans le domaine de l'information visant des systèmes de communication et de contrôle des systèmes de défense antiaérienne et antimissile et autres systèmes de défense désarmerait l'État face à un agresseur potentiel et l'empêcherait d'utiliser des moyens légaux à des fins de légitime défense.

Viser les moyens de communication, de contrôle et de transport des équipes d'intervention d'urgence peut accroître les dégâts matériels et les pertes en vies humaines dans les situations de catastrophes naturelles ou provoquées par l'homme.

Les bases de données et autres ressources informationnelles des organes chargés d'assurer le respect des lois peuvent subir des altérations ou être complètement détruites, entravant considérablement l'administration de la justice et la lutte effective contre la criminalité et compromettant le maintien de la légalité et de l'ordre.

Les actes visant à saper les systèmes politique, économique et social d'un autre État et à manipuler psychologiquement la population afin de déstabiliser la société

L'utilisation délibérée de l'information contre un adversaire n'est pas un procédé très nouveau. Mais aujourd'hui, du fait de la très vaste diffusion des nouvelles technologies dans le domaine des télécommunications, ce moyen d'action acquiert un potentiel qualitativement différent. En raison de la possibilité de lancer des actions massives, les technologies de l'information et de la communication pourraient devenir un instrument majeur de conflit entre États. Comme précisé dans la réponse du Gouvernement de la Fédération de Russie au Rapport du Secrétaire général de 2001 intitulé *Les progrès de la téléinformatique dans le contexte de la sécurité internationale* :

En raison de la possibilité de lancer des actions massives, les technologies de l'information et de la communication pourraient devenir un instrument majeur de conflit entre États.

La forte pression résultant de la prédominance d'un nombre limité de sources d'information peut servir à exercer une action psychologique négative sur la population d'un pays, sur le personnel des structures d'importance cruciale, les institutions administratives et gouvernementales et les organes législatifs.

La suggestion d'une incapacité de régler ses propres problèmes, d'une méfiance à l'égard des organes du pouvoir et d'un état de désespoir, la neutralisation de la volonté et la provocation de conflits pour des motifs religieux, ethniques ou d'autres raisons d'ordre social sapent les fondements de l'État et déstabilisent la société. Somme toute, une telle situation peut entraîner une stratification antagonique des groupes sociaux, déclencher une guerre civile ou aboutir à une désintégration complète de l'État[13].

La guerre de l'information et le droit international

Il ne fait aucun doute que les armes de l'information peuvent être réellement utilisées. Certaines forces armées préparent déjà des unités spéciales à des opérations militaires reposant sur les technologies de l'information et de la communication. L'armée de l'air des États-Unis, par exemple, n'a pas dissimulé ses projets ; elle se prépare à mettre sur pied un commandement spécial (Air Force Cyberspace Command)[14].

La communauté internationale prendra d'autres actions face à la menace d'utilisation des technologies de l'information et de la communication à des fins hostiles selon que le droit international actuel sera jugé suffisant ou non pour garantir la sécurité de l'information au niveau international. Ce fut confirmé, en 2004, lors d'une conférence internationale d'experts sur les attaques de réseaux informatiques et l'applicabilité du droit international humanitaire[15], et lors des discussions du Groupe d'experts gouvernementaux des Nations Unies en 2004 et 2005.

La sécurité de l'information au niveau international devrait reposer sur le droit international existant (*jus ad bellum*), qui définit comment contrer les menaces contre la paix et la sécurité internationales, et sur le droit international humanitaire (*jus in bello*), qui porte sur les méthodes et les moyens de guerre, la protection des États qui ne sont pas parties au conflit, ainsi que sur les personnes et biens qui sont ou pourraient être touchés par le conflit.

Les initiatives de la communauté internationale visant à clarifier ce sujet complexe ne devraient pas entamer le droit légitime des États de recourir à la légitime défense face à une utilisation hostile des technologies de l'information et de la communication, tout comme ils ont le droit de riposter à une attaque d'armes classiques.

La Charte des Nations Unies

La Charte des Nations Unies est la pierre angulaire du droit international s'agissant du maintien de la paix et la sécurité internationales. Elle stipule, entre autres, que :

- Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies. (Art. 2 al. 4) ;
- Le Conseil de sécurité constate l'existence d'une menace contre la paix, d'une rupture de la paix ou d'un acte d'agression et fait des recommandations ou décide quelles mesures seront prises conformément aux Articles 41 et 42 pour maintenir ou rétablir la paix et la sécurité internationales (Art. 39) ;

- Le Conseil de sécurité peut décider quelles mesures n'impliquant pas l'emploi de la force armée doivent être prises pour donner effet à ses décisions, et peut inviter les Membres des Nations Unies à appliquer ces mesures (Art. 41) ;
- Si le Conseil de sécurité estime que les mesures prévues à l'Article 41 seraient inadéquates ou qu'elles se sont révélées telles, il peut entreprendre, au moyen de forces aériennes, navales ou terrestres, toute action qu'il juge nécessaire au maintien ou au rétablissement de la paix et de la sécurité internationales (Art. 42) ;
- Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales (Art. 51).

L'ensemble des spécialistes du droit international reconnaissent que ces règles instaurent un mécanisme universel pour préserver la paix et la sécurité internationales. Alors que les technologies de l'information et de la communication sont désormais conçues ou employées comme moyens de destruction (autrement dit les « armes de l'information ») et que la communauté internationale n'a pas encore convenu de la place de la sécurité de l'information dans le droit international existant, la Charte des Nations Unies pourrait être interprétée de façon à laisser aux acteurs internationaux une liberté importante d'utiliser les technologies de l'information et de la communication pour mener des actions agressives et régler des conflits et différends internationaux[16].

Cette situation surprenante découle du fait que les actions hostiles dans le domaine de l'information ne sont pas encore envisagées explicitement par le droit international sur le même plan que des actions hostiles avec des armements classiques – même si l'interconnectivité du monde d'aujourd'hui et sa dépendance à l'égard des technologies de l'information et de la communication signifient qu'une telle attaque serait aussi dévastatrice qu'une attaque classique, voire peut-être même plus. Les difficultés sont exacerbées par l'absence d'interprétations communément admises de notions telles que l'« acte d'agression » (Art. 1), la « force » (Art. 2 al. 4) et l'« agression armée » (Art. 51) s'agissant de la sécurité de l'information.

Les attaques informationnelles comme actes d'agression

La résolution 3314 (XXIX) de l'Assemblée générale, en date du 14 décembre 1974, définit l'acte d'agression[17]. L'article 3 de l'Annexe à la résolution stipule que :

> L'un quelconque des actes ci-après, qu'il y ait eu ou non déclaration de guerre, réunit, sous réserve des dispositions de l'article 2 et en conformité avec elles, les conditions d'un acte d'agression :
>
> *a*) L'invasion ou l'attaque du territoire d'un État par les forces armées d'un autre État, ou toute occupation militaire, même temporaire, résultant d'une telle invasion ou d'une telle attaque, ou toute annexion par l'emploi de la force du territoire ou d'une partie du territoire d'un autre État ;
>
> *b*) Le bombardement, par les forces armées d'un État, du territoire d'un autre État, ou l'emploi de toutes armes par un État contre le territoire d'un autre État ;
>
> *c*) Le blocus des ports ou des côtes d'un État par les forces armées d'un autre État ;
>
> *d*) L'attaque par les forces armées d'un État contre les forces armées terrestres, navales ou aériennes, ou la marine et l'aviation civiles d'un autre État ;
>
> *e*) L'utilisation des forces armées d'un État qui sont stationnées sur le territoire d'un autre État avec l'accord de l'État d'accueil, contrairement aux conditions prévues dans l'accord ou

toute prolongation de leur présence sur le territoire en question au-delà de la terminaison de l'accord ;

f) Le fait pour un État d'admettre que son territoire, qu'il a mis à la disposition d'un autre État, soit utilisé par ce dernier pour perpétrer un acte d'agression contre un État tiers ;

g) L'envoi par un État ou en son nom de bandes ou de groupes armés, de forces irrégulières ou de mercenaires qui se livrent à des actes de force armée contre un autre État d'une gravité telle qu'ils équivalent aux actes énumérés ci-dessus, ou le fait de s'engager d'une manière substantielle dans une telle action.

Même si cette résolution n'a pas été adoptée par consensus, ses dispositions indicatives donnent au Conseil de sécurité de l'ONU et à tous les membres de la communauté internationale des critères pour déterminer un acte d'agression.

L'utilisation d'une arme de l'information peut être interprétée comme un acte d'agression si l'État victime a des raisons de penser que l'attaque a été menée par les forces armées d'un autre État et visait à perturber le fonctionnement d'installations militaires, à détruire des capacités de défense ou économiques, ou à violer la souveraineté de l'État sur un territoire particulier.

La question du territoire

Conformément à l'article 41 de la Charte des Nations Unies, le Conseil de sécurité peut décider des mesures pouvant être prises pour donner effet à ses décisions et notamment « l'interruption complète ou partielle des relations économiques et des communications ferroviaires, maritimes, aériennes, postales, télégraphiques, radioélectriques et des autres moyens de communication », autrement dit un blocus. Dans son acception classique, un blocus s'applique aux frontières d'un État alors qu'un blocus de l'information pourrait pénétrer sur le territoire d'un État et toucher la totalité des foyers, des bureaux, des institutions ou des sociétés.

Un blocus cybernétique pourrait être perçu comme une ingérence dans les affaires intérieures d'un État, une violation de sa souveraineté voire comme une saisie partielle de son territoire national, autant d'actions qui violent cette norme internationale. La situation devient absurde si les forces armées d'un État prennent des mesures pour imposer et maintenir un « blocus de l'information ». Dans ce cas, l'État attaqué pourrait invoquer son droit naturel de légitime défense, individuelle ou collective, qui implique le recours à la force militaire et l'emploi d'armes classiques.

L'absence de définition précise de la notion de « territoire » s'agissant du cyberespace vient s'ajouter aux lacunes du droit sur la sécurité internationale. L'alinéa 4 de l'article 2 de la Charte des Nations Unies oblige les Membres de l'Organisation à s'abstenir de recourir à la menace ou à l'emploi de la force contre l'intégrité territoriale d'un autre État. Cela implique qu'un territoire sous la juridiction d'un État doit être séparé des autres États par une frontière officielle. Il n'existe toutefois pas dans le domaine de l'information de concepts comme le territoire et les frontières nationales. Un État pourrait considérer l'ensemble (ou une partie) des infrastructures mondiales de l'information comme étant son territoire, revendiquer sa compétence pour des éléments pertinents et, sur cette base, prendre des mesures pour les défendre.

Identifier l'agresseur

Une autre difficulté se pose : comment identifier avec certitude l'agent qui lance une attaque informationnelle. D'un point de vue technique, il est difficile de localiser d'où provient une attaque de ce type. Même si l'on parvient à localiser dans un pays l'origine d'une attaque, il est difficile

de déterminer si l'agresseur a agi à titre individuel ou au nom d'une organisation criminelle, du Gouvernement ou des forces armées. Dans de tels cas, l'auteur présumé d'un acte agressif peut être accusé à tort et non pas identifié de manière certaine, comme l'ont montré les événements récents.

La protection des installations des infrastructures essentielles

Le droit international ne couvre pas expressément l'utilisation des technologies de l'information et de la communication comme moyen de pression coercitif sur un État ennemi.

Selon les lois et coutumes de la guerre sur terre établies par la Convention de La Haye du 18 octobre 1907, « Il est interdit d'attaquer ou de bombarder, par quelque moyen que ce soit, des villes, villages, habitations ou bâtiments qui ne sont pas défendus »[18]. Les États parties sont, en outre, tenus de prendre « toutes les mesures nécessaires [...] pour épargner, autant que possible, les édifices consacrés aux cultes, aux arts, aux sciences et à la bienfaisance, les monuments historiques, les hôpitaux et les lieux de rassemblement de malades et de blessés, à condition qu'ils ne soient pas employés en même temps à un but militaire »[19]. Ces règles permettent de lutter contre les maux superflus des populations civiles et des blessés lors d'opérations militaires.

Pour pouvoir appliquer ces dispositions au cyberespace, il faudrait impérativement « marquer » d'une certaine manière les systèmes d'information qui assurent la viabilité des installations des infrastructures sociales essentielles : qu'il s'agisse d'installations individuelles (et notamment des hôpitaux civils ou militaires, des abris, etc.) ou d'installations concernant des régions entières (alimentation en eau, réseaux électriques, barrages, etc.). Dans le monde réel, certaines de ces installations (comme les hôpitaux) peuvent être identifiées par un signe distinctif – une croix rouge ou un croissant rouge – qui indique leur statut protégé. Il n'existe pas dans le cyberespace de tels signes ni de critères pour désigner ces systèmes comme des infrastructures essentielles.

La perfidie

S'agissant de la guerre de l'information, empêcher la perfidie est l'un des problèmes les plus urgents qui se pose en droit international humanitaire.

Conformément à l'article 23 de la Convention de La Haye, les belligérants n'ont pas le droit « de tuer ou de blesser par trahison des individus appartenant à la nation ou à l'armée ennemie ». L'esprit de chevalerie devrait persister dans les relations entre belligérants même lors des hostilités. L'interdiction de tuer ou blesser l'ennemi en violant cette promesse est l'essence même de cette règle de droit.

Il semblerait raisonnable d'avoir les mêmes attentes à l'égard des parties à un conflit interétatique qui lancent des attaques avec les technologies de l'information et de la communication sur les infrastructures civiles de l'information d'un autre État. Le matériel et les logiciels commerciaux utilisés dans les installations des infrastructures offrent une certaine garantie de qualité et de sécurité. La prise de « positions » anticipée dans les logiciels des systèmes des technologies de l'information et de la communication de la partie adverse faciliterait le lancement d'une attaque informationnelle. Il pourrait s'agir, par exemple, de programmes intégrés dans le logiciel sans que l'acheteur en soit informé ou sans son aval. Inclure, par exemple, un code malveillant dormant ou des « accès dérobés » à ces produits constitue un abus de confiance délibéré et une violation calculée de la confiance et pourrait être considéré comme une perfidie. Le droit international humanitaire interdit déjà la perfidie[20].

Suggestions finales

En conclusion, la communauté internationale doit développer plusieurs domaines qui, à terme, renforceraient la sécurité de l'information au niveau international. Il faudrait, sur le plan juridique :

- déterminer la licéité de l'utilisation des technologies de l'information et de la communication à des fins hostiles ;
- élaborer des normes régissant le fonctionnement, les moyens et l'utilisation des infrastructures mondiales de l'information ;
- renforcer les règles techniques dans le domaine de la sécurité de l'information et les procédures d'investigation pour identifier l'auteur d'une attaque informationnelle ;
- interdire l'utilisation des technologies de l'information et de la communication visant à endommager les installations des infrastructures essentielles ;
- instaurer un système de « cyber-identification » pour les installations des infrastructures essentielles ;
- réviser les règles des belligérants pour qu'elles tiennent compte des infrastructures mondiales de l'information et de leurs éléments situés dans des États neutres ;
- définir des mesures de confiance portant sur les logiciels disponibles dans le commerce ;
- et étendre l'interdiction de la perfidie aux technologies de l'information et de la communication disponibles dans le commerce.

Notes

1. Deirdre Collings et Rafal Rohozinski, *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations* (Workshop Report), United States Army War College 2006, p. 10.
2. Военный энциклопедический словарь [Encyclopédie militaire], Moscou, Военное издательство, 1983, p. 523.
3. Signée à Moscou, le 2 septembre 1998, traduction française tirée du document des Nations Unies A/53/371-S/1998/848.
4. Assemblée générale, Les progrès de la téléinformatique dans le contexte de la sécurité internationale, document des Nations Unies A/RES/53/70, 4 janvier 1999.
5. Assemblée générale, Les progrès de la téléinformatique dans le contexte de la sécurité internationale, Rapport du Secrétaire général, document des Nations Unies A/54/213, 10 août 1999.
6. Assemblée générale, Les progrès de la téléinformatique dans le contexte de la sécurité internationale, document des Nations Unies A/RES/54/49, 23 décembre 1999.
7. Assemblée générale, Les progrès de la téléinformatique dans le contexte de la sécurité internationale, document des Nations Unies A/RES/56/19, 7 janvier 2002.
8. Ibid.
9. Cette réponse intitulée « Questions liées aux travaux du Groupe d'experts gouvernementaux sur le problème de la sécurité de l'information » figure dans le document de l'Assemblée générale, *Les progrès de la téléinformatique dans le contexte de la sécurité internationale. Rapport du Secrétaire général*, document des Nations Unies A/58/373, 17 septembre 2003, page 9.
10. Assemblée générale, Les progrès de l'informatique et de la télématique et la question de la sécurité internationale, document des Nations Unies A/RES/61/54, 19 décembre 2006.
11. Voir, par exemple, Assemblée générale, Création d'une culture mondiale de la cybersécurité, document des Nations Unies A/RES/57/239, 31 janvier 2003 ; et Assemblée générale, Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information, document des Nations Unies A/RES/58/199, 30 janvier 2004.
12. Cette partie se fonde sur la réponse du Gouvernement de la Fédération de Russie au Rapport du Secrétaire général sur les progrès de la téléinformatique dans le contexte de la sécurité internationale. Voir Assemblée générale, *Les progrès de la téléinformatique dans le contexte de la sécurité internationale, Rapport du Secrétaire général*, Additif, document des Nations Unies A/56/164/Add.1, 3 octobre 2001.
13. Ibid., Section 3, page 3.

14. Voir, par exemple, la déclaration de 2006 du Secrétaire de l'Armée de l'air, Michael W. Wynne, *Cyberspace as a Domain in which the Air Force Flies and Fights*, à l'adresse <www.af.mil/library/speeches/speech.asp?id=283>.
15. Karin Bystrom (sous la direction de), *Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, 17-19 novembre 2004, Stockholm, 2005.
16. Thomas C. Wingfield, *The Law of Information Conflict. National Security Law in Cyberspace*, Aegis Research Corporation, 2000.
17. Assemblée générale, Définition de l'agression, résolution 3314 (XXIX), 14 décembre 1974.
18. Lois et coutumes de la guerre sur terre (Convention IV de La Haye), 18 octobre 1907, art. 25.
19. Ibid., article 27.
20. Protocole additionnel I aux Conventions de Genève, art. 37.

Les infrastructures essentielles de l'information : failles, menaces et parades

Myriam Dunn Cavelty

La bataille cybernétique qui a opposé récemment l'Estonie et la Fédération de Russie a, de nouveau, attiré l'attention sur les questions de sécurité du cyberespace et de protection des infrastructures essentielles de l'information. Fin avril 2007, les autorités estoniennes voulurent retirer un mémorial de la deuxième guerre mondiale, une statut de bronze représentant un soldat soviétique, ce qui déclencha une bataille cybernétique de trois semaines au cours de laquelle des attaques par déni de service inondèrent plusieurs sites web parmi lesquels ceux du Parlement estonien, de banques, de ministères, de journaux et de services audiovisuels, paralysant les sites en saturant les capacités de leurs serveurs.

Cette altercation russo-estonienne en ligne fit les gros titres[1] et divers responsables se saisirent du thème de la cyberguerre, confirmant la tendance fréquente à dramatiser le thème de la cybersécurité[2]. D'aucuns affirmèrent, de manière explicite ou implicite, que la Fédération de Russie était derrière cette attaque et que c'était le premier cas connu d'un État visant un autre par une opération de cyberguerre[3]. Un fonctionnaire de l'Organisation du Traité de l'Atlantique Nord aurait déclaré : « Je ne désignerai personne, mais ces actes n'étaient pas l'œuvre de quelques individus. Ils représentaient clairement une opération concertée. Les Estoniens ne sont pas seuls concernés par ce problème. C'est une affaire grave pour l'ensemble de l'alliance »[4].

Une fois passée l'indignation soulevée par cette affaire, l'on peut observer les faits avec réalisme : il est aujourd'hui évident que les « attaques » n'avaient pas été lancées par le Gouvernement russe ni ses services de sécurité. De fausses adresses IP – en l'occurrence, celle d'un ordinateur du Gouvernement russe était impliquée dans l'attaque par déni de service – sont régulièrement utilisées dans les attaques lancées par des « hacktivistes »[5]. De plus, les attaques étant peu sophistiquées et utilisant de vieilles méthodes, elles étaient probablement lancées par un grand nombre de jeunes pirates informatiques appelés *script kiddies*. Ce sont des adolescents qui n'ont pas une compétence informatique réelle, mais qui se servent de programmes et techniques facilement disponibles pour déceler et exploiter les failles d'autres ordinateurs connectés à Internet. En fin de compte, malgré tout le bruit qu'elles firent, ces attaques n'eurent qu'un effet relativement négligeable (une caractéristique classique des attaques par déni de service).

De tels incidents doivent impérativement être considérés pour ce qu'ils sont, mais il ne faut pas, pour autant, rejeter les craintes de cyber-attaques au motif qu'elles sont exagérées. Ces craintes, liées au sentiment de très grande vulnérabilité des sociétés modernes, retiennent depuis longtemps déjà l'attention des experts des questions de sécurité. Cet article explique comment et pourquoi, au cours de la dernière décennie, les questions de cybersécurité ont parfois dominé le débat *politique* sur

---

Myriam Dunn Cavelty dirige le New Risks Research Unit au Centre pour les études de sécurité de l'ETH Zurich (Suisse) et coordonne le réseau Crisis and Risk Network, voir <www.crn.ethz.ch>.

la sécurité. Nous évoquerons les différentes menaces qui semblent peser sur les sociétés modernes interconnectées, les mettrons en perspective et nous intéresserons plus particulièrement aux obstacles et aux éléments sans lesquels il ne peut y avoir de mesures de protection aux niveaux national et international.

La protection des infrastructures essentielles de l'information, une priorité politique en matière de sécurité

Les plans de défense nationale incluent, depuis des décennies, des principes de protection pour les infrastructures et objets présentant une importance stratégique[6]. Le concept actuel de protection des infrastructures essentielles dépasse pourtant largement les considérations d'ordre militaire et les principes classiques de défense nationale. Il est aujourd'hui un point crucial du débat sur la sécurité nationale à cause de deux facteurs interdépendants qui se renforcent : la multiplication des menaces après la fin de la guerre froide, surtout s'agissant des acteurs malveillants et de leurs capacités ; et une nouvelle faiblesse de la société moderne qui dépend fortement de systèmes d'information peu sûrs.

Pendant la guerre froide, la sécurité nationale était principalement menacée par les intentions agressives d'États qui voulaient en dominer d'autres. La fin de la guerre froide mit un terme à ces menaces très claires : après la désintégration de l'Union soviétique, la plupart des pays durent tenir compte de « nouvelles » menaces dans leurs préoccupations en matière de sécurité[7]. Ces problèmes se caractérisent pas une très grande incertitude : « qui, quand, quoi, comment, où et pourquoi ? »[8]. Ils ne peuvent, de toute évidence, pas être considérés comme des « menaces » imminentes, directes et certaines, mais plutôt comme des « risques » qui, par définition, sont indirects, incertains et se situent dans l'avenir[9].

En raison de ces risques diffus et de la difficulté de localiser et identifier les ennemis, les politiques de sécurité ne se concentrent plus uniquement sur les acteurs, les capacités et les motivations mais étudient aussi les faiblesses de la société dans son ensemble. Au début des années 90, l'armée des États-Unis a joué un rôle déterminant dans l'apparition de cette nouvelle façon d'envisager les menaces. Comme il ne restait qu'une seule superpuissance, les États-Unis, ce pays semblait devoir être la cible de la guerre asymétrique. Les ennemis qui étaient quasiment sûrs d'échouer face à l'armée américaine pourraient tenter de faire plier le pays en frappant des cibles plus faciles qui jouent un rôle crucial dans le fonctionnement de la société : les infrastructures essentielles. Elles sont indispensables car leur paralysie ou leur destruction fragiliserait la sécurité nationale et compromettrait les intérêts économiques et sociaux d'un État. Il s'agit, par exemple, des infrastructures de télécommunications, des réseaux électriques, de transport et stockage du gaz et du pétrole, des services bancaires et financiers, des réseaux de transport, des systèmes d'approvisionnement en eau, des services d'aide médicale d'urgence et de la fonction publique.

La crainte que des actions asymétriques soient lancées contre de telles cibles est exacerbée par la révolution dite de l'information. Aujourd'hui, presque toutes ces infrastructures dépendent de systèmes de contrôle informatiques pour garantir, en permanence, la fiabilité de leur bon fonctionnement. Les technologies de l'information et de la communication sont, bien souvent, omniprésentes, elles relient les systèmes des infrastructures qui deviennent ainsi interdépendants. Les éléments des infrastructures de l'information qui sont indispensables pour assurer la continuité de leur fonctionnement sont appelés infrastructures essentielles de l'information. Elles font partie des infrastructures critiques d'un État et comprennent, entre autres, les ordinateurs, les logiciels, Internet, les satellites et les fibres optiques.

De par leur nature, les infrastructures essentielles de l'information sont généralement considérées comme peu sûres. La plupart des composants sont mis au point dans le secteur privé, où la pression de la concurrence oblige à réduire le délai de mise sur le marché et où la sécurité n'est pas une

préoccupation principale lors de la conception des systèmes. Les failles des ordinateurs et des réseaux sont donc inévitables et sont à l'origine d'instabilités et de points de défaillance graves des infrastructures de l'information[10]. De nombreux chercheurs s'accordent à dire que les infrastructures, en raison de leur complexité, sont leur propre ennemi[11]. L'utilisation croissante des technologies de l'information et de la communication et la multiplication des besoins fonctionnels entraînent un enchevêtrement des systèmes ; il est donc vain de chercher à préserver la séparation de systèmes ayant chacun un mode de responsabilité propre bien défini. La distinction entre l'intérieur et l'extérieur du système est confuse, tout comme la frontière entre les systèmes. L'attaque d'une infrastructure a un effet multiplicateur, même une attaque relativement petite peut produire un impact important[12]. Depuis la fin de la guerre froide, la diffusion des technologies de l'information et de la communication semble avoir facilité les menaces asymétriques en facilitant l'accès aux instruments pouvant servir à mener une attaque et en augmentant les probabilités de succès d'une attaque. Les frontières qui sont poreuses dans le monde réel n'existent tout simplement pas dans le cyberespace.

La menace qui pèse sur les infrastructures essentielles de l'information

Comme la plupart des infrastructures essentielles sont gérées, surveillées ou contrôlées par des systèmes vulnérables, les politiques de protection se sont concentrées, dans les années 90, sur les infrastructures de l'information[13]. Aujourd'hui, les infrastructures de l'information sont encore considérées comme un point d'entrée facile et vulnérable, mais il reste difficile d'identifier les menaces qui pèsent sur les infrastructures essentielles de l'information, leurs auteurs et la nature probable des attaques.

La gamme d'auteurs potentiels est très vaste, puisqu'il peut s'agir d'adolescents (les *script kiddies* évoqués plus haut), de pirates expérimentés utilisant des techniques sophistiquées, de criminels, de terroristes voire d'États. Il serait étrange de regrouper tous ces acteurs dans la même catégorie ; ils sont donc parfois séparés en deux groupes selon leur complexité organisationnelle, leurs motivations et leurs ressources, même si la frontière entre les deux catégories reste floue : le premier groupe représente une menace « non structurée » et le second une menace « structurée »[14].

La menace non structurée est aléatoire et relativement limitée. Il s'agit d'adversaires dont l'organisation et les fonds sont limités et qui ont des buts à court terme comme des pirates isolés ou de petits groupes de criminels organisés. Les ressources, instruments, compétences et fonds de ces acteurs sont trop limités pour qu'ils puissent lancer des attaques sophistiquées contre des infrastructures essentielles ; ce n'est d'ailleurs pas leur motivation. Ils agissent pour le plaisir des sensations fortes, le prestige ou pour l'argent. À l'inverse, les menaces organisées sont nettement plus méthodiques et mieux appuyées. Il s'agit, dans ce cas, d'acteurs bénéficiant d'importants moyens, d'un appui professionnel organisé et ayant accès à des produits de renseignement ; leurs objectifs s'inscrivent dans le long terme. Cette catégorie regroupe des services secrets, des terroristes bien organisés, des pirates informatiques professionnels impliqués dans la guerre de l'information, des groupes criminels plus importants et des espions industriels.

Malheureusement, la frontière entre les deux catégories n'est pas claire. Même si les menaces non structurées ne représentent généralement pas un problème direct pour la sécurité nationale, les acteurs de la catégorie des menaces structurées peuvent très bien se faire passer pour des acteurs de l'autre catégorie ou chercher à obtenir l'aide d'individus doués appartenant à cette catégorie. Les pirates informatiques ordinaires ne cherchent pas à provoquer la violence ni à engendrer des conséquences graves sur les plans économique ou social[15], mais il est à craindre qu'une personne ayant les capacités de provoquer des dégâts graves mais n'ayant pas de raison d'agir dans ce sens puisse être convaincue, par de grosses sommes d'argent, de fournir ses connaissances à des acteurs malveillants.

Les réseaux d'informations étant globalisés, des attaques peuvent être lancées depuis n'importe où ; il est donc très difficile de découvrir l'origine d'une attaque à condition déjà qu'elle ait été détectée. Le temps qui s'écoule entre le moment où un individu lance une action, l'intrusion elle-même et les effets de l'intrusion complique l'identification des acteurs impliqués. Des méthodes plus sophistiquées, en partie automatisées, permettent aujourd'hui de provoquer plus de dégâts avec une seule attaque. En outre, les technologies se développent extrêmement vite : le délai entre la découverte d'une faille d'un système et l'apparition d'un outil ou d'une technique permettant d'exploiter cette faille ne cesse de diminuer. En fait, la technologie utilisée dans de nombreuses attaques est très simple d'utilisation, peu coûteuse et largement disponible sur les forums et divers sites web, tout comme les outils de cryptage et d'anonymat. Les menaces cybernétiques tombent sans aucun doute dans la catégorie des « nouveaux » défis : elles sont indirectes et très incertaines.

Le cyberterrorisme est peu probable

Comme on pouvait s'y attendre, les attaques du 11 septembre 2001 ont exacerbé l'accent mis sur le terrorisme et le cyberterrorisme dans le débat sur la protection des infrastructures essentielles. Lorsqu'il s'agit d'évoquer des événements catastrophiques, les médias sont fascinés par le préfixe « cyber » et utilisent régulièrement des titres à sensation[16]. De leur côté, les experts et les responsables gouvernementaux mettent régulièrement en garde contre le cyberterrorisme qui menace la sécurité nationale. Des informations apparaissent ainsi de manière curieuse : les éléments qui sont avancés lors d'auditions reposent généralement sur des histoires (vraies ou fausses) reportées dans les médias ; les médias reprennent ensuite ces déclarations de hauts fonctionnaires.

Le « cyberterrorisme » joue sur deux craintes liées à l'inconnu : le pouvoir des technologies informatiques et les victimes que font des attaques aveugles et violentes[17]. Ce terme, qui soulève les passions, est souvent utilisé de manière inopportune, alors qu'il serait des plus important qu'il soit défini avec précision et employé à bon escient, en raison des craintes qu'il suscite. Les seules opérations pouvant être considérées comme du cyberterrorisme devraient être celles menées par des terroristes aux motivations politiques, religieuses ou idéologiques, et dont les effets destructeurs ou perturbateurs effraient[18].

Selon cette définition, aucun des incidents survenus jusqu'à présent ne peut être considéré comme du cyberterrorisme. En réalité, même si la plupart des groupes terroristes ont profité de la révolution de l'information pour établir leur présence sur le web afin de lever des fonds, recruter et diffuser de la propagande non censurée[19], jusqu'à présent, le cyberespace a été utilisé par les terroristes pour son effet multiplicateur au niveau de la collecte d'informations et de la définition de cibles et non pas comme arme offensive. De l'avis de certains experts, il semble peu probable qu'il devienne une arme de choix[20]. Même si nous ne pouvons ignorer complètement la menace en raison de la rapidité des évolutions technologiques et des changements des capacités des groupes terroristes[21], les décideurs et les experts doivent prendre garde d'exacerber une angoisse cybernétique en exaltant la médiatisation de cette question.

Jusqu'à présent, le cyberespace a été utilisé par les terroristes pour son effet multiplicateur au niveau de la collecte d'informations et de la définition de cibles et non pas comme arme offensive.

Les infrastructures des sociétés modernes sont exposées à toutes sortes de menaces et de risques, et le terrorisme n'est pas le plus probable ni le plus dangereux en termes de dégâts. Les risques de catastrophe naturelle, de défaillance mécanique ou d'acte accidentel d'un utilisateur autorisé sont tout aussi graves que le risque d'attaque délibérée. En raison de la complexité des infrastructures essentielles de l'information, même des opérations planifiées de maintenance peuvent provoquer des perturbations malgré de rigoureuses procédures d'autorisation et d'évaluation. Le débat sur la protection des infrastructures essentielles de l'information a tout à gagner à ne pas trop se focaliser sur

le risque d'attaques malveillantes mais plutôt sur l'ensemble d'événements potentiellement dangereux, y compris les défaillances dues à des erreurs humaines ou à des problèmes techniques. Cela permet d'apprécier à leur juste valeur les multiples aspects du problème de sécurité et nous évite d'abuser du mot terrorisme.

La protection des infrastructures essentielles de l'information : vers une stratégie adaptée à tous types de risques

Pour des raisons techniques et pratiques, mais aussi de coûts, il est impossible de garantir une protection absolue des infrastructures essentielles contre tous risques et menaces. Il faut donc recenser les points les plus vulnérables autrement dit les structures les plus indispensables et leurs points vitaux. Il faudrait aussi comparer la probabilité d'une menace et le coût d'une protection. Au moment d'étudier des mesures concrètes de protection, il est important de connaître la nature de la menace : protéger une installation contre un groupe de pirates informatiques expérimentés ou protéger des systèmes contre le risque d'accès non autorisés sont des opérations très différentes. Il n'existe pas de solution unique : les mesures de protection doivent être adaptées à des installations précises pour faire face à des menaces particulières.

Tant qu'il n'existera pas de données fiables sur la nature probable des menaces, une autre approche garantira de meilleurs résultats. Elle consiste à identifier les *effets* probables de la défaillance d'une infrastructure ou installation précise et à les atténuer. La logique est très simple surtout pour les infrastructures essentielles de l'information : lorsque le but est de préserver des services fiables, peu importe que l'effet de surprise provienne de l'intérieur ou de l'extérieur de l'infrastructure. Dans les faits, il est souvent difficile de déterminer si un événement préjudiciable particulier est dû à une attaque malveillante, une défaillance d'un composant ou à un accident[22]. La question principale n'est pas tant de savoir ce qui explique la défaillance de l'intégrité de l'information, mais plutôt de connaître les conséquences et complications qu'elle pourrait entraîner. Un réseau électrique peut connaître une défaillance à cause d'une simple erreur de manipulation sans aucune influence extérieure, ou d'une attaque sophistiquée lancée par un pirate informatique. Dans les deux cas, le résultat est le même : une panne de courant pouvant avoir un effet d'entraînement et provoquer des pannes successives dans les systèmes interconnectés. Savoir si la panne est due à un terroriste, une simple erreur humaine ou à une défaillance naturelle, ne permet pas d'arrêter ni de limiter les effets.

Il est donc intéressant d'opter pour une stratégie adaptée à « tous types de risques » ; elle convient pour toutes les initiatives de protection, quelle que soit la nature de la menace, et se concentre sur la capacité de réaction face à toute une série d'événements imprévus. L'objectif est d'améliorer la résistance, autrement dit la capacité d'un système à retrouver, dans l'adversité, son statut original ou à s'adapter à de nouvelles conditions[23]. La plupart des ripostes et mesures de précaution peuvent être utilisées aussi bien face à des événements délibérés ou naturels, à l'exception des activités des services de renseignement et de certaines actions relevant de la responsabilité des forces militaires ou de police (comme la protection physique) qui sont précisément axées sur les menaces délibérées de certains acteurs[24].

La nécessité de coopérer avec le secteur privé

Une stratégie adaptée à tous types de risques, comme toute politique de protection des infrastructures essentielles de l'information[25], implique une coopération : lorsqu'il s'agit de garantir la sécurité de leurs citoyens, les gouvernements ne peuvent agir seuls. Nombre de pays ont privatisé différents secteurs comme l'énergie, les communications, les transports, ou les services financiers, ou le feront bientôt[26]. Le secteur privé contrôle donc largement la possession, le fonctionnement et l'offre des infrastructures

essentielles de l'information. Le secteur privé a beaucoup plus de ressources techniques et un accès plus important aux infrastructures essentielles de l'information qu'un gouvernement[27]. Ces ressources n'ont cependant pas servi à améliorer la sécurité : la volonté de satisfaire les actionnaires en optimisant les profits des sociétés entraîne souvent des mesures de sécurité minimales. Les gouvernements veulent pourtant que le secteur privé suive des mesures de protection conformes aux paramètres ou cadres définis par les autorités publiques[28]. S'ils veulent convaincre le secteur privé sans adopter de réglementations lourdes, les gouvernements doivent trouver une solution qui offrira des avantages à tous.

Par chance, les États ont un certain nombre de services intéressants à offrir au secteur privé. De toute évidence, les exploitants des infrastructures essentielles de l'information connaissent mieux leurs activités que n'importe quel service gouvernemental et peuvent généralement être avertis ou conseillés par de nombreuses autres sources. Il n'empêche, un service gouvernemental chargé de la protection des infrastructures essentielles de l'information pourrait fournir des analyses non techniques réalisées par les services de renseignement nationaux et internationaux concernant, par exemple, la nature des organisations criminelles. Grâce à un échange mené par une entité gouvernementale « neutre », le secteur privé pourrait profiter de l'expérience d'autres acteurs du secteur privé et des enseignements tirés[29]. Enfin, les États peuvent offrir une assistance financière pour la recherche sur des technologies de protection et les coûts de mise en œuvre[30].

Face à un problème mondial, une action globale s'impose

Les actions nationales ne peuvent pas tout résoudre : la vulnérabilité des sociétés modernes – du fait qu'elles reposent sur des systèmes interdépendants – a des causes et des conséquences globales. Les infrastructures de l'information dépassant les frontières territoriales, les installations qui sont vitales pour la sécurité nationale et le fonctionnement indispensable de l'économie d'un État peuvent se trouver sur le territoire d'autres pays. De plus, le cyberespace – cet immense enchevêtrement presque omniprésent d'échanges électroniques – existe là où se trouvent des câbles téléphoniques, des ordinateurs ou des ondes électromagnétiques, ce qui entrave sérieusement la capacité pour un État de le réguler ou le contrôler seul. Pour être efficace, une politique de protection s'appliquant aux éléments stratégiquement importants des infrastructures de l'information doit trouver des solutions transnationales.

Des tensions sous-jacentes concernant l'utilisation du cyberespace expliquent, en partie, pourquoi des règles et normes n'ont pu être adoptées et appliquées au niveau international[31]. Certains États élaborent des doctrines et même des capacités leur permettant d'utiliser le cyberespace pour prendre un avantage militaire : ils investissent dans des doctrines et technologies militaires destinées à perturber les infrastructures (de l'information) de pays rivaux. Des utilisations offensives et agressives, et des initiatives visant à protéger le cyberespace contre les actions d'agresseurs sont menées parallèlement[32]. Des appels ont donc été lancés pour contrôler l'utilisation informatique dans les armées nationales par des normes de maîtrise des armements ou de comportement multilatéral, des accords pouvant porter sur la mise au point, la distribution et le déploiement d'armes cybernétiques ou sur leur utilisation[33]. Les méthodes classiques de maîtrise des armements ne seront clairement pas très utiles, principalement parce qu'il est impossible de vérifier ce genre de contrôles. Les approches structurelles, les actions visant à interdire complètement les moyens de guerre de l'information ou à limiter leur disponibilité, sont en grande partie impossibles en raison de l'omniprésence des technologies de l'information et du fait qu'elles sont à double usage[34]. Les seules options réellement envisageables pour la maîtrise des armements dans ce domaine semblent être principalement l'échange d'informations et l'élaboration de normes, et même ces possibilités ne sont étudiées qu'avec modération.

L'utilisation du cyberespace provoque des tensions ; les méthodes classiques de maîtrise des armements ne peuvent résoudre les défis que posent les technologies de l'information mais d'autres stratégies internationales semblent plus prometteuses. L'harmonisation des législations pour faciliter les poursuites contre les auteurs d'actes de cybercriminalité est une question centrale pour tous les États. La cybercriminalité représente une menace pour la prospérité économique et la stabilité sociale de tous les États qui sont connectés aux infrastructures globales de l'information. Tous les États ont donc intérêt à travailler ensemble pour concevoir un régime international[35] qui garantira la fiabilité et la capacité de survie des réseaux de l'information. Il s'agit là aussi d'une stratégie de résistance plutôt que d'une tactique fondée sur une menace. Les conventions multilatérales sur la criminalité informatique comme la Convention sur la cybercriminalité du Conseil de l'Europe, pourraient être élargies et complétées. Les organisations internationales pourraient favoriser l'élaboration et l'adoption de normes de sécurité de l'information et diffuser des recommandations et des directives sur les pratiques optimales. Au niveau du droit international, des mécanismes et institutions, comme Interpol, pourraient servir à l'échange d'information – pour permettre une alerte rapide des attaques – et pour les enquêtes sur la cybercriminalité. De meilleurs mécanismes de coopération pourraient également être créés.

Il faut cependant veiller à ne pas engager d'actions déjà menées au niveau national ou à un niveau inférieur : les principes de subsidiarité et de proportionnalité doivent être systématiquement pris en compte. Les actions engagées au niveau international devraient se concentrer sur les difficultés qu'un État ou une région ne peut régler seul, comme celles concernant les infrastructures mondiales comme Internet, ou des relations d'interdépendance très étroite de grande ampleur. Les organisations internationales peuvent ainsi renforcer le réseau complexe d'initiatives nationales et régionales, qui se chevauchent parfois dans le domaine de la protection des infrastructures essentielles de l'information. Elles peuvent ainsi améliorer la sécurité et la fiabilité des systèmes, des méthodes de gestion et des efforts internationaux de surveillance.

La coopération : la solution pour la protection des infrastructures essentielles de l'information

La protection des infrastructures essentielles de l'information est désormais une priorité politique en matière de sécurité. Le cyberterrorisme est souvent mentionné dans ce contexte, même si la menace est bien plus large, puisqu'elle va de la criminalité aux catastrophes naturelles en passant par de simples erreurs humaines. Il est quasiment impossible d'assurer en permanence une protection totale contre toutes les menaces possibles, non seulement pour des raisons techniques et pratiques, mais aussi à cause des coûts. L'on peut, en revanche, se focaliser sur des stratégies de prévention et tenter de limiter autant que faire se peut les conséquences d'une attaque éventuelle.

Comme les fournisseurs des infrastructures sont les principaux acteurs en mesure d'appliquer, au niveau des différentes infrastructures, les garanties techniques nécessaires à la sécurité des technologies de l'information, les gouvernements nationaux doivent coopérer avec le secteur privé pour garantir la sécurité à leurs citoyens. Les mesures de protection nationales connaissent toutefois des limites : verrouiller les infrastructures mondiales de l'information est une tâche globale. À l'heure actuelle, les divergences entre les différentes politiques de protection des infrastructures essentielles de l'information sont un obstacle majeur à l'élaboration d'un régime international car les régimes internationaux doivent reposer sur un minimum d'attentes et d'intérêts communs des principaux acteurs (nationaux). Cependant, en raison des intérêts qui sont les leurs sur les plans économiques et de la sécurité, les pays industrialisés s'efforcent de surmonter ces obstacles temporaires afin de progresser résolument dans le sens de conventions et mécanismes internationaux forts pour protéger l'environnement mondial de l'information.

Notes

1. Voir, par exemple, « Cyberattack on Estonia Stirs Fear of 'Virtual War' », *International Herald Tribune*, 18 mai 2007, à l'adresse <www.iht.com/articles/2007/05/18/news/estonia.php> ; « The Cyber Raiders Hitting Estonia », *BBC News*, 17 mai 2007, à l'adresse <news.bbc.co.uk/1/hi/world/europe/6665195.stm> ; « Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-attacks », *The Sydney Morning Herald*, 16 mai 2007, à l'adresse <www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html>.
2. Myriam Dunn Cavelty, à paraître en 2007, *Cyber-security and Threat Politics: US Efforts to Secure the Information Age*, Londres, Routledge.
3. « Russia Accused of Unleashing Cyberwar to Disable Estonia », *The Guardian*, 17 mai 2007, à l'adresse <www.guardian.co.uk/frontpage/story/0,,2081512,00.html>.
4. Ibid.
5. Le mot hacktiviste vient de la fusion des termes anglais hacker et activist. Les hacktivistes mènent des opérations de piratage contre un site Internet afin de perturber son fonctionnement mais ne provoquent pas de dégâts graves. Il s'agit, par exemple, de blocages ou de « sit-in » virtuels, de bombardement automatisé avec des courriers électroniques, d'intrusions, de virus ou de vers. Voir Dorothy E. Denning, 2001, « Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy », dans J. Arquilla et D. Ronfeldt (sous la direction de), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica (Californie), RAND, p. 239 à 288.
6. Eric A. M. Luiijf, Helen H. Burger et Marieke H. A. Klaver, 2003, « Critical Infrastructure Protection in The Netherlands: A Quick-scan », dans Urs E. Gattiker, Pia Pedersen et Karsten Petersen (sous la direction de), *EICAR Conference Best Paper Proceedings 2003*, à l'adresse <www.crypto.rub.de/imperia/md/content/lectures/kritis/bpp_13_cip_luiijf_burger_klaver.pdf>.
7. B. Buzan, O. Wæver et J. de Wilde, 1998, *Security: A New Framework for Analysis*, Boulder (Colorado), Lynne Rienner.
8. E. O. Goldman, 2001, « New Threats, New Identities, and New Ways of War: The Sources of Change in National Security Doctrine », *Journal of Strategic Studies*, vol. 24, nº 2, p. 45.
9. J. van Loon, 2000, « Virtual Risks in an Age of Cybernetic Reproduction », dans B. Adam, U. Beck et J. van Loon (sous la direction de), *The Risk Society and Beyond: Critical Issues for Social Theory*, Londres, Sage, p. 165 à 182.
10. Michael Näf, 2001, « Ubiquitous Insecurity? How to 'Hack' IT Systems », *Information & Security: An International Journal*, nº 7, p. 104 à 118.
11. M. J. G. van Eeten, E.M. Roe, P. Schulman et M.L.C. de Bruijne, 2006, « The Enemy Within: System Complexity and Organizational Surprises », dans M. Dunn et V. Mayer (sous la direction de), *International CIIP Handbook 2006. Vol. II: Analyzing Issues, Challenges, and Prospects*, Zurich, Centre pour les études de sécurité de l'ETH Zurich, à l'adresse <www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157>, p. 89 à 109.
12. Gouvernement du Canada, Bureau de la protection des infrastructures essentielles et de la protection civile. Analyse de menace, nº TA03-001, 12 mars 2003, à l'adresse <ww3.ps-sp.gc.ca/opsprods/other/TA03-001_f.pdf>.
13. Les attaques du 11 septembre 2001 démontrèrent que les terroristes pouvaient provoquer d'énormes dégâts en attaquant directement et physiquement des infrastructures essentielles et soulignèrent la nécessité de réexaminer également la question des protections physiques. Voir J. D. Moteff, 2003 (mis à jour le 13 mars 2007), *Critical Infrastructures: Background, Policy, and Implementation*, Congressional Research Service report RL30153, Washington, à l'adresse <www.fas.org/sgp/crs/homesec/RL30153.pdf>, p. 3.
14. National Research Council, 1991, *Computers at Risk: Safe Computing in the Information Age*, Washington, National Academy Press; Kenneth A. Minihan, Director, National Security Agency, Statement to the Senate Governmental Affairs Committee on Vulnerabilities of the National Information Infrastructure, à l'adresse <www.senate.gov/~gov_affairs/62498minihan.htm >, 24 juin 1998.
15. Dorothy E. Denning, 2002, « Is Cyber Terror Next? », dans Craig Calhoun, Paul Price et Ashley Timmer (sous la direction de), *Understanding September 11*, New York, W.W. Norton, à l'adresse <www.ssrc.org/sept11/essays/denning.htm>.
16. Voir, par exemple, « Bracing for Guerrilla Warfare in Cyberspace », *CNN Interactive*, 6 avril 1999 ; « Terror Groups Hide behind Web Encryption », *USA Today*, 5 février 2001 ; « Suspect Claims Al Qaeda Hacked Microsoft – Expert », *Newsbytes*, 17 décembre 2001 ; « FBI: Al Qaeda May Have Probed Government Sites », *CNN*, 17 janvier 2002 ; « Islamic Cyberterror. Not a Matter of If But of When », *Newsweek*, 20 mai 2002.
17. M. M. Pollitt, « Cyberterrorism – Fact or Fancy? », *Proceedings of the 20th National Information Systems Security Conference*, octobre 1997, p. 285 à 289.
18. Maura Conway, 2002, « Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet », First Monday, vol. 7, nº 11, <firstmonday.org/issues/issue7_11/Conway> ; Myriam Dunn Cavelty, à paraître en 2007, « Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate », *Journal of Information Technology and Politics*, vol. 4, nº 1.

19. Timothy L. Thomas, 2003, « Al Qaeda and the Internet: The Danger of 'Cyberplanning' », *Parameters*, printemps, p. 112 à 123 ; Gabriel Weimann, 2004, *www.terror.net. How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report 116 ; Gabriel Weimann, 2004, *Cyberterrorism—How Real Is the Threat?*, United States Institute of Peace, Special Report 119.
20. S. Barak, 2004, « Between Violence and 'E-jihad': Middle Eastern Terror Organizations in the Information Age », dans L. Nicander et M. Ranstorp (sous la direction de), *Terrorism in the Information Age – New Frontiers?*, Stockholm, Swedish National Defence College, p. 83 à 96.
21. Institute for Security Technology Studies, Technical Analysis Group, 2004, *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Dartmouth College (New Hampshire), à l'adresse <www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf>.
22. R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, et N. R. Mead, 1997 (mis à jour en 1999), *Survivable Network Systems: An Emerging Discipline*, technical report CMU/SEI-97-TR-013, ESC-TR-97-013, à l'adresse <www.cert.org/research/97tr013.pdf>, p. 3.
23. John A. McCarthy, 2007, « Introduction: From Protection to Resilience: Injecting 'Moxie' into the Infrastructure Security Continuum », dans *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, CIP Program Discussion Paper Series, Washington, George Mason University, à l'adresse <cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf >, p. 2 et 3.
24. Sergio Bonin, 2007, *International Biodefense Handbook 2007: An Inventory of National and International Biodefense Practices and Policies*, Zurich, Centre pour les études de sécurité de l'ETH Zurich, p. 378.
25. I. Abele-Wigert et M. Dunn, 2006, *International CIIP Handbook 2006. Vol. I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*, Zurich, Centre pour les études de sécurité de l'ETH Zurich.
26. Jan Joel Andersson et Andreas Malm, 2006, « Public-Private Partnerships and the Challenge of Critical Infrastructure Protection », dans M. Dunn et V. Mauer (sous la direction de), op. cit., p. 139 à 167.
27. Z. Baird, 2002, « Governing the Internet: Engaging Government, Business, and Nonprofits », *Foreign Affairs*, vol. 81, nº 6, p. 15 à 20.
28. Seymour E. Goodman, Pamala B. Hassebroek, Daving Kind et Andy Azment, 2002, *International Coordination to Increase the Security of Critical Network Infrastructures*, Document CNI/04 ; Olivia Bosch, 2002, *Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection*, les deux papiers furent présentés lors d'un atelier organisé par l'UIT à Séoul, du 20 au 22 mai 2002 sur le thème « Infrastructures de réseaux critiques : créer un climat de confiance ».
29. Centre pour les études de sécurité de l'ETH Zurich, 2006, *Information Security in Swiss Companies: A Survey on Threats, Risk Management and Forms of Joint Action*, Zurich ; Manuel Suter, 2007, *A Generic National Framework For Critical Information Infrastructure Protection*, papier présenté lors de la deuxième réunion de coordination de l'UIT sur la grande orientation C5 du Sommet mondial sur la société de l'information : Établir la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication, à l'adresse <www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf>.
30. I. Abele-Wigert et M. Dunn, op. cit., p. 385 à 402.
31. A. Rathmell, 2001 « Controlling Computer Network Operations », *Information & Security: An International Journal*, vol. 7, p. 121 à 144.
32. Ibid.
33. Heinrich Böll Stiftung, 2001, *Perspectives for Peace Policy in the Age of Computer Network Attacks*, Conference Proceedings, à l'adresse <www.boell.de/downloads/medien/DokuNr20.pdf> ; Dorothy E. Denning, 2001, *Obstacles and Options for Cyber Arms Controls*, papier présenté lors de la Arms Control in Cyberspace Conference, Heinrich Böll Foundation, Berlin, 29-30 juin 2001, à l'adresse <www.cs.georgetown.edu/~denning/infosec/berlin.doc>.
34. Ibid.
35. Un régime peut être défini comme un « ensemble de principes, normes, règles et procédures de décision implicites et explicites sur lesquels les acteurs ont les mêmes attentes dans un domaine précis des relations internationales ». Voir Stephen D. Krasner (sous la direction de), 1983, *International Regimes*, Ithaca (New York), Cornell University Press, p. 2.

Le terrorisme et la gouvernance de l'Internet : les questions cruciales

Maura Conway

Si la gouvernance mondiale est un sujet vaste et complexe, les sujets liés à ce que l'on peut appeler la « gouvernance de l'Internet » le sont tout autant. Les énigmes technologiques du cyberespace viennent compliquer encore un peu plus la difficulté de « légiférer » au niveau mondial ; en effet, ces efforts doivent déjà tenir compte des préoccupations économiques, culturelles, juridiques, politiques et de développement des différents États et protagonistes. Le déclenchement de la guerre dite globale contre le terrorisme est venu compliquer les choses. Aujourd'hui, des acteurs infra-étatiques et non étatiques exploiteraient – ou se prépareraient à exploiter – le pouvoir d'Internet pour harceler et attaquer leurs ennemis. Le terrorisme international était déjà une préoccupation majeure de sécurité avant le 11 septembre 2001 et l'apparition d'Internet au cours de la décennie précédente, mais les événements du 11 septembre et les avancées des technologies de l'information et de la communication ont ajouté de nouvelles dimensions au problème. Dans les journaux et les magazines, dans les films et à la télévision, dans les travaux de recherche et d'analyse, le « cyberterrorisme » est le nouveau mot à la mode. Depuis les événements du 11 septembre 2001, la question qui intéresse tout le monde est de savoir si le cyberterrorisme sera la prochaine étape. Il semble toutefois généralement admis que le risque, dans un avenir proche, d'une attaque numérique de l'ampleur des événements du 11 septembre ne soit pas très grand. Cela ne signifie pas pour autant que les spécialistes des relations internationales pourront continuer d'ignorer le pouvoir transformateur d'Internet.

Cet article examine les difficultés de la gouvernance de l'Internet face à l'utilisation croissante de ce moyen de communication par les terroristes. Nous examinerons plus particulièrement le durcissement des actions menées par des acteurs étatiques et infra-étatiques depuis les attaques de septembre 2001 aux États-Unis et de juillet 2005 au Royaume-Uni face à la présence croissante des groupes extrémistes sur Internet. Les défis de la gouvernance sont nombreux et variés, et concernent notamment :

- les débats sur le rôle des différents acteurs impliqués dans le processus de gouvernance, y compris les gouvernements nationaux, les hacktivistes* et les fournisseurs d'accès Internet ;
- la riposte législative adaptée face à la présence terroriste sur Internet ;
- et le débat entre la liberté de parole et le contrôle du discours.

La description et l'analyse de ces défis sont au cœur de cet article. Il convient toutefois au préalable d'examiner ce qu'on entend précisément par « gouvernance de l'Internet ».

Maura Conway est chargée de cours à la School of Law and Government de la Dublin City University, Irlande. Ses principaux intérêts de recherche concernent le terrorisme et Internet, et notamment les analyses théoriques et les discours dans les médias sur le cyberterrorisme, ainsi que le fonctionnement et l'efficacité des sites web terroristes. Une version longue de cet article paraîtra sous le titre « Terrorism, the Internet, and International Relations: the Governance Conundrum » dans M. Dunn, V. Mauer et F. Krishna-Hensel (sous la direction de), à paraître, 2007, *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Londres, Ashgate.

* [Note du traducteur. L'hacktiviste ou cybermilitant est un pirate informatique dont la motivation est principalement idéologique. Ce mot vient de la fusion des termes anglais *hacker* et *activist*.]

Qu'est-ce que la « gouvernance de l'Internet » ?

Les structures de gouvernance d'Internet étaient particulières au moment de la conception et du développement d'Internet. Il s'agissait, au départ, d'un projet de gouvernement : à la fin des années 60, le Gouvernement américain finança la création de l'Agence pour les projets de recherche avancée de défense (DARPA), chargée de concevoir une installation de communication qui pourrait survivre à une attaque nucléaire. Dans les années 80, une communauté plus large utilisait les installations de ce réseau qui était désormais appelé Internet. En 1986, un groupe de travail (Internet Engineering Task Force) fut créé pour gérer le développement d'Internet par un processus de décision concertée impliquant diverses personnes. En 1994, la Fondation nationale pour la science des États-Unis décida d'impliquer le secteur privé en sous-traitant la gestion du Système de noms de domaine (DNS) à Network Solutions. Ce choix provoqua la colère de nombreux utilisateurs et déclencha un conflit qui ne fut réglé qu'en 1998 avec la création d'une nouvelle organisation, l'Internet Corporation for Assigned Names and Numbers (ICANN), un partenariat sans but lucratif entre le public et le privé chargé de préserver la stabilité opérationnelle d'Internet grâce à une large représentation des communautés d'Internet au niveau mondial par des processus partant de la base et fondés sur le consensus.

Depuis la création de l'ICANN, le débat sur la gouvernance de l'Internet se caractérise par un engagement plus direct des gouvernements nationaux, principalement dans le cadre de l'ONU et de ses institutions. Le premier Sommet mondial sur la société de l'information, organisé à Genève en décembre 2003, a officiellement inscrit la question de la gouvernance de l'Internet à l'ordre du jour diplomatique. La Déclaration de principes et le Plan d'action adoptés en 2003, lors du Sommet mondial sur la société de l'information, proposaient un certain nombre d'actions dans le domaine de la gouvernance de l'Internet, et notamment la création d'un groupe de travail sur la gouvernance de l'Internet[1]. Cela devint nécessaire car « l'Internet » et « la gouvernance » faisaient l'objet d'une controverse, tout comme le concept même de « gouvernance de l'Internet ».

La « gouvernance » fut particulièrement discutée, surtout lors du Sommet mondial sur la société de l'information. La confusion terminologique fut à l'origine de malentendus. Lorsque l'expression « gouvernance de l'Internet » fut introduite lors du Sommet mondial sur la société de l'information, de nombreux pays l'associèrent au concept de gouvernement. Il semblait que les questions de gouvernance de l'Internet devraient être réglées principalement au niveau intergouvernemental avec une participation limitée d'autres acteurs. Quelles étaient les principales raisons de cette confusion terminologique ? Gelbstein et Kurbalija soulignent qu'il n'est pas forcément évident pour tout le monde que le terme « gouvernance » ne signifie pas « gouvernement ». Ils rappellent, par exemple, que l'expression « bonne gouvernance » est utilisée par la Banque mondiale pour encourager la réforme des États par une amélioration de la transparence, une réduction de la corruption et une multiplication de l'efficacité de l'administration et que, dans ce contexte, le terme « gouvernance » est directement lié aux fonctions essentielles des gouvernements[2].

Dans son analyse de la gouvernance de l'Internet, Klein s'appuie sur le texte déterminant de Robert Dahl *Democracy and Its Critics* (1989), dans lequel Dahl identifie ce qu'il considère comme les conditions minimales indispensables à la création d'un système de gouvernance efficace : l'autorité, le droit, des sanctions et la compétence de juridiction. « Ces quatre mécanismes rendent possible la gouvernance : l'*autorité* dirigeante peut prendre une décision politique applicable à sa *juridiction*, inscrire cette décision dans le *droit* et imposer des *sanctions* à quiconque désobéit » [italiques dans l'original][3]. Dahl a une vision de la gouvernance plus proche de celle de « gouvernement » que ce que pourraient admettre la plupart des acteurs – autres que les gouvernements nationaux – impliqués dans le développement d'Internet. En réalité, le groupe de travail sur la gouvernance de l'Internet a depuis publié une définition pratique de la notion de « gouvernance de l'Internet » : « Il faut entendre par « gouvernance de l'Internet » l'élaboration et l'application par les États, le secteur privé et la société civile,

dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet »[4]. Cela ne signifie pas que les quatre éléments identifiés par Dahl ne sont pas importants – ils reviennent régulièrement dans toute discussion sur la relation entre l'utilisation terroriste d'Internet et la gouvernance de l'Internet ; la définition du Groupe de travail sur la gouvernance de l'Internet attire cependant notre attention sur les conséquences des débuts d'Internet et notamment l'importance acquise par des acteurs autres que les États dans le processus de la gouvernance de l'Internet.

Le terrorisme et Internet : bref historique

En un peu plus de quatre semaines, en avril et mai 2004, Abou Moussab Al-Zarqaoui, ancien dirigeant de Al-Qaida en Iraq aujourd'hui décédé, « connut rapidement la gloire, ou l'infamie mondiale, en combinant délibérément une violence extrême et la publicité d'Internet »[5]. Début avril 2004, Al-Zarqaoui diffusa sur Internet un enregistrement audio de 30 minutes dans lequel il expliquait qui il était et pourquoi il combattait et donnait des détails sur les attaques dont lui et son groupe étaient responsables. Avant cette campagne de relations publiques sur Internet, chacune des attaques lancées par Al-Zarqaoui devait tuer un grand nombre de personnes afin d'être remarquée dans le chaos et la progression quotidienne du nombre de morts en Iraq. En s'exposant sur Internet, Al-Zarqaoui réussit à contrôler l'interprétation de ses actions violentes et eut un impact plus fort avec des opérations de moindre envergure.

En mai 2004, Al-Zarqaoui alla plus loin encore en exploitant au maximum l'effet multiplicateur d'Internet : il se fit filmer en train de décapiter un otage américain et diffusa cette vidéo en ligne[6]. L'objectif de cette vidéo était de montrer des images qui capteraient l'attention de ses alliés comme de ses ennemis. Ce fut, en ce sens, un succès incontestable ; Al-Zarqaoui prit très peu de risques dans cette affaire, mais « réussit, au moins aussi bien qu'une bombe tuant 100 personnes à Nadjaf, à compromettre les projets des États-Unis. Il devint, par la même occasion, un héros pour les jihadistes dans le monde entier »[7]. L'accès libre à des vidéos aussi atroces et à d'autres « snuff movies » sur Internet a provoqué une prise de conscience : l'aspect le plus important de la relation entre le terrorisme et Internet n'est pas le problème très discuté du cyberterrorisme, mais l'utilisation quotidienne d'Internet par les terroristes pour des activités allant de la diffusion d'informations au recrutement, qui ont commencé des années avant l'apparition d'Al-Zarqaoui.

Aujourd'hui, quasiment tous les groupes militants actifs sont présents sur Internet et nombre d'entre eux sont le sujet de plus d'un site. Certains de ces groupes ont déjà montré qu'ils ont compris le pouvoir de ce réseau global d'informations pour mettre en avant leur position : le Hezbollah libanais a clairement démontré cette capacité, tout comme les Tigres tamouls et Al-Qaida. Il n'est donc pas étonnant que ces groupes fassent l'objet d'une attention accrue depuis les attentats du 11 septembre 2001. Le reste de cet article s'attache à décrire et analyser les initiatives de gouvernance de l'Internet lancées par ceux qui s'inquiètent de l'utilisation croissante d'Internet par des extrémistes afin, notamment, de diffuser de l'information et d'effectuer du recrutement : la question qui se pose est celle du contrôle du contenu, autrement dit les efforts visant à réguler le type de matériel disponible sur Internet.

La question du contrôle du contenu

Qui se charge du contrôle du contenu ?

S'agissant du terrorisme, les gouvernements sont généralement les acteurs principaux en matière de contrôle du contenu puisqu'ils définissent ce qui doit être contrôlé et comment. Certains groupes de

particuliers, et notamment des hacktivistes, sont également prêts à s'impliquer et l'ont fait avec succès en perturbant la présence en ligne d'un certain nombre d'organisations terroristes. Concrètement, bien sûr, le contrôle réglementé du contenu des sites de même que les initiatives privées nécessitent la participation d'entreprises privées, et plus particulièrement des fournisseurs d'accès Internet et des sociétés de moteurs de recherche ; les États, tout comme les groupes privés et les particuliers, font de plus en plus pression sur ces sociétés pour contrôler le contenu ayant un lien avec le terrorisme. Nous évoquerons aussi les technologies de contrôle adaptées qui sont disponibles.

Trois types de politiques en matière de contenu

Les politiques concernant le contenu des sites Internet reposent généralement sur l'un des trois angles suivants : celui des droits de l'homme (liberté d'expression et droit de communiquer), du gouvernement (contrôle réglementé du contenu) ou de la technologie (instruments de contrôle du contenu).

D'après l'article 19 de la Déclaration universelle des droits de l'homme des Nations Unies (1948), la liberté d'expression et le droit de chercher, de recevoir et de répandre des informations est un droit fondamental de l'homme. D'un autre côté, la Déclaration reconnaît aussi que la liberté d'expression est contrebalancée par le droit qu'ont les États de limiter cette liberté au nom de la morale, de l'ordre public et du bien-être général (article 29). Par conséquent, la discussion et l'application de l'article 19 doivent chercher le juste équilibre entre ces deux préoccupations. Ce régime international ambigu ouvre la voie à des interprétations diverses des règles concernant la liberté d'expression et à des divergences d'application.

Le contrôle du contenu est étroitement lié à la liberté d'expression et aux préoccupations concernant les restrictions de cette liberté. Le contrôle des discours sur Internet est particulièrement controversé aux États-Unis où le premier amendement garantit une large liberté d'expression et même le droit de publier des discours incitant à la haine et d'autres documents analogues. Trouver le juste équilibre entre le contrôle du contenu et la liberté d'expression est un défi particulièrement difficile et la plupart des débats récents sur la gouvernance de l'Internet, y compris les procès et la législation, cherchent cet équilibre. Si le Congrès américain penche pour un contrôle plus strict du contenu, surtout depuis le 11 septembre 2001, la Cour suprême des États-Unis cherche à défendre les protections du premier amendement. Cet attachement à la liberté d'expression influence fortement la position des États-Unis dans les discussions internationales sur la gouvernance de l'Internet. Par conséquent, si les États-Unis ont signé la Convention sur la cybercriminalité, leur Constitution leur interdit de signer le Protocole additionnel à la Convention, qui porte sur la criminalisation des actes racistes et xénophobes commis par le biais de systèmes informatiques[8]. Autrement dit, si les gouvernements de l'Union européenne et autres signataires peuvent aujourd'hui invoquer le Protocole additionnel, en plus des autres lois sur les crimes inspirés par la haine permettant de poursuivre des groupes terroristes et leurs partisans qui publient en ligne du matériel incitant à la haine, les mêmes options juridiques ne sont pas possibles pour les autorités américaines.

Trouver le juste équilibre entre le contrôle du contenu et la liberté d'expression est un défi particulièrement difficile.

C'est pour cette raison que de nombreux sites de groupes terroristes sont hébergés aux États-Unis. Un fournisseur d'accès Internet basé au Connecticut proposait ainsi des services de colocation et d'hébergement à un site du Hamas dans des centres de données situés au Connecticut et à Chicago. Si des sites comme ceux soutenus par le Hamas font l'objet d'une surveillance plus étroite depuis le 11 septembre 2001, des sites web similaires avaient déjà été auparavant le sujet de discussions. En 1997, une controverse éclata lorsque l'on apprit que l'Université d'État de New York (SUNY) à Binghamton hébergeait le site web des Forces armées révolutionnaires de Colombie (FARC) et qu'un site de solidarité avec le mouvement révolutionnaire Túpac Amaru fonctionnait depuis l'Université

de Californie, à San Diego (UCSD). Les responsables de l'Université d'État de New York fermèrent rapidement le site des FARC. À San Diego, les autorités se prononcèrent en faveur de la liberté d'expression et le site du mouvement Túpac Amaru resta sur les serveurs de l'Université pendant quelques années.

Malgré les garanties constitutionnelles, les États ne sont pas impuissants, sur le plan technologique, face aux groupes de violence politique qui tentent d'utiliser Internet pour diffuser de l'information. Les États disposent de nombreuses technologies pour limiter la façon dont les dissidents utilisent Internet. L'utilisation d'Internet est efficace pour le recrutement et d'autres types d'actions politiques si les utilisateurs et le public concerné ont accès aux messages communiqués par Internet. Les États peuvent donc enrayer l'efficacité de ces stratégies en limitant l'accès des utilisateurs et du public aux technologies Internet, en censurant directement le contenu diffusé sur Internet, en contrôlant l'infrastructure Internet, ou en combinant ces deux options. Le point central du filtrage gouvernemental est généralement un index de sites web auxquels les citoyens ne peuvent accéder. Si un site web figure sur cette liste, l'accès n'est pas autorisé. Sur un plan technique, le filtrage se fait par un blocage sélectif des adresses IP par routeur, et utilise des serveurs proxy et des redirections DNS. Le contenu des sites est filtré dans de nombreux pays ; outre les pays habituellement associés à ces pratiques, comme la Chine, l'Arabie saoudite et Singapour, d'autres emploient de plus en plus la censure. Par exemple, l'Australie dispose d'un système de filtre pour certaines pages nationales, et le Land allemand de Rhénanie-du-Nord-Westphalie exige des fournisseurs d'accès Internet qu'ils filtrent, principalement mais pas uniquement, l'accès des sites néonazis.

Trois types de contenu

Les discussions sur le contenu des sites considèrent généralement trois types de contenu. Le premier type est celui pour lequel tout le monde convient qu'un contrôle est nécessaire. Ainsi, le contrôle de la diffusion de la pédopornographie en ligne est le sujet qui suscite le plus grand consensus. S'agissant du terrorisme, si le droit international (*jus cogens*) interdit l'incitation et l'organisation d'actes terroristes (ce qui signifie que la nécessité d'éliminer d'Internet ce type de contenu fait l'objet d'un consensus général), des différends continuent de surgir. La raison en est qu'il n'existe pas, au niveau mondial, de définition du terrorisme communément admise ce qui rend difficile, pour ne pas dire impossible, un éventuel accord sur ce qui pourrait être considéré comme un soutien au terrorisme dans une situation donnée.

S'agissant du contrôle, le deuxième type de contenu généralement examiné est celui qui pourrait être sensible pour des pays, des régions ou des groupes ethniques en raison de leurs valeurs religieuses ou culturelles. L'on ne peut nier qu'une communication mondialisée et plus intensive compromet les valeurs religieuses et culturelles. En fait, la plupart des procès liés à Internet portent sur ce type de contenu. L'Allemagne a une jurisprudence très développée dans ce domaine, en raison des nombreux procès intentés contre les responsables de sites web hébergeant du matériel nazi. En France, un tribunal a ordonné à Yahoo.com (États-Unis) d'empêcher les citoyens français d'accéder aux parties d'un site vendant des objets nazis. En Asie et au Moyen-Orient, la plupart des actions de contrôle du contenu sont officiellement justifiées par la protection de valeurs culturelles. Cela signifie généralement l'interdiction d'accéder à des sites pornographiques ou de jeux d'argent, ainsi qu'à des sites à caractère politique radical.

Le troisième type de contenu est celui des sites proposant des documents sensibles sur les plans politiques et idéologiques, ce qui implique, en fin de compte, une censure d'Internet. Se pose alors un dilemme entre le monde « réel » et le « cyberespace ». Les règles qui s'appliquent aux discours dans le monde réel peuvent s'appliquer à Internet. Le meilleur exemple pour illustrer cette situation est probablement la décision-cadre du Conseil concernant la lutte contre le racisme et la xénophobie

qui précise explicitement que « ce qui est illégal hors ligne est illégal en ligne »[9]. Ceux qui estiment qu'il faudrait une législation propre à Internet, adaptée à ses particularités, invoquent l'argument suivant : la quantité (autrement dit l'intensité de la communication, le nombre de messages, etc.) fait une différence qualitative. Selon ce point de vue, le problème des discours sur Internet incitant à la haine et liés au terrorisme n'est pas l'absence de réglementation, mais le fait que leur diffusion sur Internet pose d'autres problèmes juridiques en raison de l'ampleur et de la rapidité d'Internet. De plus en plus de gens sont exposés à ce type de discours et il est difficile d'appliquer les règles existantes. Par conséquent, la différence avec Internet est plus liée à la difficulté d'appliquer les règles qu'aux règles elles-mêmes.

Le paysage législatif contemporain

Le vide juridique qui prévalait au début de l'utilisation d'Internet s'agissant du contenu des sites laissait aux gouvernements nationaux une très grande liberté de contrôle. Les dispositions réglementaires nationales sur le contenu peuvent permettre de mieux défendre les droits de l'homme et de régler le rôle parfois ambigu des fournisseurs d'accès Internet, des services de répression, et d'autres acteurs, mais ces lois peuvent être cause de dissensions. Ces dernières années, de nombreux pays ont adopté, pour la première fois, une législation en matière de contrôle du contenu Internet. Certaines de ces lois s'expliquent par l'explosion de l'utilisation d'Internet et la nécessité qui est alors apparue de protéger les intérêts des citoyens-utilisateurs ; une grande partie de cette législation fut cependant adoptée à la hâte après le 11 septembre 2001 en raison de risques perçus contre la sécurité nationale. Les défenseurs des libertés du citoyen et d'autres soulignent le caractère inconsidéré et l'efficacité incertaine de telles politiques.

La position des États-Unis

Tout de suite après les événements du 11 septembre, le Federal Bureau of Investigation (FBI) fut impliqué dans la fermeture officielle de centaines, si ce n'est de milliers, de sites Internet basés aux États-Unis. Ainsi, plusieurs programmes radio radicaux diffusés sur Internet, comme ceux de *IRA Radio*, *Al Lewis Live* et *Our Americas* furent retirés, fin septembre 2001, par un fournisseur d'accès Internet dans l'Indiana après que le FBI eut informé cette société que ses biens pouvaient être saisis au motif qu'elle faisait l'apologie du terrorisme[10]. Comme ces sites et de nombreux autres qui furent fermés n'incitaient pas directement à la violence et ne levaient pas de fonds, ils n'enfreignaient pas les lois américaines et nombre d'entre eux furent remis en ligne assez vite après avoir été fermés.

De toutes les lois adoptées à la suite du 11 septembre 2001, la plus intéressante pour la gouvernance de l'Internet est le USA PATRIOT Act de 2001, qui rend illégal le fait de conseiller ou d'aider des terroristes, y compris par l'intermédiaire d'un site Internet[11]. Le cas de Babar Ahmad est, à cet égard, très intéressant. Ahmad, un citoyen britannique, publiait deux sites web jihadistes influents, azzam.com et qoqaz.net, qui étaient hébergés aux États-Unis ; il est accusé d'avoir réuni, par l'intermédiaire de ces sites, des fonds pour des militants islamistes en Tchétchénie et ailleurs. Le Gouvernement britannique a accepté une demande d'extradition des États-Unis et Ahmad devrait être jugé aux États-Unis pour avoir utilisé Internet à des fins liées au terrorisme, ce qui tombe sous le coup de la loi en tant que « conspiration en vue de fournir un appui matériel à des terroristes »[12]. Il ne s'agit pas seulement de la sollicitation de soutien financier évoquée ci-dessus, mais aussi, selon une requête déposée en 2004 auprès de la US District Court du Connecticut, de l'appel enjoignant tous les musulmans d'« utiliser tous les moyens à leur disposition pour suivre un entraînement physique et militaire au jihad » et leur donnant des « instructions explicites » pour réunir des fonds et les acheminer vers des organisations fondamentalistes violentes par le biais d'organisations écrans se faisant passer pour des organisations caritatives[13].

Les mêmes charges pèsent contre d'autres personnes résidant aux États-Unis. Cependant, en raison de l'importance de la protection de la liberté d'expression aux États-Unis, au moins deux personnes ont été jugées puis libérées sans qu'aucune charge ne soit retenue suite à des plaintes similaires : il s'agit de Sami Omas Al-Hussayen, candidat au doctorat en informatique à l'Université de l'Idaho, qui avait créé et entretenait un site web radical, et de Sami Amin Al-Arian, professeur à l'Université de Floride du Sud accusé, entre autres, d'avoir utilisé Internet pour publier et recenser des actes de violence commis par le Jihad islamique palestinien. Le procès de Babar Ahmad permettra, une nouvelle fois, d'éprouver le USA PATRIOT Act. Il sera intéressant de suivre l'impact de cette affaire sur les discours liés au terrorisme diffusés sur Internet aux États-Unis.

La position du Royaume-Uni

Les attentats de Londres, en juillet 2005, incitèrent le Gouvernement britannique à prendre des mesures contre les sites web terroristes hébergés au Royaume-Uni. Tout de suite après les attaques, le Ministre de l'intérieur de l'époque, Charles Clarke, indiqua dans un discours parlementaire qu'il chercherait à étendre les pouvoirs de l'État pour « s'occuper de ceux qui fomentent le terrorisme ou qui incitent d'autres à commettre des actes terroristes »[14]. Dans son discours, Clarke précisa que le fait de publier des sites web ou d'écrire des articles destinés à fomenter ou à provoquer le terrorisme étaient des activités qui relèveraient de ces nouveaux pouvoirs[15]. Le projet de loi de 2005 visant à prévenir le terrorisme fut adopté de justesse par le Parlement en octobre 2005 ; l'opposition se focalisa sur deux mesures principales : les nouveaux pouvoirs proposés pour la police permettant une garde à vue de 90 jours sans inculpation et la proposition de délit d'« incitation au terrorisme ou de glorification du terrorisme ». Un délit d'« apologie du terrorisme » devait clairement permettre de sanctionner la création, la mise à jour et l'hébergement de nombreux sites web actuellement opérationnels au Royaume-Uni.

Cette clause pourrait aussi être utilisée pour étouffer des discours politiques légitimes et c'est la plus grande critique qu'elle suscite. D'autres mesures de ce projet de loi susceptibles d'avoir un impact sur l'utilisation terroriste d'Internet au Royaume-Uni, comme le fait de déclarer illégaux « les actes menant au terrorisme » et le fait de donner ou suivre un « entraînement terroriste », furent dans l'ensemble très peu contestées lors des débats au Parlement. En l'occurrence, le Gouvernement fut mis en échec sur la question de la garde à vue. Les autres dispositions du projet de loi furent pourtant adoptées et constituent le Terrorism Act 2006[16]. À l'heure où nous écrivons cet article, nous ignorons quel sera l'impact de cette nouvelle législation sur les documents liés au terrorisme produits par des citoyens britanniques ou diffusés au Royaume-Uni par l'intermédiaire d'Internet.

Les initiatives internationales

Au niveau international, les principales initiatives de contrôle du contenu ont été engagées par des pays européens qui disposent déjà de lois fortes contre l'incitation à la haine et par des institutions régionales européennes qui veulent imposer ces mêmes règles au cyberespace. Le principal instrument juridique international traitant de la question du contenu est le Protocole additionnel à la Convention sur la cybercriminalité du Conseil de l'Europe. Le Protocole définit divers types de discours incitant à la haine qui devraient être interdits sur Internet, y compris le matériel raciste et xénophobe, la justification de génocide ou de crimes contre l'humanité. L'Organisation pour la sécurité et la coopération en Europe (OSCE) est également active dans ce domaine. En juin 2003, la conférence de l'OSCE sur la liberté des médias et Internet a adopté les Recommandations d'Amsterdam sur la liberté des médias et Internet. Elles encouragent la liberté d'expression et tentent de réduire la censure

Le principal instrument juridique international traitant de la question du contenu est le Protocole additionnel à la Convention sur la cybercriminalité du Conseil de l'Europe.

sur Internet. En juin 2004, l'OSCE organisa une réunion sur « La relation entre la propagande raciste, xénophobe et antisémite sur Internet et les crimes inspirés par la haine ». Cette rencontre portait principalement sur les possibilités d'utilisation malveillante d'Internet et la liberté d'expression. L'OSCE a ainsi permis à des opinions politiques et théoriques très diverses de s'exprimer sur ces deux aspects du contrôle du contenu, même si ces discussions n'ont débouché sur aucune règle nouvelle.

Sur un plan plus pratique, en mai 2007, les ambassadeurs de l'Union européenne sont convenus que le nouveau portail en ligne très sécurisé de l'Office européen de police (Europol), connu sous le nom de *Check the Web*, devra être renforcé pour la lutte contre le terrorisme. Ce site web permet aux 27 États de l'Union de mettre en commun des données sur les discussions (*chat*) sur Internet et la propagande islamistes et contient des informations sur les experts qui surveillent le web dans les pays de l'Union.

Le portail *Check the Web* n'est accessible qu'à certains services et experts, mais le Safer Internet Action Plan de l'Union européenne, a permis la création d'un réseau européen de numéros d'urgence, connu sous le nom de Inhope, permettant au grand public de signaler des contenus illégaux. Il se concentre, pour l'heure, principalement sur deux types de contenus illégaux, la pornographie impliquant des enfants et la pédophilie. Rien n'empêche les gouvernements nationaux ni les instances de l'Union européenne de mettre en place un système analogue pour tout contenu ayant un lien avec le terrorisme.

Le rôle des acteurs privés

Il incombe clairement aux gouvernements de légiférer sur le contenu des sites Internet ayant un lien avec le terrorisme même si, en raison de la nature d'Internet, des groupes et sociétés privés ne sont jamais très loin. Cette partie examine plus particulièrement le cas des acteurs autres que les États et leur rôle dans les efforts visant à éliminer d'Internet le matériel ayant un lien avec le terrorisme. Nous nous intéresserons plus particulièrement à deux groupes : les moteurs de recherche et les hacktivistes.

Les logiciels de géolocalisation

Les analyses sur la gouvernance de l'Internet avançaient souvent que les initiatives de censure étaient inutiles en raison de la nature décentralisée d'Internet. Aujourd'hui, cette affirmation n'est plus fondée à bien des égards : l'Internet repose sur de nombreuses techniques et technologies qui peuvent permettre un contrôle efficace. Cela étant, d'un point de vue technologique, les mécanismes de contrôle peuvent être contournés. Dans les pays où le contrôle du contenu est dirigé par les gouvernements, des utilisateurs astucieux ont trouvé les moyens techniques d'échapper à ces contrôles.

Il est encore difficile aujourd'hui d'identifier précisément qui se trouve derrière chaque écran d'ordinateur, mais il est relativement facile de connaître le fournisseur d'accès Internet utilisé. Les lois nationales adoptées récemment à travers le monde obligent les fournisseurs d'accès Internet à identifier leurs utilisateurs et, le cas échéant, à communiquer aux autorités les informations nécessaires à leur sujet. De nombreux gouvernements ont également annoncé leur intention de surveiller de plus près ceux qui ont accès à Internet dans des lieux publics, et notamment dans les cybercafés. Ces derniers font désormais l'objet d'une surveillance accrue en Inde, en Italie, en Thaïlande et dans une foule d'autres pays, la « sécurité nationale » étant l'argument généralement invoqué. Plus Internet sera ancré géographiquement, moins sa gouvernance sera unique. Par exemple, avec la possibilité de localiser géographiquement des transactions et des utilisateurs Internet, la question complexe de la compétence pourra être réglée plus facilement avec les lois existantes.

Les logiciels de géolocalisation sont une solution technique pour localiser un ordinateur et filtrer l'accès à certains contenus. L'affaire Yahoo! a été, de ce point de vue, très importante, puisque le groupe d'experts consulté a indiqué que dans 90% des cas, Yahoo! serait en mesure de déterminer si les pages de l'un de ses sites présentant des objets nazis étaient consultées depuis la France. Cet avis technologique a aidé la cour à prendre une décision finale. Les éditeurs de géolocalisation affirment qu'ils sont en mesure aujourd'hui d'identifier sans erreur le pays d'accès ainsi que la ville (dans 85% des cas), surtout s'il s'agit d'une grande ville. Ces logiciels peuvent donc aider les sociétés qui proposent du contenu sur Internet à filtrer les accès selon la nationalité et éviter ainsi des procès à l'étranger.

Le contrôle du contenu par les moteurs de recherche

Il existe de grandes différences entre la disponibilité et l'accès à du matériel en ligne : le fait que du matériel soit disponible sur Internet ne signifie pas automatiquement qu'un grand nombre d'utilisateurs peut y accéder. Ce sont généralement des moteurs de recherche qui conduisent l'utilisateur final vers un contenu sur le web. Par conséquent, si un site ne peut être trouvé avec Google ou un autre moteur de recherche important, sa visibilité est sérieusement compromise. Par exemple, sur les sites allemand et français de Google, il est impossible de trouver des sites web proposant du matériel nazi. Cela traduit une certaine auto-censure de la part de Google pour éviter d'éventuels procès. Après le 11 septembre 2001, de nombreuses sociétés Internet éliminèrent délibérément des sites jugés terroristes. Yahoo! retira ainsi des dizaines de sites faisant partie de Jihad Webring, une coalition de 55 sites en rapport avec le jihad et Lycos Europe mit en place une équipe de 20 personnes pour repérer les activités illégales de ses sites web et retirer le contenu lié au terrorisme. De tels comportements peuvent être considérés comme ayant un caractère politique et ont été critiqués, notamment par les partisans de la liberté d'expression.

Les hackers et les hacktivistes

Les événements du 11 septembre 2001 ont incité de nombreux particuliers et groupes privés à rechercher sur Internet des sites « terroristes » afin de les perturber. Les hackers étaient particulièrement bien placés pour ce genre d'activités. Ainsi, tout de suite après les attaques du 11 septembre, un groupe se faisant appeler The Dispatchers annonça qu'il allait détruire les serveurs web et l'accès à Internet en Afghanistan et s'en prendrait aussi aux nations qui soutenaient le terrorisme. Le groupe entreprit de détourner des centaines de sites web et lança des attaques par déni de service contre des cibles diverses allant du Ministère iranien de l'intérieur au Palais présidentiel de l'Afghanistan. Tous les groupes de pirates informatiques n'approuvaient pas cette guerre dite des hackers. Le 14 septembre 2001, le Chaos Computer Club, une organisation de hackers allemands, demanda l'arrêt des protestations et appela tous les hackers à cesser ces actions. Au cours des semaines qui suivirent les attaques, les détournements de pages web firent beaucoup de bruit, mais ils étaient dans l'ensemble peu nombreux et peu sophistiqués. S'il n'y eut pas d'escalade de ces attaques, c'est peut-être que beaucoup de hackers, craignant d'être associés aux attaques du 11 septembre, limitèrent d'eux-mêmes leurs activités.

Il n'a jamais été aisé pour les terroristes d'utiliser Internet, même avant septembre 2001. Les pages d'accueil ont fait l'objet d'attaques par déni de service et autres attaques pirates ; leurs fournisseurs d'accès Internet furent également touchés ce qui provoqua des difficultés plus durables. Ainsi, en 1997, l'Institute for Global Communications (IGC), un fournisseur d'accès Internet basé à San Francisco, hébergeant les pages de *Euskal Herria Journal*, publié par les partisans de l'organisation séparatiste basque ETA, fit l'objet d'un bombardement de courriers électroniques. Les attaques contre IGC commencèrent après l'assassinat par l'ETA d'un conseiller municipal populaire dans le Nord de

l'Espagne. Les protestataires voulaient que le site soit retiré d'Internet ; IGC finit par céder mais pas sans avoir archivé une copie du site, permettant à d'autres de publier des miroirs : des sites miroirs apparurent sur une demi-douzaine de serveurs sur trois continents. Cette campagne de bombardement électronique souleva néanmoins la crainte d'une nouvelle ère de censure due à l'intervention directe d'hacktivistes anonymes.

Depuis septembre 2001, un certain nombre d'organisations plus structurées ont été créées pour surveiller les sites web terroristes. L'une des plus connues est Internet Haganah, qui se décrit comme un mouvement anti-insurrectionnel pour Internet. Search for International Terrorist Entities (SITE), basé à Washington, se concentre, comme Internet Haganah, sur les groupes terroristes islamistes. Le service de renseignement payant de SITE aurait pour client le FBI, le Office of Homeland Security et divers groupes de médias. Mais quels sont les objectifs de ces organisations privées ? SITE rassemble (et vend) des informations provenant de sources librement accessibles. La co-fondatrice et directrice de SITE, Rita Katz, a déclaré : « Il est, en fait, dans notre intérêt que certains de ces sites de terreur soient gérés par des sociétés américaines. Pour les activités de surveillance, c'est un avantage lorsque ces sites sont hébergés par des serveurs aux États-Unis »[17]. Quant à Aaron Weisburd, qui dirige Internet Haganah, son objectif est de veiller à ce que les extrémistes continuent de passer d'une adresse à une autre : « Notre but n'est pas de les réduire au silence, mais de veiller à ce qu'ils continuent de bouger, qu'ils continuent à parler, les obliger à commettre des erreurs, afin de réunir, à chaque étape, autant d'informations que possible à leur sujet »[18]. Weisburd commence par examiner un site, puis effectue une recherche « whois » pour obtenir plus de précisions. S'il réunit des preuves d'extrémisme, il contacte la société d'hébergement et l'enjoint de retirer le site de ses serveurs. S'il réussit, Internet Haganah peut ensuite acheter le nom de domaine pour que l'adresse ne soit plus jamais utilisée. Depuis sa création en 2003, Internet Haganah revendique, ou affirme avoir aidé, l'arrêt de plus de 600 sites qui, d'après Internet Haganah, étaient liés au terrorisme.

Conclusion : et maintenant ?

Si les risques d'un « 11 septembre numérique » ne sont pas énormes dans un avenir proche, depuis 2001, Internet a mûri. Le terrorisme comme Internet sont des phénomènes mondiaux importants, qui traduisent et influencent divers aspects de la politique mondiale. Grâce à sa portée mondiale et à la richesse de son contexte multilingue, Internet a le pouvoir d'influencer sur des plans très divers différents types de relations sociales et politiques. À la différence des médias classiques, l'architecture ouverte d'Internet limite les efforts des gouvernements visant à réguler les activités sur Internet ce qui laisse aux utilisateurs une très grande liberté pour influencer Internet à leur guise. Certains sont des terroristes qui utilisent de plus en plus les nouveaux médias pour atteindre leurs objectifs. Les terroristes d'aujourd'hui, comme ceux de jadis, utilisent les médias habituels mais reconnaissent aussi l'importance de voies de communication plus directes.

Déjà en 1982, Alex Schmid et Janny De Graaf reconnaissaient que :

> Si des terroristes veulent faire passer un message, ils devraient avoir la possibilité de le faire sans avoir à tuer ou utiliser une bombe. Les mots valent moins que les vies. L'opinion ne sera pas plongée dans la terreur en voyant un terroriste s'exprimer ; les gens ont peur s'ils voient, non pas un terroriste, mais ses victimes [...]. Si les terroristes pensent qu'ils ont de solides arguments, ils cherchent à les présenter à l'opinion. Les sociétés démocratiques ne devraient pas craindre cela[19].

Tout le monde n'est cependant pas de cet avis. Au fil du temps, les acteurs étatiques et non étatiques ont cherché, avec plus ou moins de succès, à empêcher la disponibilité en ligne de matériel lié au terrorisme. Les gouvernements autoritaires ont eu un peu de succès avec des technologies qui

entravent la capacité de leurs citoyens d'accéder à certains sites. Les gouvernements démocratiques ont, pour leur part, moins de possibilités et même si des lois plus restrictives ont été adoptées récemment dans un certain nombre de juridictions, il n'est pas certain qu'elles seront plus efficaces que les initiatives précédentes qui visaient à contrôler, par exemple, l'incitation à la haine sur Internet. S'agissant des sites web terroristes et de leur suppression, les initiatives privées engagées par différents acteurs infra-étatiques en collaboration avec des fournisseurs d'accès Internet ont été bien plus efficaces. Les activités des hacktivistes soulèvent toutefois un certain nombre de questions importantes s'agissant de la liberté d'expression et de savoir qui peut et qui devrait fixer ces limites. La capacité qu'ont des acteurs politiques et économiques privés de contourner le processus démocratique et d'obtenir que le matériel qu'ils jugent inacceptable d'un point de vue politique soit retiré d'Internet est préoccupante. De telles initiatives devraient, en fait, nous inciter à reconsidérer la législation, pas simplement pour mettre en place certains contrôles – et interdire, par exemple, la mise en ligne et la diffusion de vidéo de décapitation –, mais en inscrivant dans la loi des protections plus fortes pour les discours politiques radicaux.

Notes

1. Voir Plan d'action, Sommet mondial sur la société de l'information, Genève, 12 décembre 2003, document WSIS-03/GENEVA/DOC/5-F, à l'adresse <www.itu.int/wsis/docs/geneva/official/poa-fr.html>, par. 13 b.
2. Eduardo Gelbstein et Jovan Kurbalija, 2005, *Internet Governance: Issues, Actors and Divides*, Genève, DiploFoundation et Global Knowledge Partnership, à l'adresse <www.diplomacy.edu/isl/ig>, p. 10 à 12.
3. Hans Klein, 2002, « ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy », *The Information Society*, vol. 18, n° 3, p. 194 et 195.
4. *Rapport du groupe de travail sur la gouvernance de l'Internet*, document WSIS-II/PC-3/DOC/5-F, 1er août 2005, par. 10.
5. Paul Eedle, « Al Qaeda's Super-Weapon: The Internet », papier présenté lors de la conférence intitulée « Al-Qaeda 2.0: Transnational Terrorism After 9/11 », Washington, 1er et 2 décembre 2004.
6. Cette vidéo s'intitule « Abu Musab al-Zarqawi shown slaughtering an American », et il est très probable, selon la CIA, que Al-Zarqaoui ait décapité lui-même l'otage (« Jamaat al-Tawhid wa'l-Jihad / Unity and Jihad Group », *Global Security.org*, à l'adresse <www.globalsecurity.org/military/world/para/zarqawi.htm>, et « 'Zarqawi' beheaded US man in Iraq », *BBC News*, 13 mai 2004, à l'adresse <news.bbc.co.uk/2/hi/middle_east/3712421.stm>).
7. Eedle, op. cit.
8. Protocole additionnel à la Convention sur la cybercriminalité, signé à Strasbourg, 28 janvier 2003, à l'adresse <conventions.coe.int/Treaty/FR/Treaties/Html/189.htm>.
9. Proposition de décision-cadre du Conseil concernant la lutte contre le racisme et la xénophobie, Journal officiel des Communautés européennes 2002/C 75/E17, 26 mars 2002.
10. Al Lewis Live peut toujours être écouté sur Pacifica Radio aux États-Unis. En mars 2002, le site IRA Radio fut autorisé à revenir en ligne, <www.iraradio.com>. Il semble avoir été fermé de nouveau quelque temps après février 2003. Les autres sites mentionnés ne sont plus en ligne.
11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).
12. *United States of America* v. *Babar Ahmad and Azzam Publications*, Indictment, United States District Court, District of Connecticut, à l'adresse <www.usdoj.gov/usao/ct/Documents/AHMAD%20indictment.pdf>.
13. « British Man Arrested on Several Terrorism-related Charges », communiqué de presse, United States Attorney's Office District of Connecticut, 6 août 2004, à l'adresse <www.usdoj.gov/usao/ct/Press2004/20040806.html>.
14. Charles Clarke, dans House of Commons Debates, *Hansard*, vol. 436, 20 juillet 2005, colonne 1255.
15. Ibid.
16. Le texte de cette loi est disponible dans son intégralité sur le site web de l'Office of Public Sector Information du Royaume-Uni, <www.opsi.gov.uk/acts/acts2006/20060011.htm>. Voir notamment la Partie 1, section 3, « Application of ss. 1 and 2 to internet activity etc ».).
17. Citée dans John Lasker, « Watchdogs Sniff Out Terror Sites », *Wired News*, 25 février 2005.
18. Ibid. ; voir aussi Gary Bunt, 2003, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments*, Londres, Pluto Press, p. 24 et 93.
19. Alex P. Schmid et Janny De Graaf, 1982, *Violence as Communication: Insurgent Terrorism and the Western News Media*, Londres, Sage, p. 170.

Les aspects militaires de la sécurité de l'information au niveau international dans le contexte de l'élaboration de principes de droit international universellement admis

Sergei KOMOV, Sergei KOROTKOV et Igor DYLEVSKI

Près d'une décennie s'est écoulée depuis que la Fédération de Russie a engagé son initiative au sein des Nations Unies sur la question de la sécurité de l'information au niveau international. Ce sujet complexe est étroitement lié à un certain nombre de principes fondamentaux du droit international, et notamment l'interdiction des guerres d'agression, le non-recours à la menace ou à l'emploi de la force et la non-ingérence dans les affaires intérieures d'un autre État.

Le choc que provoquèrent les deux guerres mondiales sur l'humanité influença particulièrement la transition de la communauté internationale vers des moyens civilisés de règlement des problèmes internationaux. Après la première guerre mondiale, l'expression « guerre d'agression » fut considérée, pour la première fois, dans un certain nombre d'instruments internationaux comme un crime international. Le Pacte Kellogg-Briand fut le premier traité multilatéral à établir en droit international l'interdiction des guerres d'agression[1]. Le Traité proclamait la renonciation à la guerre comme instrument de politique nationale pour régler les différends internationaux et précisait que le règlement de tous les différends ne peut être que pacifique.

Après la deuxième guerre mondiale, l'interdiction des guerres d'agression évolua vers le principe général de non-recours à la menace ou à l'emploi de la force dans les relations internationales. Le principe de non-ingérence dans les affaires intérieures d'autres États est également devenu un principe impératif du droit international.

L'Union soviétique a joué un rôle décisif dans l'instauration du principe d'interdiction des guerres d'agression et son évolution vers les principes de non-recours à la menace ou à l'emploi de la force. Notamment, en 1933, l'Union soviétique soumit un projet de définition de l'agression à la Commission générale de la Conférence internationale sur le désarmement ; bien que cette définition ne fut pas adoptée, elle jeta les bases pour de nombreux instruments internationaux élaborés à la suite de la deuxième guerre mondiale. En 1953, la délégation soviétique soumit un nouveau projet de définition de l'agression au Comité spécial créé par l'Assemblée générale des Nations Unies[2].

Avec du recul, le projet de définition de 1953 présentait l'avantage important d'avoir une portée très large qui englobait quatre grands types d'agressions : les agressions directes (militaires), indirectes, économiques et idéologiques[3]. Ce projet proposait de reconnaître pour coupable d'agression indirecte, l'État qui, le premier :

Sergei Komov, Sergei Korotkov et Igor Dylevski sont des experts du Ministère de la défense de la Fédération de Russie. Ils ont participé aux travaux du Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (2004-2005) et au groupe d'experts sur la sécurité de l'information de l'Organisation de Shanghai pour la coopération (2006-2007).

a) encourage des activités subversives dirigées contre un autre État (actes de terrorisme, de sabotage, etc.) ;

b) favorise l'incitation à la guerre civile dans un autre État ;

c) ou favorise une révolution à l'intérieur d'un autre État ou des changements de politique favorables à l'agresseur.

Les actes suivants étaient considérés comme des agressions idéologiques :

a) encourager la propagande en faveur de la guerre ;

b) encourager la propagande en faveur de l'emploi des armes atomiques, bactériennes, chimiques et de toutes les autres armes de destruction massive ;

c) et aider à la propagande en faveur des idées fascistes et nazies, de l'exclusivisme racial ou national ou de la haine et du mépris à l'égard d'autres nations.

Le projet de définition précisait aussi que d'autres actes d'agression que ceux énumérés pouvaient être reconnus par le Conseil de sécurité pour des actes d'agression.

En raison d'importantes divergences de vues entre les membres du Comité spécial lors de sa VII[e] session, le projet de définition de l'agression qui fut convenu ne portait plus que sur le type militaire. En décembre 1974, cette définition fut adoptée par l'Assemblée générale des Nations Unies[4]. Cette résolution présente une définition générale de l'agression (article 1), précise ce qu'est la preuve suffisante à première vue d'un acte d'agression (article 2) et énumère les principaux actes d'agression (article 3). Elle souligne que cette liste n'est pas exhaustive et que le Conseil de sécurité peut qualifier d'autres actes d'actes d'agression conformément aux dispositions de la Charte (article 4). Elle stipule, en outre, que « aucune considération de quelque nature que ce soit, politique, économique, militaire ou autre, ne saurait justifier une agression » (article 5).

La Charte des Nations Unies a été un élément essentiel dans l'évolution du principe d'interdiction des guerres d'agression vers le principe plus fondamental de non-recours à la menace ou à l'emploi de la force ; elle stipule en effet que « Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies » (alinéa 4 de l'article 2).

D'autres instruments internationaux confirmèrent et développèrent ce principe pour en faire une norme impérative du droit international. La *Déclaration de 1970 relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies*[5] stipule que :

> Une guerre d'agression constitue un crime contre la paix, qui engage la responsabilité en vertu du droit international.
>
> Conformément aux buts et principes des Nations Unies, les États ont le devoir de s'abstenir de toute propagande en faveur des guerres d'agression.
>
> […]
>
> Tout État a le devoir de s'abstenir de recourir à toute mesure de coercition qui priverait de leur droit à l'autodétermination, à la liberté et à l'indépendance les peuples mentionnés dans la formulation du principe de l'égalité de droits et de leur droit à disposer d'eux-mêmes[6].

Cette déclaration lie, en outre, le principe de non-recours à la menace ou à l'emploi de la force à celui de non-ingérence dans les affaires intérieures d'un autre État :

> [...] non seulement l'intervention armée, mais aussi toute autre forme d'ingérence ou toute menace, dirigées contre la personnalité d'un État ou contre ses éléments politiques, économiques et culturels, sont contraires au droit international.
>
> Aucun État ne peut appliquer ni encourager l'usage de mesures économiques, politiques ou de toute autre nature pour contraindre un autre État à subordonner l'exercice de ses droits souverains et pour obtenir de lui des avantages de quelque ordre que ce soit. Tous les États doivent aussi s'abstenir d'organiser, d'aider, de fomenter, de financer, d'encourager ou de tolérer des activités armées subversives ou terroristes destinées à changer par la violence le régime d'un autre État ainsi que d'intervenir dans les luttes intestines d'un autre État.
>
> L'usage de la force pour priver les peuples de leur identité nationale constitue une violation de leurs droits inaliénables et du principe de non-intervention[7].

À l'aube du troisième millénaire, de nombreux experts comprirent la nécessité d'une interdiction juridique de recourir non seulement à la force des armes mais aussi à toute autre violence constituant un recours illicite à la force pour une agression ou une ingérence dans les affaires intérieures d'un autre État. Une interprétation aussi large de la notion de « force » couvre aussi bien la coercition économique et énergétique, ainsi que toute autre forme de violence dans les relations internationales.

Aujourd'hui, toutes les sociétés dépendent de l'information. La conduite de ce qu'on appelle les « opérations d'information » est donc l'une des formes de force les plus dévastatrices. Ces opérations visent principalement à perturber le fonctionnement des principales installations militaires, industrielles et administratives de l'ennemi, à manipuler l'information et à influencer psychologiquement les troupes, la population civile et les autorités politiques et militaires d'un autre État en utilisant, en premier lieu, les technologies de l'information et de la communication.

Ces technologies permettent, en effet, de lancer des attaques électroniques ou informatiques qui sont radicalement différentes des attaques physiques classiques. Avec les moyens électroniques, la guerre passe d'une dimension physique à une dimension virtuelle. Aujourd'hui, un État peut être attaqué sans que son territoire ne soit envahi physiquement. Ce genre d'attaque peut provoquer des dégâts sur différents niveaux comme des défaillances techniques d'installations essentielles aux niveaux industriel, économique, énergétique ou des transports, ainsi qu'un effondrement financier et une crise de très grande ampleur. De plus, la perturbation de l'ordre civil et de l'autorité militaire peut provoquer d'importants dégâts non matériels et notamment démoraliser ou désorienter la population ou entraîner une panique générale.

Aujourd'hui, un État peut être attaqué sans que son territoire ne soit envahi physiquement.

Les États-Unis occupent le premier rang mondial des opérations d'informations et entendent poursuivre la multiplication de leurs ressources de renseignement déjà puissantes et de leurs capacités pour les guerres électroniques et les opérations psychologiques[8]. Par exemple, l'armée de l'air des États-Unis a annoncé la création du Air Force Cyber Command, qui sera opérationnel cette année. Dans le Commandement des forces stratégiques des États-Unis, le service principal chargé des opérations d'information est le Joint Functional Component Command for Network Warfare[9].

Les experts militaires connaissent très bien le potentiel des opérations d'information. Elles sont toutefois un phénomène relativement nouveau dans les relations internationales. Pour de nombreuses raisons politiques et générales, les membres de la communauté internationale doivent procéder à une évaluation juridique de cette question au niveau international.

Il n'est pas étonnant que les États-Unis s'opposent aux initiatives de discussions des aspects militaires du problème de la sécurité de l'information au niveau international. Ils ont joué un rôle clef dans la plupart des actions militaires majeures des cinquante dernières années et n'ont pas reconnu

par le passé des dispositions importantes, communément admises, régulant le recours à la force dans les relations internationales et l'ingérence dans affaires intérieures d'autres États. Ce n'est pas nouveau : dès le milieu du xx^{e} siècle, lors de discussions sur l'élément idéologique de la définition soviétique de la notion d'« agression », un représentant américain avait exprimé son désaccord, arguant que ce qui pouvait être considéré comme de la propagande dans un pays pouvait n'être que l'affirmation d'une presse libre dans un autre[10]. Plus récemment, dans le cadre de l'élaboration du Statut de Rome de la Cour pénale internationale, la délégation des États-Unis a soulevé une objection sur la définition de l'agression de 1974 ; d'aucuns ont interprété cette action comme une initiative visant à éviter la possibilité de voir une agression être jugée comme un crime international avec les responsabilités que cela implique[11].

De telles raisons expliquent pourquoi, en 2005, le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale[12] ne parvint pas à un consensus sur un projet de rapport. La possibilité d'examiner en profondeur, au niveau d'un forum d'experts, la question de la sécurité de l'information au niveau international a été repoussée jusqu'en 2009 date à laquelle un nouveau Groupe d'experts gouvernementaux doit débuter ses travaux.

Sur un plan juridique, il importe, avant tout, d'appliquer à la planification et à l'exécution des opérations d'information, les principes universellement admis de droit international sur les relations entre États. Cela implique naturellement d'adapter ces principes à la nature particulière des nouvelles relations interétatiques. Cette approche jettera les bases juridiques internationales nécessaires pour traiter, de manière générale, la sécurité de l'information au niveau international et, en particulier, ses aspects politiques et militaires. Les aspects juridiques d'autres domaines pertinents, comme le droit de l'espace, le droit humanitaire et la responsabilité internationale, devront être aussi pris en considération.

L'exécution et l'élaboration de principes essentiels de droit international

À l'heure actuelle, il n'existe pas en droit international de dispositions qui, sans ambiguïté, interdisent, autorisent ou régulent d'une autre manière les opérations d'information. De telles questions pourraient néanmoins être envisagées dans le cadre de l'application de principes juridiques internationaux essentiels. En particulier, la définition de l'agression de 1974 susmentionnée[13] stipule que non seulement la violence militaire mais aussi d'autres actes d'agression peuvent être qualifiés d'actes d'agression conformément à la Charte des Nations Unies. Cette disposition n'a toutefois pas encore été utilisée. Même auparavant, l'Iran avait proposé à l'Assemblée générale, en 1953, que toute action allant indiscutablement dans le sens d'une attaque armée ou se traduisant par une coercition compromettant l'indépendance d'un État devrait être qualifiée d'agression.

Depuis l'adoption de la Charte des Nations Unies, le principe de non-recours à la menace ou à l'emploi de la force contre l'intégrité territoriale ou l'indépendance politique d'un autre État n'a été appliqué que sur un plan physique. L'embargo pétrolier de 1973 conduisit de nombreux pays à s'interroger sur le point de vue selon lequel le recours à la force n'incluait pas les mesures de coercition économique, alors que la Charte des Nations Unies interdit le recours à la menace ou à l'emploi de la force de toute manière incompatible avec les buts des Nations Unies. D'autres États soutinrent que la disposition en question ne s'appliquait pas à une manifestation de force de ce genre[14].

En fin de compte, les résolutions des Nations Unies et la pratique n'apportent pas de réponse claire à la question de savoir si une attaque menée dans le cadre d'une campagne d'information peut être considérée comme une agression, un recours à la force ou une menace d'emploi de la force. Il importe donc de définir en détail les concepts d'« agression », de « force » et de « menace d'emploi de la force » dans le contexte de la sécurité de l'information au niveau international.

Pour ce qui est de considérer « l'information et l'influence psychologique » comme une intervention dans les affaires intérieures d'un État, il convient de se fonder sur les dispositions de la *Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies*[15] et la *Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et la protection de leur indépendance et de leur souveraineté*[16]. Cette dernière précise d'ailleurs « Aucun État n'a le droit d'intervenir, directement ou indirectement, pour quelque raison que ce soit, dans les affaires intérieures ou extérieures d'un autre État. En conséquence, non seulement l'intervention armée, mais aussi toute autre forme d'ingérence ou toute menace, dirigées contre la personnalité d'un État ou contre ses éléments politiques, économiques et culturels, sont condamnées »[17].

Même si ces documents n'offrent pas de définition précise d'une « intervention dans les affaires intérieures des États », ils contiennent une liste non exhaustive d'actions constituant une intervention. Cette base juridique nous permet de conclure que presque toute opération d'information visant un effet psychologique, effectuée en temps de paix par rapport à un autre État, peut être qualifiée d'intervention dans ses affaires intérieures. Même de bonnes intentions, comme la défense de la démocratie, **ne peuvent** justifier de telles opérations.

La *Déclaration de 1981 sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures des États* poussa plus loin le principe de non-ingérence dans les affaires intérieures des États. Les droits et obligations des États incluent :

- « Le droit des États et des peuples d'avoir librement accès à l'information et de développer pleinement et sans ingérence leur système d'information et de communications et de mettre leurs moyens d'information au service de leurs aspirations et intérêts politiques, sociaux, économiques et culturels, sur la base notamment des articles pertinents de la Déclaration universelle des droits de l'homme et des principes du nouvel ordre international de l'information »[18] ;
- « Le devoir d'un État de s'abstenir de toute campagne de diffamation, de tout dénigrement ou propagande hostile aux fins d'intervention ou d'ingérence dans les affaires intérieures d'autres États »[19] ;
- et « Le droit et le devoir des États de lutter, dans le cadre des prérogatives que leur confère leur constitution, contre la diffusion d'informations erronées ou déformées qui pourrait être considérée comme une ingérence dans les affaires intérieures d'autres États ou comme pouvant nuire à la défense de la paix, de la coopération et des relations amicales entre États et nations »[20].

En conséquence, la diffusion de désinformations par un État contre un autre, largement utilisée dans les opérations d'information, pourrait être considérée comme une ingérence dans les affaires intérieures et devrait entraîner des conséquences au niveau de la responsabilité internationale.

Le droit international interdit que les forces armées d'un belligérant violent le territoire d'un État neutre. Les États belligérants ne sont toutefois pas tenus de ne pas utiliser les réseaux informatiques ouverts d'un État neutre. L'utilisation de réseaux informatiques passant sur le territoire d'un État neutre pour mener des opérations d'information pourrait cependant être considérée comme une violation de son territoire. De telles agressions peuvent donc être considérées comme des actes de guerre illégitimes contre un État neutre. Si un État neutre refuse de s'opposer à l'utilisation de ses réseaux pour attaquer une autre partie, il pourrait être ensuite visé par l'État victime de l'opération d'information sous prétexte que ses réseaux furent utilisés.

La licéité d'actions de représailles suite à des opérations d'information est également une question juridique importante. Pour clarifier ce point, la communauté internationale doit régler un certain

nombre de problèmes connexes. Il faut notamment pouvoir identifier avec certitude la source d'une cyber-attaque et déterminer la compétence territoriale.

Selon le droit international, des agents étrangers ne peuvent mener des activités sur le territoire d'un autre État sans avoir obtenu son accord. Dans l'Affaire du Détroit de Corfou (1949), la Cour internationale de Justice des Nations Unies (CIJ) a décidé que l'entrée de la marine de guerre britannique dans les eaux territoriales albanaises sans autorisation était une manifestation de force et une violation du droit international[21]. Plus récemment, le Conseil de l'Europe a tenté de trouver à la question de la compétence territoriale une réponse fondée sur le droit international afin de garantir la sécurité de l'information au niveau international dans les réseaux informatiques[22]. Certains experts estiment que cette approche n'est pas très bonne ; ils pensent qu'elle signifie une violation de principes comme la souveraineté nationale et la non-ingérence dans les affaires intérieures d'autres États.

Conformément à l'article 51 de la Charte des Nations Unies, la légitime défense, individuelle ou collective, face à une agression armée est considérée comme un recours licite à la force. Un point n'est toutefois pas clair : cet article autorise-t-il une action militaire en riposte à une opération d'information menée par un État. En 1986, dans l'affaire du *Nicaragua c. États-Unis d'Amérique*, la Cour internationale de Justice des Nations Unies a conclu que les États ne sont pas autorisés à lancer des actions militaires pour riposter à des actes qui ne constituent pas des agressions armées[23]. En raison de ce précédent, à moins qu'une cyber-attaque ne soit qualifiée d'agression armée, la partie lésée ne pourra invoquer la légitime défense et riposter avec des armes classiques. Paradoxalement, vu l'ambiguïté juridique actuelle sur la question de la sécurité de l'information au niveau international, des mesures de riposte symétriques (par exemple, des attaques informationnelles) pourraient être prises en toute impunité. La solution juridique simple serait que le Conseil de sécurité qualifie une cyber-attaque comme constituant une menace pour la paix ou comme un acte d'agression, ce qui permettrait ensuite à l'État attaqué de prendre certaines mesures prévues par la Charte des Nations Unies.

Il existe, en droit international contemporain, un certain nombre de concepts pour décrire les actions prises par un État contre un autre comme l'agression, le recours à la menace ou à l'emploi de la force, et l'ingérence dans les affaires intérieures. Tous ces concepts s'appliquent aussi bien à des forces armées qu'à des groupes terroristes soutenus par des États. L'interprétation de ces concepts est conditionnée par la pratique historique de la guerre avec des moyens militaires classiques. Il est dès lors très difficile de définir les « opérations d'information » menées avec des moyens classiques ou radicalement nouveaux. Il est plus facile de qualifier la notion d'« ingérence dans les affaires intérieures d'un État » qui englobe tous les moyens possibles ayant des effets au niveau de l'information et de la psychologie. S'agissant des attaques électroniques et cybernétiques, nous pensons qu'il serait souhaitable qu'elles soient incluses dans les concepts d'« agression », de « recours à la force » et de « menace d'emploi de la force ». Ajoutons qu'il existe déjà en droit international un mécanisme, par le biais du Conseil de sécurité de l'ONU, pour déterminer une menace à la paix ou un acte d'agression. C'est ce mécanisme, utilisé conformément aux dispositions de la Charte des Nations Unies, qui doit déterminer si une opération d'information a eu lieu, quel État l'a menée, et décider des mesures qui s'imposent pour restaurer la paix et la sécurité internationales et pour empêcher une nouvelle violation de ces principes.

L'application et l'élaboration de principes dans certaines branches du droit international

D'importantes dispositions concernant les aspects militaires de la sécurité de l'information figurent dans les documents fondamentaux de certaines branches du droit international et notamment le droit international des télécommunications, le droit de l'espace, le droit international humanitaire, le droit sur la responsabilité internationale des États.

Certaines actions menées dans le cadre d'opérations d'information liées à la guerre électronique peuvent être couvertes par les instruments du *droit international des télécommunications*. Ainsi, selon la Constitution de l'Union internationale des télécommunications (UIT), toutes les stations (y compris militaires), quel que soit leur objet, doivent être établies et exploitées de manière à ne pas causer de brouillages préjudiciables aux communications ou services radioélectriques des autres États membres. Les États membres s'engagent, en outre, à prendre les mesures utiles pour réprimer la transmission ou la circulation de signaux de détresse, d'urgence, de sécurité ou d'identification faux ou trompeurs, et à collaborer en vue de localiser et d'identifier les stations sous leur juridiction qui émettent de tels signaux[24].

Par conséquent, des activités menées, en temps de paix, lors d'opérations d'information entraînant des conséquences interdites par la Constitution de l'UIT peuvent être considérées comme une violation d'un accord international. Il n'y aurait toutefois pas de violation si l'opération d'information était qualifiée de conflit armé ou si elle intervenait lors d'un conflit armé.

Si des satellites étaient utilisés pour mener une opération d'information, *le droit international de l'espace* pourrait s'appliquer. Le Traité sur l'espace extra-atmosphérique, qui est le fondement du droit international de l'espace, exige que les activités spatiales des États soient menées exclusivement à des fins pacifiques[25]. D'aucuns pensent toutefois que le droit de l'espace n'interdit pas directement l'emploi de satellites pour mener des opérations d'information. À la Conférence du désarmement, les États-Unis se sont opposés à l'examen du document de travail de 2002 intitulé « Éléments possibles d'un futur accord juridique international relatif à la prévention du déploiement d'armes dans l'espace et de la menace ou de l'emploi de la force contre des objets spatiaux »[26]. Lors de l'Assemblée générale, ils ont voté contre les résolutions sur la Prévention d'une course aux armements dans l'espace[27] et sur les Mesures propres à promouvoir la transparence et à renforcer la confiance dans les activités spatiales[28], en précisant dans leurs explications de vote qu'il n'y a pas de course aux armements dans l'espace extra-atmosphérique et donc pas de problème de maîtrise des armements que la communauté internationale doive régler. Certains craignent que cette position ne vise à préserver des conditions permettant d'utiliser l'espace extra-atmosphérique pour mener des opérations d'information au niveau mondial.

Il existe en droit international humanitaire un principe essentiel, celui d'humanité dans la lutte armée qui interdit le recours à la force à moins qu'il ne se justifie par une nécessité militaire. Le principe d'humanité concerne les méthodes et moyens de guerre, ainsi que la protection des victimes de guerre. Le droit international humanitaire limite les moyens que les belligérants peuvent employer contre l'ennemi. Il est, par exemple, interdit d'employer des armes ayant des effets sans discrimination (autrement dit, les armes visant des objectifs militaires comme des biens de caractère civil) ou causant des maux superflus[29]. Pour ne pas frapper sans discrimination, les hostilités – y compris sous la forme d'opérations d'information – devraient être limitées à des objectifs militaires, autrement dit ceux qui par leur nature, leur emplacement, leur fonction ou leur emploi jouent un rôle dans l'action militaire et dont la destruction, totale ou partielle, la saisie ou la neutralisation, dans les circonstances qui prévalent alors, offre un avantage militaire certain.

En période de conflit, la protection des biens de caractère civil, y compris contre des opérations d'information, devrait être assurée de deux façons :

- des mesures spéciales de protection devraient être prises pour vérifier que l'objectif devant être attaqué est bien un objectif militaire. Pour éviter des préjudices accessoires à des biens de caractère civil, il est important de s'abstenir de toute attaque contre des biens de caractère civil qui pourrait provoquer des dommages excessifs par rapport à l'avantage militaire réel escompté ;

- une protection spéciale des objets indispensables à la survie de la population civile, des ouvrages et installations qui représenteraient une grave menace s'ils étaient endommagés ou détruits (comme des centrales nucléaires, des barrages ou des digues), les biens culturels et ceux liés à la protection civile.

D'une certaine façon, le meilleur moyen de définir les opérations d'information par rapport au droit international humanitaire consiste à se fonder sur l'ampleur et la gravité de leurs conséquences[30]. La désorganisation du système financier d'un État, les catastrophes causées par l'homme et la panique engendrée par des opérations d'information peuvent provoquer d'importantes pertes humaines parmi les civils. Comme les technologies de l'information et de la communication sont à double usage, la distinction entre systèmes civils et militaires a disparu dans de nombreux cas. Outre les avantages militaires qu'elles apportent, les opérations d'information peuvent entraîner la défaillance de biens de caractère civil. Les opérations d'information touchant de tels biens devraient donc être interdites par le droit international humanitaire.

D'une certaine façon, le meilleur moyen de définir les opérations d'information par rapport au droit international humanitaire consiste à se fonder sur l'ampleur et la gravité de leurs conséquences.

Le droit international humanitaire n'interdit pas les ruses de guerre, comme le camouflage, de fausses opérations, la désinformation, etc. La perfidie est toutefois interdite. Il s'agit de : l'utilisation illicite du pavillon parlementaire, des insignes militaires et de l'uniforme de l'ennemi, de l'ONU ou de la Croix-Rouge ; ou de tuer ou capturer un adversaire par la perfidie. Il est néanmoins très difficile de faire la distinction entre perfidie et ruses de guerre dans une opération d'information visant à manipuler le sentiment de la population civile ou des dirigeants militaires ou politiques. Comme il n'existe pas encore en droit international de critère précis sur cette question, d'aucuns affirment qu'une telle manipulation ne constitue pas une violation du droit international humanitaire. Il ne faut toutefois pas oublier que la manipulation et la déformation de l'information servirent à justifier le déclenchement de deux guerres mondiales au siècle dernier et certains affirment que la manipulation de données de renseignement trompa l'opinion publique mondiale pour légitimer les actions récentes en Iraq.

Enfin, il importe de préciser que si les opérations d'information comme forme d'action militaire sont couvertes par les règles actuelles du droit international humanitaire, il faudrait appliquer **à ces opérations** tous les accords existants sur les lois et coutumes de la guerre.

Quant à la *responsabilité juridique internationale des États* pour des faits internationalement illicites (en cas de violation d'une obligation internationale d'un État), elle est bien établie en droit international contemporain, surtout s'agissant du recours à la menace ou à l'emploi de la force.

Les crimes contre la paix, les crimes de guerre et les crimes contre l'humanité furent, pour la première fois, qualifiés de crimes internationaux les plus graves dans les statuts du Tribunal militaire international de Nuremberg et du Tribunal de Tokyo. Une résolution de l'Assemblée générale de 1946[31] reconnut les principes du statut de la Cour de Nuremberg comme principes de droit international, autrement dit les principes instaurant la responsabilité des États et la responsabilité pénale des individus ayant commis des crimes internationaux. Ces principes sont universellement admis.

S'agissant des opérations d'information, nous pensons que les éléments de responsabilité d'un État pour des faits internationalement illicites sont les suivants :

- diffusion d'informations interdites par le droit international, y compris la propagande de guerre et la promotion du recours à la force, la propagande de la violence, et des informations provocantes, etc. ;
- diffusion d'informations spécialement destinées à produire des effets psychologiques ou idéologiques sur la population ou sur certaines personnes (fausses informations, informations fomentant les dissensions religieuses et autres hostilités, etc.) ;

- cyber-attaques contre les systèmes d'information des infrastructures essentielles d'un État et attaques contre d'autres infrastructures provoquant des dégâts économiques considérables ;
- et brouillage radio, transmission ou circulation de signaux de détresse, d'urgence, de sécurité ou d'identification faux ou trompeurs, etc.

Selon la gravité de leurs conséquences, de tels actes pourraient être qualifiés de crimes internationaux, autrement dit les pires délits, impliquant de graves mesures de responsabilité internationale.

Face à la menace d'opérations d'information, par exemple contre les installations d'infrastructures essentielles, l'on doit pouvoir soulever la question de contrôles de la fabrication et de la prolifération des moyens servant à la guerre de l'information ce que d'aucuns appellent les « armes de l'information ». Imposer des contrôles sur les exportations de technologies destinées à des fins spécifiques pourrait être un moyen de contrôler de telles armes. Pourtant, certains éléments comme les connaissances et les technologies très largement disponibles ne sont pas soumis à des contrôles à l'exportation. Pour instaurer un système juridique international de contrôle des armes de l'information, nous devrions nous inspirer de l'expérience de l'élaboration et l'application des régimes et des procédures de contrôle instaurés par le droit international pour d'autres types d'armes, tout en tenant compte des caractéristiques propres aux armes de l'information.

Conclusion

Au cours du siècle dernier, lorsque les armes chimiques, biologiques puis nucléaires furent créées, nous fûmes incapables d'élaborer des instruments internationaux sur le désarmement nucléaire et les instruments interdisant les armes biologiques et chimiques ne furent adoptés que tardivement. S'agissant des armes nucléaires, la communauté internationale doit encore convenir de leur interdiction.

Aujourd'hui, une menace politique et militaire totalement nouvelle fait son apparition. La communauté internationale ne doit pas laisser la situation se répéter pour les mesures visant à contrer le risque de prolifération des armes de l'information et doit lutter contre la non-sanction de la conduite d'opérations d'information. Pour y parvenir, la communauté internationale devrait, dans les meilleurs délais, vaincre son inertie face à des violations régulières des principes universellement admis du droit international et définir une barrière juridique internationale fiable face à la menace émergente d'agressions informationnelles.

Notes

1. Traité général de renonciation à la guerre comme instrument de politique nationale, signé à Paris le 27 août 1928.
2. Document des Nations Unies A/AC.66/L.2/Rev.1, 14 septembre 1953.
3. K.A. Baginyan, « Агрессия – тягчайшее международное преступление. К вопросу об определении агрессии » [L'agression comme délit international majeur. De la définition de l'agression] *Sovetskoe Gosudarstvo i Pravo*, vol. 1, 1955.
4. Assemblée générale des Nations Unies, Définition de l'agression, Résolution 3314 (XXIX), 14 décembre 1974.
5. Assemblée générale des Nations Unies, Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies, Résolution 2625 (XXV), 24 octobre 1970, annexe.
6. Assemblée générale des Nations Unies, Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies, Résolution 2625 (XXV), 24 octobre 1970, annexe.
7. Ibid.

8. United States Department of Defense Directive (DODD) S-3600.1, Information Operations, octobre 2001 ; DOD Information Operations Roadmap, 30 octobre 2003 ; FM 3-13 Information Operations: Doctrine, Tactics, Techniques and Procedures, 28 novembre 2003, SS FM 100-6 ; Joint Pub 3-13 Information Operations, 13 février 2006.
9. « A Special Subdivision for Neutralizing Foreign Media Created in the USA », *NEWSru.com*, 23 novembre 2005.
10. K.A. Baginyan, « Багинян К.А. Агрессия – тягчайшее международное преступление. К вопросу об определении агрессии. » [L'agression comme délit international majeur. De la définition de l'agression] *Sovetskoe Gosudarstvo i Pravo*, vol. 1, 1955.
11. V.A. Kartashkin (sous la direction de), *Human Rights and Armed Conflicts,* Norma Infra, Moscou, 2001, p. 137.
12. Créé conformément à la décision de l'Assemblée générale, Les progrès de la téléinformatique dans le contexte de la sécurité internationale, document des Nations Unies A/RES/56/19, 7 janvier 2002.
13. Assemblée générale des Nations Unies, Définition de l'agression, Résolution 3314 (XXIX), 14 décembre 1974.
14. K.A. Baginyan, « ягчайшее международное преступление. К вопросу об определении агрессии » [L'agression comme délit international majeur. De la définition de l'agression] *Sovetskoe Gosudarstvo i Pravo*, vol. 1, 1955.
15. Assemblée générale des Nations Unies, Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies, Résolution 2625 (XXV), 24 octobre 1970, annexe.
16. Assemblée générale des Nations Unies, Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et la protection de leur indépendance et de leur souveraineté, Résolution 2131 (XX), 21 décembre 1965.
17. Ibid., par. 1
18. Assemblée générale, Déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures des États, document des Nations Unies A/RES/36/103, 9 décembre 1981, par. I, al. c.
19. Ibid., par. II, al. j.
20. Ibid., par. III, al. d.
21. Affaire du Détroit de Corfou (Fond), Arrêt du 9 avril 1949, *CIJ Recueil*,1949, p. 34 et 35.
22. Convention sur la cybercriminalité (ETS No 185), signée à Budapest le 23 novembre 2001.
23. Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique). Arrêt du 27 juin 1986, *CIJ Recueil*, 1986, par. 195 et 232.
24. Constitution de l'Union internationale des télécommunications (adoptée à Genève, le 22 décembre 1992), art. 45, 47 et 48.
25. Le Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes (signé le 27 janvier 1967).
26. Représentants permanents de la Chine et de la Fédération de Russie, Éléments possibles d'un futur accord juridique international relatif à la prévention du déploiement d'armes dans l'espace et de la menace ou de l'emploi de la force contre des objets spatiaux, document de la Conférence du désarmement CD/1679, 28 juin 2002.
27. Assemblée générale, Prévention d'une course aux armements dans l'espace, document des Nations Unies A/RES/61/58, 3 janvier 2007.
28. Assemblée générale, Mesures propres à promouvoir la transparence et à renforcer la confiance dans les activités spatiales, document des Nations Unies A/RES/61/75, 18 décembre 2006.
29. Protocole additionnel I aux Conventions de Genève du 12 août 1949, art. 35 al. 2, art. 52 al. 2, art. 57.
30. Кубышкин А.В., Международно-правовые проблемы обеспечения информационной безопасности государства [Le problème juridique international que représente le fait d'assurer la sécurité de l'information d'un État], Thèse de doctorat, Académie d'État de droit de Moscou, 2002.
31. Assemblée générale des Nations Unies, Confirmation des principes de droit international reconnus par le statut de la Cour de Nuremberg, Résolution 95 (I), 11 décembre 1946.

Qui se charge de maîtriser les dangers du cyberespace ?

Henning WEGENER

Les particuliers, les politiciens et les observateurs universitaires sont de plus en plus conscients des risques majeurs et souvent mondiaux que représentent, en plus de leurs intérêts considérables, l'introduction et les avancées rapides des nouvelles technologies. Nous vivons dans une société, où le risque est mondial, et qui fait l'objet d'une analyse de plus en plus poussée et se caractérise par des tendances de plus en plus inquiétantes[1]. Alors que nous nous félicitons de nos progrès technologiques, le monde est devenu, par ses nouveaux aspects, très dangereux.

La fragilité du cybermonde

La vulnérabilité des systèmes de technologies de l'information et de la communication qui imprègnent tous les aspects de l'activité humaine et progressent de manière exponentielle est un facteur de risque important. Ces technologies ont ouvert la voie à de nouvelles possibilités en termes de création de richesse, d'efficacité gouvernementale, de développement humain et d'opportunités commerciales, et ont favorisé l'émergence d'un nouveau type de société du savoir avec de nouvelles options pour le partage et l'acquisition des connaissances. Les technologies de l'information sont désormais la matière première essentielle de toute activité sociétale. Les moyens informatiques, les télécommunications, Internet et les capacités des réseaux à haut débit réduisent à néant les frontières et les distances et rendent de plus en plus réelle la perspective d'une société mondiale avec une nouvelle division du travail, des bénéfices partagés et des sociétés nationales plus ouvertes et interdépendantes.

La cause première de vulnérabilité est tout simplement la multiplication des technologies de l'information et de la communication dans le monde. Plus d'un milliard d'ordinateurs et plusieurs dizaines de milliards d'autres processeurs et microprocesseurs, tout aussi vulnérables, fonctionnent aujourd'hui dans le monde, ces derniers imbriqués dans des systèmes dirigent de manière invisible des équipements vitaux de contrôle, de surveillance et de direction. La migration imminente de la plupart des téléphones, des instruments informatiques et capteurs, aussi bien fixes que mobiles, au protocole Internet (IP) va multiplier le nombre d'instruments vulnérables. Les technologies de l'information et les télécommunications seront inévitablement mêlées et imbriquées dans la prochaine génération de réseaux ; l'informatique sera à la fois omniprésente et invisible dans un environnement « ambiant intelligent ». À peu de chose près, tous ces équipements numériques sont connectés, ce qui favorise une croissance exponentielle de la connectivité. En raison des avancées révolutionnaires de l'informatique – comme les percées concernant la miniaturisation des circuits intégrés, le traitement des données, les vitesses de transmission ou les capacités de stockage, l'apparition de la robotique et de systèmes intelligents, l'amélioration de l'ergonomie des machines –, les appareils occupent notre

---

Ambassadeur Henning Wegener, ancien diplomate allemand, est Président du groupe permanent de surveillance sur la sécurité de l'information de la World Federation of Scientists.

environnement comme jamais auparavant, connectant d'une manière nouvelle les gens, les objets et les informations ; ils annoncent aussi une nouvelle génération de perturbations numériques et impliquent un véritable tournant dans notre façon d'envisager et de traiter la question de la sécurité de l'information. La progression rapide de toute une série de techniques sans fil, et notamment de capteurs très envahissants et de technologies d'identification par radiofréquence, ne fait qu'accroître cette vulnérabilité.

Les avantages des nouvelles technologies peuvent être compromis par des perturbations numériques autrement dit par une utilisation malveillante de ces technologies. Les possibilités sont diverses et incluent les attaques cybernétiques, les virus, les messages spam contenant un cheval de Troie ou d'autres logiciels malveillants, le sabotage des systèmes de données, etc. ainsi que la transmission d'informations cachées (par exemple, l'échange d'informations entre organisations criminelles). Les sociétés modernes imbriquées dépendent fortement de ces nouvelles technologies ; c'est précisément ce qui fait leur fragilité. Les menaces du cyberespace concernent particulièrement le fonctionnement et la sécurité du système mondial : l'absence ou à tout le moins une maîtrise correcte de la cybercriminalité, du cyberterrorisme et de la cyberguerre nous sont essentielles.

L'absence ou à tout le moins une maîtrise correcte de la cybercriminalité, du cyberterrorisme et de la cyberguerre nous sont essentielles.

La progression stupéfiante du niveau des menaces

La progression de la menace n'est pas nouvelle ; elle est une évidence. Au moins, depuis le début des années 90, la cybercriminalité et l'insécurité cybernétique font l'objet d'analyses, de débats et d'actions publiques et privées qui suivent la courbe de croissance des risques cybernétiques. Ce qui est nouveau, par contre, c'est que la cybercommunauté entre dans une ère nouvelle inquiétante ; elle est, en effet, de plus en plus exposée à des menaces graves. La course ancestrale entre attaque et défense, où les agresseurs sont généralement plus forts et disposent de moyens plus perfectionnés, est encore plus inégale dans le cybermonde car l'agresseur ne subit aucune contrainte de temps et de lieu, et dispose de moyens d'attaques rapidement renouvelables. L'intensité et la sophistication des techniques d'attaque utilisées aujourd'hui, de même que le niveau d'organisation de leurs auteurs sont vraiment stupéfiants. L'on peut désormais sérieusement douter de la possibilité de gagner la bataille pour la cybersécurité[2].

Si les vulnérabilités se multiplient, la menace semble progresser encore plus rapidement. La vitesse d'apparition et de diffusion de nouvelles sortes de virus – souvent une vingtaine par jour –, l'importance écrasante du spam (qui représenterait selon de récentes estimations plus de 90% du trafic total de messages électroniques), la sophistication des sites de phishing et la propagation des réseaux botnet* (pour lancer des attaques par déni de service paralysantes) sont phénoménales. Chaque jour, plusieurs dizaines de milliers d'ordinateurs sont recrutés dans des réseaux secrets et utilisés, à l'insu de leurs propriétaires, pour propager des virus, du spam ou pour commettre des vols massifs de données. Dans certains pays, plus de 70% des ordinateurs personnels seraient ainsi contaminés.

Les auteurs de ces crimes ne sont plus des pirates informatiques cherchant à s'amuser, mais principalement des groupes organisés aux intentions délictueuses qui ont de grandes compétences technologiques et économiques. Ils maîtrisent de plus en plus le développement rapide de nouveaux logiciels d'attaque, qui arrivent très vite sur le marché noir. Outre l'appât du gain, d'autres motivations politiques plus sombres peuvent guider ces groupes. L'on imagine sans mal la diffusion de ce potentiel dévastateur à des cyberterroristes ou à des États résolus à lancer une cyberguerre.

* [Note du traducteur. Un réseau botnet est un réseau d'ordinateurs infectés pour être utilisés sans que leurs propriétaires le sachent. Ce terme vient de la fusion en anglais de l'abréviation *bot* pour robot et *net* pour réseau.]

Une menace pour la paix et la sécurité internationales

Les cyber-attaques peuvent avoir trois types de conséquences : des conséquences économiques, la perturbation d'infrastructures essentielles, et des menaces pour la sécurité nationale et les capacités des systèmes militaires ou de défense et des premiers intervenants.

Les dégâts économiques provoqués par les cybercriminels atteignent déjà des proportions stupéfiantes. En raison, entre autres, du secret industriel et de l'ignorance de l'existence même de certains délits, il est difficile d'obtenir des chiffres précis, mais les pertes annuelles sont estimées à plusieurs dizaines de milliards de dollars. Les cyber-attaques contre des infrastructures essentielles dépendant toujours plus des technologies de l'information et de la communication (comme les barrages, l'aviation et le contrôle aérien, les réseaux électriques, les pipelines, les usines aux processus de production dangereux ou sensibles, les systèmes bancaires, les systèmes nationaux de santé, les bases de données essentielles des gouvernements et de l'industrie, etc.) représentent également un grave problème. Ces infrastructures sont généralement entre des mains privées et sont particulièrement vulnérables car la plupart de leurs systèmes de contrôle réparti et de leurs systèmes d'acquisition et de contrôle des données sont connectés à Internet, et peuvent donc être perturbés. En raison de la forte interdépendance de ces systèmes, des cyber-attaques peuvent avoir des conséquences immédiates graves sur l'ensemble des systèmes politiques et économiques nationaux et même des effets transfrontaliers importants. Par des effets instantanés de réaction en chaîne, des attaques successives contre diverses structures peuvent multiplier les dégâts.

Des États et des acteurs non étatiques peuvent aujourd'hui lancer, directement ou non, des cyber-attaques contre des capacités de défense nationale d'un autre pays en désactivant ses systèmes électriques et de communication, en bloquant les systèmes d'appel d'urgence, en agissant sur l'acquisition de renseignements, le fonctionnement des systèmes d'armes ou les procédures de commandement et de contrôle. Une possibilité encore plus troublante est la capacité ou plutôt la probabilité de lancer plusieurs attaques qui endommageraient simultanément des intérêts économiques, des infrastructures essentielles ainsi que des capacités militaires et de défense.

La cyberguerre, avec l'utilisation d'« armes de l'information », est une technique bien réelle. La crise numérique qui a frappé l'Estonie en avril 2007, avec des attaques extérieures massives, manifestement bien orchestrées, contre des réseaux publics et privés, est peut-être bien la première attaque ayant les caractéristiques d'une cyberguerre. Comme l'a prouvé cet événement, des attaques combinées sont désormais une possibilité réelle. Si l'on combine ces fragilités et la menace actuelle du terrorisme international, des scénarios alarmants deviennent plausibles. La sécurité de l'information et les concepts de paix et stabilité nationales et internationales sont aujourd'hui intrinsèquement liés.

L'importance de la coopération internationale

La cybermenace est asymétrique ; elle est par nature invisible, non linéaire et peut perturber le tissu social et les installations capitales d'un ou plusieurs États, et tout cela avec un engagement et des investissements minimums. Le problème est mondial et ne peut être réglé par les efforts d'un seul État ou d'un groupe d'États, ni même de régions. Internet n'a pas de frontière et des attaques peuvent être lancées depuis des lieux très éloignés ou non identifiables, ou depuis des pays où le cadre réglementaire est insuffisant. Repérer et suivre les agresseurs dans un cybermonde sans frontière et les faire répondre de leurs actes implique une action multilatérale qui dépasse les juridictions et les frontières nationales. Une action concertée de la communauté internationale et des mesures harmonisées ou compatibles de tous les États s'imposent. Une coopération portant sur les domaines juridique, politique, technique et économique est indispensable pour repérer et suivre ces agresseurs. Garantir la sécurité de l'information est une gageure universelle.

Les gouvernements nationaux et la communauté internationale travaillent sur des normes de sécurité pour les technologies de l'information et les télécommunications, des cadres pour la protection des infrastructures essentielles et des stratégies antispam. Une industrie puissante de cybersécurité a fait son apparition. La cybersécurité est une activité florissante et la croissance de cette industrie est prodigieuse. Des filtres antispam, des antivirus plus sûrs, des anti-spyware (contre les logiciels espion), des techniques de cryptage, des réseaux quantiques sûrs et des lignes à haut débit protégées ne sont que quelques-unes des réalisations de l'industrie de la sécurité des techniques de l'information. Nombre de ces mesures sont toutefois inutiles face aux nouveaux logiciels malveillants qu'introduisent régulièrement des systèmes d'attaque très inventifs. Malgré tous ces efforts, l'équilibre actuel entre l'attaque et la défense est loin d'être rassurant ; une action internationale collective s'impose de toute urgence.

Le défi qui se pose à la communauté internationale est vaste et complexe en raison des questions devant être réglées et du nombre d'acteurs impliqués. La gestion du cyberespace inclut un cadre réglementaire détaillé, concernant notamment la gouvernance de l'Internet, et implique des mécanismes intergouvernementaux, les gouvernements, le secteur privé et la société civile, qui sont tous appelés, de manière pratique, les « acteurs » du cybermonde.

Un régime international naissant

La volonté qu'a chacun de défendre ses intérêts et un besoin croissant évident d'enrayer l'insécurité cybernétique et de favoriser l'atténuation des risques, ont poussé tous les secteurs de la société dans la plupart des pays à s'attaquer aux menaces cybernétiques : les actions engagées dans le monde sont tellement nombreuses qu'il serait vain de chercher à proposer ne serait-ce qu'une liste schématique des acteurs et activités intéressantes.

Un défi aussi complexe ne se prête pas à une rationalisation facile et ne peut se réduire à de simples structures organisationnelles. Il n'existe pas de solutions organisationnelles homogènes permettant de savoir « qui gère la situation », mais une relation est toutefois possible, sur la base d'une vision commune, entre tous les acteurs impliqués. Une structure de commandement homogène ne peut être mise en place, mais un modèle de responsabilité partagée et des modes de travail opérationnel sont envisageables. Les objectifs doivent être les suivants : sensibiliser davantage le monde aux risques cybernétiques, optimiser les synergies, prévoir des processus de partage d'informations et d'apprentissage mutuel et établir des mécanismes de coordination. Les exigences réglementaires sont tout aussi importantes : il faut harmoniser les codes valables au niveau mondial et les faire respecter pour lutter contre les cyber-attaques, ne laisser aucune possibilité de contourner la réglementation, et donner une orientation générale à l'évolution future du cybermonde. Les failles de la cyberprotection doivent être comblées de toute urgence, surtout dans les pays en développement ; les structures de l'information sont particulièrement vulnérables ; le renforcement des capacités dans les économies en développement doit aller de pair avec le renforcement de la sécurité.

Les principes théoriques les plus adaptés sont peut-être ceux d'un régime international, définis dans les années 80[3]. L'idée est qu'un régime international convient lorsque le comportement des acteurs internationaux doit être coordonné autour d'une question précise, aussi complexe soit-elle. Les régimes, organisés autour d'une institution centrale (ou plusieurs), répondent à des besoins fonctionnels essentiels dans un « domaine précis des relations internationales » et se fondent sur des « principes, normes, règles et procédures de décision » implicites ou explicites « sur lesquels les acteurs ont des attentes convergentes »[4] ; cela inclut aussi des procédures de règlement des conflits. L'ouverture à tous est une caractéristique importante des régimes. Le financement du système international, le régime de non-prolifération, le Protocole de Kyoto et d'autres accords environnementaux, les mécanismes de financement et de rééchelonnement de la dette pour les pays en développement et de nombreux

autres accords ont été, à un moment ou à un autre, considérés comme des régimes internationaux. Goodman *et al*. analysèrent, voilà quelques années, le régime du transport aérien civil, axé sur l'Organisation de l'aviation civile internationale et basé sur une série de traités internationaux sur la sécurité de l'aviation ; ils pensaient que ce régime pourrait servir de modèle à une coopération internationale sur le cyberterrorisme et la cybercriminalité[5].

En 2001, la World Federation of Scientists avança la première l'idée d'un « ordre universel sur le cyberespace », un concept prioritaire pour gérer l'ère numérique et maîtriser les diverses menaces, allant de la cybercriminalité à la cyberguerre[6]. Cette proposition est totalement compatible avec le concept de régime ; encore plus depuis que les auteurs ont développé l'idée de négocier au niveau mondial un droit circonstancié sur le cyberespace comme élément fondamental de l'ordre universel qu'ils proposent. Depuis, cette idée a été poussée plus loin dans une publication de l'Institut des Nations Unies pour la formation et la recherche (UNITAR) qui soutient que le cyberespace fait partie du patrimoine commun de l'humanité et que chacun a le droit légitime de profiter, sans entrave, de ses avantages[7]. La notion de régime est un concept propice pour organiser les activités nationales et internationales du cyberespace et mérite d'être examinée de plus près.

La direction du régime sur le cyberespace

L'une des recommandations de la World Federation of Scientists précise qu'en raison de son caractère universel, le système des Nations Unies devrait diriger les activités intergouvernementales sur le fonctionnement et la protection du cyberespace. Cette idée ne semble susciter aucune opposition. La cybersécurité est d'ailleurs un motif de préoccupation pour l'Assemblée générale des Nations Unies qui, par une série d'activités et de résolutions, la plus récente étant la résolution 61/54 sur « Les progrès de l'informatique et de la télématique et la question de la sécurité internationale », a souligné la nécessité d'examiner au niveau multilatéral les risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et de revoir les principes internationaux pertinents.

Par chance, les Nations Unies semblent décidées à jouer un rôle majeur, comme l'ont démontré les deux sessions du Sommet mondial sur la société de l'information qui eurent lieu à Genève, en 2003, et à Tunis, en 2005. Ce Sommet fut l'un des plus importants et des plus réussis jamais organisés sous l'égide des Nations Unies. Les documents finaux des deux conférences, adoptés par consensus, contiennent un début de codification des principes devant régir le cybermonde, une base prometteuse pour un ordre universel du cyberespace. L'Agenda de Tunis pour la société de l'information insiste plus particulièrement sur la question de la cybersécurité. En attribuant des missions précises à différents acteurs du système des Nations Unies, le Sommet mondial sur la société de l'information a clarifié quelque peu la confusion concernant les compétences au sein du système des Nations Unies. L'Annexe à l'Agenda de Tunis définit de « grandes orientations » et confie des tâches précises à différents organismes en fonction de leur domaine de compétence. Il convient de noter tout particulièrement qu'un mécanisme de suivi est prévu. Un mandat clair assigne des tâches précises à différents acteurs et la résolution 60/252 de l'Assemblée générale, en date du 27 mars 2006, prie le Conseil économique et social de superviser à l'échelon du système la suite donnée aux textes issus du Sommet lors de délibérations annuelles jusqu'en 2015 (date du prochain Sommet mondial sur la société de l'information). La Commission de la science et de la technique au service du développement est le centre de coordination pour le suivi des textes issus du Sommet et fait le point sur cette question dans son rapport annuel au Conseil économique et social qui a précisé son mandat (résolution 2006/46, 28 juillet 2006) : la Commission doit être renforcée et doit utiliser une approche multipartite et inclure d'autres organisations internationales dans ses travaux. L'on ne peut que se féliciter de cette politique d'ouverture à tous et de la clarté du mandat de la Commission. La Commission doit recevoir des services de secrétariat de la part de la Conférence des Nations Unies

sur le commerce et le développement (CNUCED) qui, comme l'attestent ses rapports annuels sur l'économie de l'information, maîtrise les questions concernant le cyberespace. Les travaux ont déjà commencé : la Commission a établi un programme de travail qui lui permettra d'évaluer les progrès réalisés dans la mise en œuvre des textes issus du Sommet[8]. Le Groupe des Nations Unies sur la société de l'information a été créé par l'Assemblée générale pour gérer la coordination interinstitutions de la mise en œuvre des textes issus du Sommet mondial sur la société de l'information. Ses membres appartiennent tous au Conseil des chefs de secrétariat des organismes des Nations Unies.

D'importantes questions de gestion et de compétence ont ainsi été examinées et les bases d'un régime cohérent sur le cyberespace semblent être en place.

D'importantes questions de gestion et de compétence ont ainsi été examinées et les bases d'un régime cohérent sur le cyberespace semblent être en place.

L'Union internationale des télécommunications (UIT) est l'unique modérateur chargé de la grande orientation C5 du Sommet mondial sur la société de l'information, « Établir la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication ». L'UIT mérite donc une attention particulière non seulement en tant qu'organisateur du Sommet mondial sur la société de l'information mais en tant que principal dépositaire multilatéral des questions de cybersécurité. L'UIT est particulièrement bien placée pour exercer un rôle de coordination et de direction grâce à ses compétences techniques uniques et à ses ressources humaines, ainsi qu'à sa combinaison d'intérêts publics et privés (700 organisations ou sociétés liées aux technologies de l'information et de la communication participent, en effet, en tant que membres ou associés, aux travaux de l'UIT). L'approche multipartite nécessaire pour s'attaquer aux problèmes de cybersécurité est ancrée dans les traditions de l'UIT. En adoptant récemment le Global Cybersecurity Agenda – qui vise à réduire la cybercriminalité dans un délai de deux ans – et en mettant en ligne le Portail cybersécurité (Cybersecurity Gateway), l'UIT remplit remarquablement son rôle de direction pour les questions de cybersécurité et pour la mise en œuvre du Sommet mondial sur la société de l'information. Elle a le potentiel pour devenir la principale instance globale d'information sur ces activités – les rencontres (pour l'instant annuelles) de tous les acteurs sur la grande orientation C5 pourraient bien devenir le pôle mondial pour la sensibilisation, le partage d'informations les plus récentes et le lancement d'actions collectives.

Le Global Cybersecurity Agenda préconise, entre autres, l'élaboration de cadres législatifs homogènes. L'UIT pourrait devenir un puissant instrument pour promouvoir, au niveau mondial, une harmonisation des normes juridiques et de la répression de la cybercriminalité. Espérons que l'Union travaillera en étroite collaboration avec le Conseil de l'Europe (dont la Convention sur la cybercriminalité est le document de référence pour un système universel de droit sur la cybercriminalité), l'Union européenne, l'Organisation de coopération et de développement économiques et l'Office des Nations Unies contre la drogue et le crime (ONUDC), qui sont tous très engagés dans ce domaine.

Un autre élément important du Global Cybersecurity Agenda est l'accent mis sur le renforcement de la sécurité des technologies de l'information et de la communication dans les pays en développement qui sont les plus vulnérables et partant le maillon faible du cybermonde. En fin de compte, les compétences croissantes de l'UIT lui permettront de devenir l'Agence internationale des technologies de l'information dont la nécessité a été soulignée à maintes reprises.

Il reste encore beaucoup à faire

La position très ferme et l'orientation générale de la direction de l'UIT sont des éléments particulièrement encourageants pour le régime international qui se met en place sur la cybersécurité. D'autres conditions sont toutefois nécessaires pour que ce régime soit réellement efficace. Un filet de sécurité sans faille implique naturellement la coopération de *tous* les gouvernements nationaux et dépend de leur rapidité

à faire leur part pour élaborer une politique de cybersécurité et appliquer une « gouvernance pour la sécurité », en sensibilisant les acteurs civils, en adoptant des lois et en accordant leurs mécanismes de répression. Il dépendra aussi de l'acceptation par tous les protagonistes, y compris le secteur privé, de la proposition d'ouverture à tous et de leur engagement total.

D'importants réseaux ne participent toujours pas aux activités de l'UIT ou d'autres acteurs multilatéraux. Les organisations internationales concernant les forces de police, comme Interpol et, dans le contexte européen, Europol, devraient jouer un rôle plus grand dans les questions liées à la cybercriminalité. Elles devraient développer leurs relations avec l'UIT, l'agence multilatérale principale, et avoir des fonctions et des pouvoirs d'investigations plus forts. L'UIT entend promouvoir la mise en place d'équipes nationales d'intervention contre la cybercriminalité ; elle devrait donc encourager la mise en place, à l'échelle internationale, du « réseau 24/7 » établi par le Groupe des huit et adopté depuis par 57 États. Ce réseau, qui figure aussi dans la Convention sur la cybercriminalité du Conseil de l'Europe, est constitué de points de contact joignables vingt-quatre heures sur vingt-quatre pour recueillir en urgence des informations ou pour fournir une assistance dans des affaires liées aux technologies de l'information et de la communication. Les équipes d'intervention d'urgence en matière de sécurité informatique (CERT) constituent un autre réseau d'alerte et de réaction important actif dans la plupart des pays. Créées par la Carnegie Mellon University aux États-Unis, les CERT existent dans des organisations publiques et privées et sont coordonnées, au niveau international, par le Forum of Incident Response Security Teams. Elles sont de toute évidence du ressort de l'UIT et leurs activités devraient être incluses dans tout régime sur la cybersécurité. L'UIT devrait travailler à la mise en place de telles équipes dans les pays où elles ne sont pas encore actives ; plusieurs organismes internationaux (comme l'Union européenne et la Coopération économique Asie-Pacifique) fournissent déjà une assistance technique dans ce sens. Le Forum sur la gouvernance de l'Internet a été créé par le Sommet mondial sur la société de l'information ; la sécurité d'Internet figure dans son mandat. Il rend compte au Secrétaire général de l'ONU : il s'agit d'un forum multipartite de concertation qui laisse une place à l'ouverture et à la flexibilité. Il n'a aucun mandat de négociation mais ses travaux peuvent jeter les bases d'activités pouvant être menées par d'autres institutions. Les travaux du Forum sur la gouvernance de l'Internet sont proches de ceux de l'UIT et les deux instances devraient travailler ensemble ; le Secrétaire général de l'UIT assistera d'ailleurs à la prochaine réunion du Forum qui aura lieu en novembre 2007. L'Alliance mondiale pour les technologies de l'information et de la communication et le développement[9], créée pour promouvoir une utilisation efficace des technologies de l'information et de la communication dans les activités de développement, apparaît de plus en plus comme un forum de discussion multipartite et ouvert, mais a – pour des raisons peu plausibles – exclu de son agenda la question de la sécurité de l'information ; elle est par conséquent moins importante dans l'architecture d'un régime sur la cybersécurité[10].

Pour qu'un régime international complet soit possible, il reste une question à examiner en priorité : l'élaboration de règles de droit international sur la cyberguerre et d'autres actions transfrontalières moins hostiles lancées par des États ou des acteurs non étatiques. Pour l'instant, il n'est pas évident de savoir dans quelle mesure les règles classiques du droit international s'appliquent aux cyber-attaques et comment les « armes de l'information » doivent être traitées par les lois régissant les conflits armés ; la World Federation of Scientists a déjà tenté, à plusieurs reprises, de lever l'ombre sur cette question, mais pour l'instant les réponses se font rares aussi bien dans les documents publiés que dans l'action multilatérale. La question de la cybersécurité implique un examen et une interprétation de la Charte des Nations Unies (qui ne fut, bien évidemment, pas rédigée en pensant à l'ère cybernétique). Quel rapport peut-on trouver entre les cyber-attaques, la guerre de l'information et les termes de la Charte ? Comment fixer la nouvelle terminologie liée aux nouvelles technologies ? La notion d'« agression armée », qui est un concept clef de la Charte, doit être précisée. L'utilisation de technologies de l'information et de la communication pour causer ou entraîner des morts ou des destructions dans

un autre État peut-elle être considérée comme telle ? Un droit international circonstancié sur le cyberespace doit traiter de la cyberguerre ; les événements récents confirment d'ailleurs l'urgence de cette question. Il est donc particulièrement opportun et nécessaire que les organes de l'ONU portent leur attention sur cette question et participent à l'élaboration de règles internationales sur la guerre dans le cyberespace[11].

Le Sommet mondial sur la société de l'information n'a pas encore traité ce sujet essentiel ni attribué de compétences en la matière. Des travaux doivent être menés de toute urgence sur cette question au niveau international avec la participation de nombreux organes car elle est liée à la définition de termes et à l'interprétation de textes juridiques. L'Assemblée générale des Nations Unies, y compris ses Première et Sixième commissions, ainsi que la Commission du droit international devraient relever le défi que représente l'élaboration d'un cadre juridique adapté définissant les actions cybernétiques légitimes et illégales des États et des acteurs non étatiques. La communauté scientifique internationale devrait considérer comme une priorité l'examen de scénarios, de critères et de sanctions juridiques internationales.

Il s'agit d'une lacune grave qu'il convient de combler. L'on peut toutefois se féliciter, d'une manière générale, qu'un régime international sur le cyberespace existe et fonctionne déjà, même s'il reste beaucoup plus à faire.

Notes

1. Ulrich Beck, 1999, *World Risk Society*, Londres, Polity Press.
2. Cet argument reprend, en partie, l'évaluation des menaces cybernétiques faite lors de la deuxième réunion de coordination de l'UIT sur la grande orientation C5 du Sommet mondial sur la société de l'information, qui a eu lieu à Genève, les 14 et 15 mai 2007. (Meeting Report, document ALC5/2007/Meeting Report v.2, 17 mai 2007, à l'adresse <www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/meetingreport.pdf>).
3. Voir Robert O. Keohane, 1982, « The Demand for International Regimes », *International Organization*, vol. 36, nº 2, p. 325 à 355 ; Stephen Krasner (sous la direction de), 1983, *International Regimes*, Ithaca (New York), Cornell University Press.
4. Stephen D. Krasner, 1983, « Structural Causes and Regime Consequences: Regimes as Intervening Variables », dans Krasner, op. cit., p. 1.
5. Seymour E. Goodman, H. H. Whiteman, Mariano-Florentino Cuéllar, 1999, « The Civil Aviation Analogy », dans Abraham D. Sofaer et Seymour E. Goodman (sous la direction de), *The Transnational Dimension of Cyber Crime and Terrorism*, Stanford (Californie), Hoover Institution Press, à l'adresse <www.ituwiki.com/index.php?title=The_Transnational_Dimension_of_Cyber_Crime_and_Terrorism>.
6. World Federation of Scientists, 2003, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, document WSIS-03/GENEVA/CONTR/6.
7. Ahmad Kamal, 2005, *The Law of Cyber-Space: An Invitation to the Table of Negotiations*, Genève, UNITAR, à l'adresse <www.unitar.org/documents/thelawofcyberspace.pdf>.
8. Commission de la science et de la technique au service du développement, *Rapport sur la dixième session (21-25 mai 2007)*, document des Nations Unies E/2007/31.
9. L'Alliance mondiale pour les technologies de l'information et de la communication et le développement a remplacé le Groupe d'étude des Nations Unies sur les technologies de l'information et des communications.
10. Un Groupe d'experts gouvernementaux chargé d'étudier les menaces qui pèsent sur la sécurité de l'information fut mis en place par l'Assemblée générale des Nations Unies, en 2003. Ce groupe, se réunit en 2004 et 2005, mais ne parvint pas à un consensus sur un rapport final, en raison principalement de l'ampleur de son mandat. Espérons que le prochain groupe, avec un mandat plus limité et un agenda plus précis, sera en mesure de faire des propositions appréciables sur les questions de cybersécurité. Voir la résolution 58/32 de l'Assemblée générale, en date du 8 décembre 2003, document des Nations Unies A/RES/58/32, 18 décembre 2003, pour le mandat du groupe, et le *Rapport du Secrétaire général*, 5 août 2005, document A/60/202, pour la fin des travaux du groupe.
11. Pour plus d'information sur le droit international et la sécurité de l'information, voir l'article de Sergei Komov, Sergei Korotkov et Igor Dylevski dans ce numéro du *Forum du désarmement*. Gregory D. Grove, Seymour E. Goodman et Stephen J. Lukasik, 2000, « Cyber-attacks and International Law », *Survival*, vol. 42, nº 3, janvier, reste un article influent sur les conséquences juridiques de la cyberguerre. Voir aussi les recommandations et discussions sur la cyberguerre dans World Federation of Scientists, 2003, op. cit. ; Vitali Tsygichko, pas de date, *Cyber Weapons as*

a New Means of Combat, et Andrey Krutskikh, pas de date, *International Information Security and Negotiations*, tous les deux disponibles à l'adresse <www.itis-ev.de/infosecur> ; et International Centre for Scientific Culture World Laboratory et World Federation of Scientists, 2005, *Information Security in the Context of the Digital Divide*, document WSIS-05/TUNIS/CONTR/01-E, p. 30 à 35.

ACTUALITÉ DE L'UNIDIR

ACTIVITÉ

Disarmament Insight : envisager la sécurité humaine différemment

Les professionnels du désarmement multilatéral sont des gens très occupés. Comme ils sont extrêmement sollicités, il peut être difficile d'attirer leur attention sur la portée de nouvelles recherches susceptibles d'améliorer l'efficacité de leur action.

Fin 2006, le projet de l'UNIDIR intitulé « Le désarmement en tant qu'action humanitaire : mettre les négociations multilatérales en état de marche » a lancé, en collaboration avec le Forum de Genève, l'initiative Disarmament Insight. Le Forum de Genève est une initiative conjointe du Bureau Quaker auprès des Nations Unies, à Genève, de l'UNIDIR et du Programme d'études stratégiques et de sécurité internationale de l'Institut universitaire de hautes études internationales (HEI).

Le projet sur le désarmement en tant qu'action humanitaire suit deux axes étroitement liés : il veut montrer que les principes humanitaires peuvent favoriser l'action du désarmement et de la maîtrise des armements et étudie plus largement de nouveaux outils et principes permettant aux négociateurs d'appréhender différemment les défis du désarmement pour mieux les résoudre.

En « envisageant différemment la sécurité humaine », l'initiative Disarmament Insight cherche à intéresser, entre autres, les spécialistes du désarmement multilatéral aux conclusions du projet sur le désarmement en tant qu'action humanitaire et à d'autres thèmes, en s'inspirant notamment des trois ouvrages du projet publiés par l'UNIDIR en 2005 et 2006.

En plus de symposiums avec les professionnels du désarmement multilatéral et d'autres activités, différentes ressources ont été développées pour le web dans le cadre de l'initiative Disarmament Insight. Elles sont disponibles en ligne à l'adresse <www.disarmamentinsight.blogspot.com>.

Le site de Disarmament Insight propose des liens vers les ouvrages issus du projet sur le désarmement en tant qu'action humanitaire, un blog mis à jour très régulièrement (où les visiteurs peuvent poster leurs commentaires) et les podcasts d'orateurs ayant participé à des événements organisés par Disarmament Insight. Parmi les podcasts récents, citons :

- L'un des plus éminents primatologues, Frans de Waal, expliquant aux diplomates du désarmement ce qu'ils peuvent apprendre de « la guerre, la paix et les primates » ;

Dans cette rubrique, nous mettons en avant une activité pour en présenter la méthodologie, les dernières avancées ou les résultats. Nous vous proposons également une description détaillée d'une nouvelle publication de l'Institut. N'oubliez pas que toutes les activités de l'UNIDIR sont présentées sur notre site web, avec les coordonnées des personnes responsables, et des extraits de nos publications, que vous pouvez commander en ligne <www.unidir.org>.

- et Paul Seabright, économiste et auteur de *The Company of Strangers: A Natural History of Economic Life*, évoquant nos connaissances sur les niveaux de violence armée et les enseignements des neurosciences et de l'économie comportementale qui pourraient être utiles aux spécialistes du désarmement multilatéral.

Pour plus d'informations, veuillez consulter le site <www.disarmamentinsight.blogspot.com>.

NOUVELLE PUBLICATION

International Assistance for Implementing the Programme of Action on the Illicit Trade in Small Arms and Light Weapons: Case Study of East Africa

Les armes légères sont un problème grave pour la sécurité et le développement de l'Afrique de l'Est. Le Burundi, le Kenya, l'Ouganda, le Rwanda et la Tanzanie luttent contre le commerce illicite d'armes légères, adoptent de nouvelles législations, fixent des objectifs nationaux et, dans certains cas, appliquent des plans d'action en coordination avec le Centre régional sur les armes légères et la Communauté de l'Afrique de l'Est. En raison de l'ampleur du problème des armes légères dans cette région qui n'a pas les capacités nécessaires, une assistance internationale est indispensable pour mettre en œuvre des programmes sur les armes légères. La plupart de l'assistance reçue entre 2001 et 2005 a été consacrée à des programmes de désarmement, démobilisation et réintégration ; 5% seulement de l'assistance ont servi à d'autres projets liés aux armes légères, principalement au Kenya, en Ouganda et en Tanzanie. Chacun des cinq pays présentés dans cette étude sont à des stades divers d'application du Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères et disposent de capacités différentes.

Début 2008, ces pays auront adopté de nouvelles politiques et législations sur les armes légères ; une assistance sera alors essentielle pour la sensibilisation et la formation liées à ces politiques et législations ainsi que pour leur application. Renforcer les capacités des points de contact nationaux est une priorité particulière pour le Burundi et le Rwanda ; améliorer les ressources et capacités disponibles le long des frontières et aux points d'entrée aux frontières, la tenue de registres, la gestion et la sécurité des stocks, le marquage des armes sont les priorités les plus importantes identifiées par les États de la sous-région. En plus de présenter les résultats de l'étude sur l'assistance internationale en Afrique de l'Est, ce rapport avance certaines recommandations de politique générale afin d'améliorer la mobilisation de ressources. Les profils des différents pays, précisant les actions prises et les besoins d'assistance, sont présentés à la fin du rapport.

Cette étude a été menée dans le cadre du projet de l'UNIDIR sur « L'assistance internationale pour l'exécution du Programme d'action des Nations Unies sur le commerce illicite des armes légères » qui cherche à élaborer un mécanisme qui aidera les États à définir leurs besoins en matière d'assistance pour appliquer le Programme d'action et donnera aux donateurs potentiels la possibilité d'avoir accès à ces informations.

International Assistance for Implementing the Programme of Action on the Illicit Trade in Small Arms and Light Weapons: Case Study of East Africa

Kerry Maze et Hyunjoo Rhee

Publication électronique, disponible sur notre site <www.unidir.org>

40 pages

UNIDIR

Gratuit