16

LABORATOIRE DE L'IRSEM 2013

IRSEM
Institut de Recherche Stratégique de l'Ecole Militaire

Laboratoire de l'IRSEM N°16

La coopération internationale et bilatérale en matière de cybersécurité: enjeux et rivalités

La question de la cybersécurité s'est posée depuis les années 1980 et elle a gagné en importance avec la démocratisation de l'usage de l'internet. Face à la nature internationale du cyberspace et de la cybercriminalité, l'État se trouve impuissant à lui-seul pour garantir sa sécurité nationale. La coopération internationale constitue donc une composante indispensable à la mise en œuvre d'une réponse qui se voudrait efficace. Une telle coopération doit cependant faire face à un certain nombre d'enjeux.

L'objectif de ce laboratoire est d'étudier les enjeux de la coopération internationale en matière de cybersécurité et ses limites quant aux intérêts propres des États.

IRSEM
1 place Joffre – case 46
75700 Paris SP 07
http://www.defense.gouv.fr/irsem

ISSN : 2116-3138
ISBN : 978-2-11-138000-4

LA COOPÉRATION INTERNATIONALE ET BILATÉRALE EN MATIÈRE DE CYBERSÉCURITÉ :

ENJEUX ET RIVALITÉS

ALIX DESFORGES

LABORATOIRES DE L'IRSEM DÉJÀ PARUS :

1- L'ASIE DU NORD-EST FACE À LA MONTÉE EN PUISSANCE DE LA CHINE
2- L'IMPACT DU PARTENARIAT ENTRE LES BRIC (BRÉSIL, RUSSIE, INDE ET CHINE) ET LES PAYS AFRICAINS SUR L'ÉVOLUTION DU RÉGIONALISME SÉCURITAIRE
3- L'ARMÉE AUSTRALIENNE DANS LA GUERRE DU VIETNAM
4- LA « RECONSTRUCTION POST-CONFLIT ». IMPLICATIONS ET LIMITES D'UN CONCEPT MULTIDIMENSIONNEL.
5- AN UNPRECEDENTED POWER SHIFT AND THE REVIVAL OF EAST ASIA
6- ATELIER DE RÉFLEXION PORTANT SUR DES PROPOSITIONS D'ÉVOLUTION DES MODALITÉS DE CONTRACTUALISATION ET DE CONDUITE DES PROGRAMMES D'ARMEMENT
7- THE ROLE OF GREENLAND IN THE ARCTIC
8- RÉFLEXION SOCIÉTALE SUR LES INTERFACES CERVEAU-MACHINE POUR L'HOMME ET IMPLICATIONS POUR LA DÉFENSE
9- LA FORMATION D'ARMÉES ÉTRANGÈRES. ÉTUDE COMPARATIVE DES POLITIQUES DES PRATIQUES DES ANNÉES 1950 À 2010.
10- L'ACADÉMIE DE LA BOUE. REGARDS CROISÉS SUR L'APPRENTISSAGE DES FORCES ARMÉES
11- LA GESTION DE LA CRISE LIBYENNE PAR L'UNION AFRICAINE : CHRONIQUE D'UNE IMPUISSANCE ANNONCÉE
12- LE ROLE SOCIAL DES ARMÉES : PERSPECTIVES COMPARATIVES ET ACTUALITÉ
13- MEDIATION REGIONALE : LE CAS ISRAELO-PALESTINIEN
14- LA PAIX PAR LE COMMERCE, DE L'EPOQUE MODERNE A NOS JOURS - MYTHE ET REALITE
15- DE L'ASYMETRIE CAPACITAIRE A L'ASYMETRIE DES BUTS DE GUERRE : REPENSER LE RAPPORT DE FORCE DANS LES CONFLITS IRREGULIERS

L'Institut de recherche stratégique de l'École militaire (IRSEM) a pour mission de promouvoir la recherche sur les questions de défense et d'encourager une nouvelle génération de chercheurs. L'ensemble de ses productions et de ses activités peut être suivi sur son site :

www. defense.gouv.fr/irsem

SOMMAIRE

INTRODUCTION

La question de la coopération internationale en matière de cybersécurité n'est pas nouvelle. Depuis une vingtaine d'année, le rôle croissant de l'internet dans le fonctionnement de la société conjugué à l'explosion de la cybercriminalité ont incité les États à coopérer afin de répondre à un phénomène de plus en plus organisé. Le 23 novembre 2001, trente États ont signé la Convention du Conseil de l'Europe sur la cybercriminalité. Cette convention pose pour la première fois les jalons d'une coopération internationale entre les États signataires en matière de lutte contre la cybercriminalité. Depuis les années 1980 et les premiers virus, les actes malveillants perpétrés grâce à l'internet ont connu une croissance exponentielle. Si des pirates informatiques existent depuis l'apparition de l'informatique et se sont constitués en communauté dès le début des années 1980 ; c'est bien la démocratisation de l'usage de l'informatique et de l'internet qui a permis l'explosion du phénomène cybercriminel. Ce dernier s'est par la suite organisé de façon spectaculaire à l'image des autres trafics illégaux (armes, drogues etc.). On estime aujourd'hui que 100 000 nouveaux logiciels malveillants sont découverts chaque jour[1] et que les revenus générés par ces activités dépassent désormais ceux du trafic de drogue[2].

Si la cybercriminalité est une facette des menaces du cyberespace, certaines peuvent constituer un véritable enjeu de sécurité nationale. Les États font face à de multiples attaques informatiques : sabotage d'infrastructures vitales (transport, énergie etc.), vol d'informations sensibles, déstabilisation politique etc. Ainsi l'informatique et l'internet induisent un facteur de risque non seulement pour la sécurité des citoyens mais aussi pour celle de l'État lui-même.

Face aux menaces informatiques, un État ne peut, à lui-seul, garantir sa sécurité ou celle de ses citoyens. La nature internationale du réseau et sa gestion quasi-inexistante au niveau international sont autant d'arguments militant en faveur d'une coopération de l'ensemble des acteurs du domaine. La coopération internationale constitue donc une composante indispensable à la mise œuvre d'une réponse qui se voudrait efficace. Pourtant une analyse précise de la situation révèle que la mise en place d'une coopération internationale doit faire face à de nombreux défis. Pourquoi, alors que tous s'accordent sur le caractère primordial de la coopération, celle-ci éprouve tant de difficultés dans sa réalisation ? Quels sont les enjeux et les rivalités qui en freinent l'exécution ? Si l'intérêt de la coopération ne semble pas être remis en cause, il semble que les spécificités du cyberespace ainsi que les intérêts propres des États, les incitent à se montrer prudents dans sa mise en œuvre.

Ainsi, après avoir étudié les enjeux de la coopération internationale en matière de cybersécurité et fait l'analyse de plusieurs initiatives, nous verrons comment les intérêts propres des États constituent un frein sérieux à l'instauration d'une coopération internationale d'envergure.

[1] Entretien de François PAGET, expert chez McAfee, réalisé par l'auteur le 23 août 2012
[2] Source Symantec : http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20090922_03 consulté le 25 septembre 2012

I- ASSURER LA SECURITE DANS LE CYBERESPACE : UN ENJEU INTERNATIONAL

a. Un réseau international et une menace globale

L'internet, en passant d'un outil réservé à quelques universitaires américains au réseau comptant plus de deux milliards d'internautes dans le monde en 2011[3], est devenu un réseau de télécommunication international. Il se fonde sur l'interconnexion des réseaux à l'échelle planétaire. Autant de câbles, modems, routeurs, serveurs qui dépendent tous de juridictions précises en cas de litiges. L'internet comme réseau technique de communication est autant contraint par la géographie physique que par les frontières politiques. Chaque pays a permis ou non le développement de son infrastructure sur son territoire selon un plan d'aménagement répondant à des critères géographiques et/ou sociologiques et/ou économiques et/ou politiques qui lui sont propres. Cette nature multi-juridictionnelle de l'internet constitue de fait un facteur incitatif pour les États dans la mise en place d'une coopération internationale en matière de cybersécurité. La menace portée par le réseau se joue des frontières des États. Elle est globale et généralisée.

De la cybercriminalité aux attaques informatiques contre les infrastructures de type *Supervisory Control And Data Acquisation* (SCADA) en passant par l'espionnage, les menaces induites par l'internet sont globales. Les nombreux chiffres disponibles sur la provenance des attaques informatiques de tout type sont sujets à caution ; ils permettent toutefois de prendre conscience de la globalité du phénomène.

Dans le domaine de la création de logiciels malveillants, ThreatExpert affirme que plus de 31% des logiciels malveillant de la planète seraient d'origine chinoise. 21% d'entre eux seraient d'origine russe et 8% brésilienne[4] en septembre 2012. A l'inverse, les attaques de type dénis de service (ou *denial of service* - DOS)[5] se caractérisent par les multiples origines géographiques des machines utilisées pour mener l'attaque. Les ordinateurs des *botnets,* réseaux d'ordinateurs zombies, seraient localisés à plus de 16% en Inde, à 10% aux États-Unis et 9% des ordinateurs zombis sont situés en Russie[6]. Les serveurs centraux utilisés pour leur contrôle sont eux principalement localisés aux États-Unis pour plus de 30% d'entre eux.

b. Des intérêts et un consensus communs

Si le caractère multi-juridictionnel du réseau rend indispensable une alliance des États pour faire face à la menace, ce n'est pas le seul point d'intérêt commun. La mise en place d'une coopération peut également permettre de réaliser des économies d'échelle en termes de coûts et de ressources par la mutualisation des efforts. La coopération constitue dès lors pour les États une économie conséquente en particulier dans le contexte économique et financier actuel. La sécurité des systèmes d'information (SSI) est un domaine pour lequel les investissements financiers et humains doivent être substantiels et continus. Ces efforts conséquents pourraient dès lors constituer un frein pour les États dans le contexte de crise économique et de réduction des dépenses des années 2010. Pourtant le secteur de la SSI a vu chaque année ses ressources augmenter dans de nombreux pays. Témoignant de la prise de conscience politique des enjeux de la SSI, l'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information a vu ses ressources financières et humaines augmenter considérablement passant d'un budget de 75 millions d'euros en 2010 pour 170 d'agents à un budget de 90 millions d'euros et 250 agents en 2012.

[3] Source : Statistiques de l'Union Internationale des Télécommunications

[4] Source : Threat Expert – Geographic Distribution of Threats http://www.threatexpert.com/ consulté le 30 septembre 2012

[5] Les attaques par déni de service visent à rendre indisponible, durant une certaine période, l'accès aux services ou ressources d'un serveur cible. Il s'agit d'attaquer les machines et serveurs d'une entreprise ou d'un gouvernement afin de les rendre inaccessibles aux utilisateurs légitimes et usuels. Cette attaque peut être conduite depuis une source unique ou utiliser de nombreux ordinateurs, le plus souvent à l'insu des utilisateurs légitimes. On parle alors de déni de service distribué. (Source : BOYER B., 2012, Cyberstratégie – L'art de la guerre numérique, Nuvis, Paris)

[6] Source : Blog SourceFire http://blog.sourcefire.com/2012/08/the-race-against-risk-2-both-sides-of.html consulté le 27 septembre

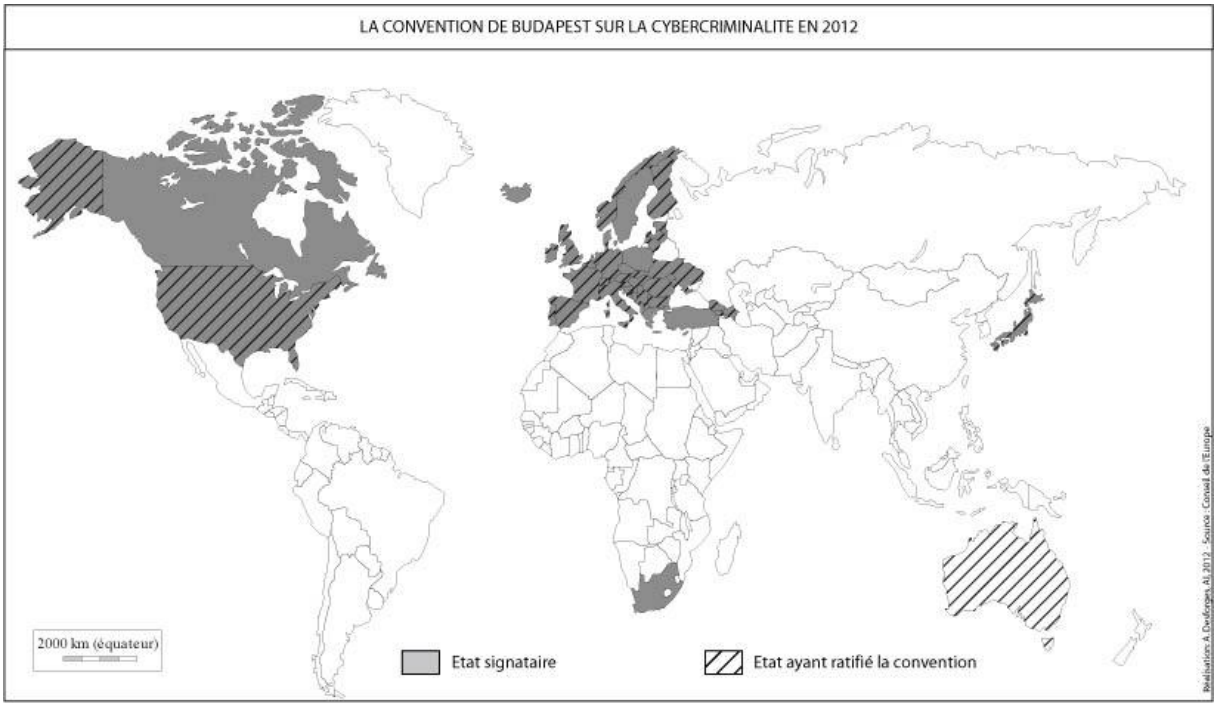
L'ensemble de ces éléments contribuent à faire de la coopération international un véritable enjeu pour les États s'ils veulent voir les menaces se réduire. D'ailleurs la majorité des États s'accordent sur le besoin absolu d'une coopération international sur le sujet. Le récent rapport d'information du Sénat sur la cyberdéfense rappelle d'ailleurs que « *la surveillance des réseaux et la mise au point des réactions en cas d'incident justifie une coopération et une assistance internationales* »[7]. Le dernier somment de l'OTAN soulignait également le besoin d'action commune des Etats : « *Pour faire face aux menaces qui pèsent sur la cybersécurité et pour améliorer notre sécurité commune, nous sommes déterminés à travailler avec les pays partenaires concernés, au cas par cas, et avec des organisations internationales (…) en vue d'accroître la coopération concrète* »[8]. En outre, les enjeux de la coopération sont également débattus au sein des différentes instances internationales (Union Européenne, G8, OCDE etc.). Les déclarations officielles faites dans ce cadre insistent toutes sur la nécessité de coopérer mais la réalité est souvent plus compliquée et la mise en place des mesures de coopération réelles demeure souvent laborieuse.

[7]BOCKEL JM, 2012, Rapport d'information du Sénat - La cyberdéfense : un enjeu mondial, une priorité nationale, p.38
[8]*Ibid*. p.61

II- ETAT DES LIEUX DE LA COOPERATION INTERNATIONALE : UN PROCESSUS SOUVENT SUPERFICIEL

a. La cybercriminalité comme point de départ

En matière de SSI, l'exemple le plus poussé de coopération internationale est sans doute celui de la Convention de Budapest. Sous l'initiative du Conseil de l'Europe, cette convention a été signée en novembre 2001 par vingt six de ses États membres. Le texte pose un cadre de coopération entre les États signataires en matière de lutte contre la cybercriminalité. Elle permet notamment l'harmonisation des législations nationales ainsi que l'amélioration des conditions de coopérations policière et judiciaire. Elle prévoit notamment que les États peuvent au nom de la Convention agir pour le compte d'un autre dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes et de perquisitions transfrontalières, compétences restant ainsi l'apanage des États. Elle couvre également les dispositions en matière d'extradition. Témoignant de l'intérêt pour les États d'encadrer leur démarche de coopération dans leurs efforts dans la lutte contre la cybercriminalité, des États non membres du Conseil de l'Europe se sont investi dans le processus dès ses débuts : l'Afrique du Sud, le Canada, les États-Unis et le Japon. Cependant, si aujourd'hui la convention a été signée par 43 États, seuls 37 d'entre eux l'ont ratifiée et transposée dans leur droit national.



Depuis 2001, les États signataires cherchent à promouvoir cette convention dans le but d'impliquer un maximum d'État dans le processus. Cependant certains pays se sont montrés particulièrement hostile au texte du Conseil de l'Europe. C'est le cas de la Russie qui refuse catégoriquement de signer la convention au motif qu'elle serait contraire à leur droit en violant la Constitution russe. Il est probable que ce refus masque une volonté de protéger une frange des cybercriminels russes, régulièrement accusés d'être à l'origine des attaques. S'ils ne sont pas directement liés au pouvoir, ils semblent toutefois bénéficier d'une certaine bienveillance sinon de laxisme de la part des autorités russes en échange de leur participation à des attaques servant les intérêts du Kremlin.

Cette coopération en matière de cybercriminalité ne doit pas être sous-estimée car les outils et les techniques utilisés pour des motifs criminels sont souvent les mêmes que ceux utilisés dans le cadre d'attaque plus stratégiques.

b. Une coopération internationale qui reste superficielle

Si la Convention de Budapest constitue un exemple de coopération internationale en matière policière et judiciaire impliquant de nombreux États, il semble que la coopération dans les domaines plus stratégiques comme celui de la défense ne jouisse pas du même succès malgré les déclarations d'intention. En effet, les quelques initiatives de coopération multilatérale qui semblent fonctionner et pérenniser sont essentiellement consacrées aux volets de l'alerte et de l'analyse de la menace. Le traitement de celle-ci et la mise en place de réponses restent avant tout du domaine interne aux États.

i. L'ENISA : une coquille vide

L'*European Network Information Security Agency* (ENISA) est l'organisme de l'Union Européenne en charge de la protection des systèmes d'information de l'Union. Il est également chargé d'impulser une politique européenne de SSI, commune aux États membres. Elle intervient auprès des autorités nationales des États membres et des institutions européennes en tant qu'expert en cybersécurité et a pour objectif de faciliter les contacts entre les différentes institutions et les entreprises. Créée en 2004, elle fait partie d'une vague de création d'agences européennes dans le domaine des transports. Contrairement à ses équivalents pour les réseaux de communication ferroviaire et aérien, l'ENISA s'est vu confiée un mandat temporaire de 5 ans et disposait d'effectifs plus restreints que ses cousines. Elle n'a en outre jamais eu un pouvoir de décision contraignant. Longtemps critiquée pour sa bureaucratie, l'agence était soumise aux velléités des États qui avaient déjà mis en place des politiques de SSI. Ils veillaient à la maintenir comme une agence de second plan[9] ne se souciant guère des avis d'une agence européenne perçue avant tout comme une entrave à leur liberté d'action. Le rapport Bockel semble d'ailleurs aujourd'hui regretter le manque de pouvoir de l'agence européenne. Il aspire à une réforme de cette dernière : « *afin d'en faire véritablement un outil de soutien réellement efficace aux États membres* »[10] (recommandation n°40).

ii. Des initiatives « balbutiantes » en matière de cybersécurité et cyberdéfense

Si en matière de cybercriminalité une coopération multilatérale a été mise en place depuis plus d'une dizaine d'années, la question d'une coopération en matière de cybersécurité et cyberdéfense est beaucoup plus récente à l'image de la prise de conscience des enjeux stratégiques de la SSI par les États. L'une des initiatives les plus importantes est la conférence de Londres qui s'est tenue en novembre 2011. A l'initiative du Royaume Uni, cette conférence a rassemblé les représentants de 61 pays ainsi que des organisations internationales (ONU, UE, OTAN) et des représentants de la société civile et de l'industrie[11].

Les débats ont essentiellement porté sur l'instauration de « règles de conduite » dans le cyberespace. Témoignant des enjeux importants soulevés par cette question, les modalités de coopération envisagées semblent exclure, à ce jour, la solution d'un traité international. Les négociations évoquent un mode de coopération plus léger et moins contraignant pour les États, comme le note le rapport d'information du Sénat sur la cyberdéfense de juillet 2012 :

> « *Les discussions se concentrent désormais sur l'idée de promouvoir au niveau international des mesures de confiance ou des « bonnes pratiques », par le biais de mesures non contraignantes, qui comprendraient deux volets :*
>
> - *d'une part, une liste de mesures concrètes, comme l'identification des autorités compétentes pour traiter les attaques visant les systèmes d'information, la mise en place d'échanges d'informations ou des exercices réguliers, voire la constitution d'un réseau au niveau international ;*
> - *d'autre part, un engagement des États à traiter les attaques informatiques transitant par leur territoire »*[12].

[9] Entretien d'Alain ESTERLE, ancien directeur technique de l'ENISA, réalisé par l'auteur le 25 juillet 2012
[10] BOCKEL JM, 2012, Rapport d'information du Sénat - La cyberdéfense : un enjeu mondial, une priorité nationale, p.126
[11] *Ibid*., p.48
[12] *Ibid*. p.54

A ce jour, la définition d'un tel accord est toujours en discussion notamment au sein de l'Organisation des Nations Unies. Il semble exister un vrai clivage entre les États et une résolution de la question paraît encore lointaine. Le rapport du Sénateur Bockel note d'ailleurs les difficultés dans la mise en place d'une coopération internationale qu'il juge « *balbutiante* »[13].

iii. Une coopération essentiellement basée sur l'alerte et l'analyse de menace

Malgré les enjeux et les déclarations d'intention, les différentes initiatives de coopération internationale sur le sujet de la cybersécurité se bornent à de l'échange d'information concernant l'alerte et l'analyse de la menace. Dans ce cadre, la coopération semble être plus ancienne que la Convention de Budapest.

Les CERT (*Computer Emergency Response Team*), organismes certifiés chargés de traiter les incidents sur les systèmes d'information constituent le premier point de contact dans le traitement de la menace. Mis en place par la DARPA dès 1988 dans le but de traiter le premier virus informatique, on compte aujourd'hui 265 CERT répartis dans 57 pays et regroupés au sein du réseau FIRST (*Forum of Incident response and security teams*)[14]. Créée en 1989, cette instance de coopération internationale entre CERT a pour vocation de favoriser les échanges entre les différents CERT répartis à travers le monde dans la prévention, la détection et le traitement des incidents. A ce titre, les CERT constituent un forum d'échange de premier ordre concernant l'alerte et l'analyse des menaces. En outre, le rapport Bockel précise qu'une structure équivalente au niveau européen regroupant spécifiquement les structures gouvernementales a été mise en place. Il s'agit de l'*European Government Computer Security Incident Response Team*. Malgré leur ancienneté et leur présence en première ligne, ces organismes ne sont que peu mentionnés lorsqu'il est question de coopération en matière de cybersécurité. Cela semble témoigner d'une reconnaissance des limites de cette coopération et de l'aveu d'un besoin d'une coopération plus approfondie.

A un niveau plus stratégique et militaire, la coopération multilatérale est également complexe à mettre en place. Suite aux attaques informatiques qui ont secoué l'Estonie en 2007, l'OTAN annonçait la création à Tallinn d'un centre d'excellence de l'OTAN consacré à la cyberdéfense, le *Cooperative Cyber Defence Centre of Excellence* (CCD COE). Le centre qui regroupe onze États membres de l'Alliance atlantique ne compte pourtant pas parmi les organismes de l'OTAN. Il possède le statut d'organisme militaire international depuis 2008, une simple homologation de l'Alliance, qui n'en fait donc pas un centre à vocation opérationnelle. La constitution même de cet organisme en Centre d'Excellence lui confère exclusivement un rôle de centre de recherche et de formation[15].

c. Des initiatives bilatérales privilégiées

Si la coopération internationale en matière de cybersécurité semble complexe à mettre en place et demeure à ce jour encore superficielle, il semble que les États privilégient les collaborations bilatérales. Alors qu'ils se montrent hésitants à mettre en place une coopération internationale, les initiatives de coopérations bilatérales connaissent *a priori* plus de succès, même s'il est souvent difficile d'évaluer les modalités précises de celles-ci. Elles semblent toutefois constituer un cadre privilégié de mise en place de coopération entre États sur les questions de cybersécurité.

Ainsi la France, par le biais de l'ANSSI, semble avoir développée une grande proximité avec ses voisins anglais et allemands. La cyberdéfense constitue d'ailleurs l'un des domaines de coopérations évoqués dans les accords de défense entre la France et la Grande Bretagne. Les modalités précises de ces accords ne sont pas connues. Cependant certaines sources évoquent la volonté de « *renforcer la résilience des (deux) systèmes nationaux et*

[13]BOCKEL JM, 2012, Rapport d'information du Sénat - La cyberdéfense : un enjeu mondial, une priorité nationale, p.53

[14]Source : www.first.org – consulté le 26 septembre 2012

[15]Source : OTAN

communs »[16]. L'ANSSI entretient également des liens très étroits avec son équivalent allemand le BSI (*Bundesamt für Sicherheit in des Informationstechnik)*, même si, une nouvelle fois, il est difficile d'en connaitre l'importance et la portée. Le rapport Bockel évoque notamment des participations lors d'exercice de gestion de crise mais ouvre également la voie à une coopération en matière industrielle. L'enjeu serait de créer une base industrielle commune dans le domaine de la cybersécurité notamment pour des raisons stratégiques. Secteur à forte valeur ajoutée, le développement d'une industrie de cybersécurité en Europe viserait tout à la production de produits de sécurité dont la chaine de fabrication serait entièrement maîtrisée par les pays européens. Il s'agit de s'assurer de la sécurité d'un produit dès sa phase de conception.

Il faut noter que l'ensemble des initiatives internationales de coopération dans ce domaine évoquent uniquement un aspect défensif ou de sécurité. La coopération internationale sur les questions offensives est encore plus limitée que sur le volet strictement défensif presque tabou. Peu d'États reconnaissent développer des capacités de lutte informatique offensive (États-Unis, Israël, Japon). Et encore moins reconnaissent les utiliser. Pourtant un contexte précis semble avoir amené deux États à coopérer pour une action ponctuelle : le ver *Stuxnet*. En effet, le journaliste du *New York Times*, David Sanger, affirme que la conception et la diffusion de ce ver visant les infrastructures nucléaires iraniennes résulte d'une action mutuelle des services américains et israéliens. L'objectif du ver étant d'entraver voire d'annihiler le développement du programme nucléaire militaire iranien. Cet exemple semble montrer que sur des projets spécifiques et de façon ponctuelle, des États pourraient coopérer en matière de lutte informatique offensive. D'autres synergies pourraient être mises en évidence et conduire à des initiatives de coopération ponctuelle entre des États.

Si les initiatives de coopération bilatérales semblent aujourd'hui privilégiées par les Etats, on peut néanmoins avancer qu'elles seules constituent un bien faible engagement des Etats vis à vis des enjeux globaux du cyberespace évoqués en première partie. A ce jour, elles semblent pourtant constituer la solution qui offre la coopération la plus avancée. Toutefois, une coopération internationale et multilatérale peut réussir trouver des bases suffisamment solides dans ces accords bilatéraux notamment via la définition de politiques communes.

[16]Source : Source : http://www.bruxelles2.eu/defense-ue/armees-europeennes/les-13-points-de-laccord-franco-britannique-sur-la-defense.html - consulté le 30 septembre 2012

III- LES LIMITES DE LA COOPERATION INTERNATIONALE EN MATIERE DE CYBERSECURITE

L'analyse des actions de coopération internationale et de leurs enjeux mettent en exergue les différents freins à la mise en œuvre d'une coopération approfondie dans le domaine de la cybersécurité et de la cyberdéfense. On en distingue principalement de trois types : ils sont juridiques, politiques et stratégiques. Si les freins juridiques et politiques sont importants, il s'avère que les enjeux stratégiques pour les États constituent la principale entrave à toute initiative de coopération internationale.

a. Les limites juridiques

i. La nature globale du réseau

Si la nature internationale du réseau fait de la coopération internationale une nécessité, elle en constitue également un frein majeur. La problématique de l'attribution des attaques illustre parfaitement les difficultés de mise œuvre d'une coopération internationale. En effet, si pour les acteurs politiques, la question de l'attribution des attaques informatiques est avant tout une question technique ; les techniciens évoquent, eux, comme principale frein à l'identification des criminels, le caractère multi-juridictionnel de l'internet et les difficultés de coopération internationale qu'il induit. Pour certains experts, il serait même possible d'identifier la source pour 80% des attaques informatiques si les acteurs concernés acceptaient de coopérer[17]. Les services de police et de gendarmerie spécialisés de la lutte contre la cybercriminalité sont tous les jours confrontés aux vraies barrières juridiques créées par les frontières. La frontière constitue ainsi souvent une véritable protection pour le cybercriminel qui profite alors des limites de coopération pour poursuivre et développer ses activités illégales.

ii. Des législations nationales trop disparates et des procédures trop longues

Les législations nationales en matière de cybercriminalité et cybersécurité sont particulièrement disparates à travers le monde. La diversité des états d'avancement des législations nationales constitue un facteur supplémentaire dans la difficulté de mise en œuvre d'une coopération.

En outre, les procédures de coopération conjuguées à l'inertie des bureaucraties étatiques entrainent des temps de traitement des dossiers souvent trop longs pour espérer identifier les auteurs d'actes malveillants. Or les preuves numériques sont souvent éphémères. Les différents opérateurs et moteurs de recherche conservent les données de connexion pendant une durée limitée définie par les législations nationales. En France, les fournisseurs d'accès internet doivent conserver ces données pour une durée d'un an.

b. Les limites politiques : des conceptions diverses de la cybersécurité

Les freins politiques sont encore plus décisifs en matière de coopération internationale car, au-delà de l'internet, ils sont le reflet des différentes conceptions étatiques de la sécurité. Les débats autour de la proposition conjointe de la Russie et de la Chine en 2011 sur l'instauration d'un code de conduite dans le cyberespace illustrent parfaitement ces acceptions diverses. La mise en valeur de la liberté d'expression sur l'internet par les représentants des États occidentaux (Union Européenne, Etats-Unis etc.) se voulait être une réponse à l'initiative sino-russe. Le texte proposé par Moscou et Pékin évoque deux éléments distincts. Il met certes en avant la sécurité des systèmes d'information mais y ajoute un volet sur la sécurité de l'information elle-même. Le texte précise que les États devront coopérer pour « *enrayer la diffusion d'informations incitant au terrorisme, séparatisme et extrémisme ou relevant de la stabilité politique, économique et sociale des autres pays ainsi que leur environnement spirituel et culturel* »[18]. L'initiative répond en fait à un double objectif. Le premier objectif relève d'une géopolitique externe à ces pays : apparaître comme une puissance dans le cyberespace et se poser en concurrents des États-Unis. Le second objectif relève lui davantage d'une logique

[17]Entretien de François PAGET, expert chez McAfee, réalisé par l'auteur le 23 août 2012

[18] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, 66ème session, International code of conduct for information security.

géopolitique interne. Il s'agit de garantir l'unité et l'intégrité de ces États qui font face à des velléités séparatistes fortes ainsi qu'une vive opposition au régime en place. Comme le note le rapport du Sénateur Bockel de telles mesures sont « *inacceptables pour la majorité des pays attachés aux principes de la liberté d'expression et de protection de la vie privée* »[19]. Pour Joe Biden, vice-président américain, une telle initiative conduirait exclusivement à un contrôle gouvernemental des ressources de l'internet[20].

Les différentes acceptions de la sécurité sur l'internet s'illustrent également dans les débats relatifs à la définition des termes utilisés pour désigner la menace. Si la cybercriminalité semble avoir trouvé un cadre à peu près accepté par tous, ce n'est pas le cas pour les termes de *cyberguerre*, *cyberespionnage* ou encore *cyberterrorisme.*

Julien Nocetti, chercheur à l'IFRI, résume ces différentes conceptions en ces termes : « *Quand la Chine souhaite rendre Internet « sain », et l'Iran « pur », les États-Unis veulent un web « hygiénique », tandis que la France ambitionne de le « civiliser ».* »[21]

c. Les limites stratégiques : quand les enjeux nationaux annihilent la coopération internationale

i. Renseignement, informations stratégiques et souveraineté

Toute coopération approfondie dans le domaine de la cybersécurité et de la cyberdéfense engage les États à un échange d'informations sur leur environnement (types de systèmes utilisés, mesures de sécurité en vigueur etc.), leur stratégie de défense ainsi que leurs capacités. Or ces éléments constituent autant d'informations qui pourraient être utilisées dans le but de leur nuire. Le cyberespace pose la question d'une redéfinition de l'ennemi. Derrière une ligne de front l'ennemi reste identifiable, mais caché derrière un proxy, il est difficile de déterminer avec assurance qui constitue l'ennemi. Un individu isolé ? Une entité criminelle ou mafieuse ? Un groupe terroriste? Un État ? Ennemi ? Allié ? Témoignant du caractère majeur de cette question, le Livre Blanc sur la Défense et la Sécurité Nationale fait d'ailleurs de la sécurité des systèmes d'informations un enjeu de souveraineté de premier plan au côté de la dissuasion nucléaire, du secteur des missiles balistiques et des sous-marins nucléaires d'attaque.

L'internet ouvre de larges possibilités d'espionnage et de renseignements notamment pour les États mais pas seulement. Et l'utilisation d'informations dispensées par les États de façon volontaire par exemple dans le cadre de coopérations internationales n'est pas à exclure. Ainsi la mise en œuvre d'une coopération internationale résulte d'un difficile compromis entre la nécessité de coopérer à petite échelle pour faire face aux enjeux globaux de l'internet et l'exigence de la sauvegarde de sa propre sécurité. Les États ne semblent aujourd'hui pas prêts à courir le risque de leur propre menace.

Par ailleurs, il n'est pas nécessairement dans l'intérêt des États d'établir des règles internationales contraignantes. Un *status quo* garantit une certaine impunité aux auteurs d'une attaque, y compris lorsque celle-ci est menée par un État.

ii. Au cœur des questions stratégiques : la confiance

Comme évoqué ci-dessus, le principal enjeu pour les États pour la coopération en matière de cybersécurité et cyberdéfense est celui du partage de l'information. Or l'échange et le partage de l'information repose avant tout sur la confiance accordée à son interlocuteur. Les difficultés d'identification formelle de son adversaire posent dès lors un frein décisif à la mise en place d'une coopération entre États. Le rapport du Sénateur Bockel sur la cyberdéfense note d'ailleurs qu' « *il n'existe pas de véritables alliés dans le cyberespace* »[22]. Et combien

[19]BOCKEL JM, 2012, Rapport d'information du Sénat - La cyberdéfense : un enjeu mondial, une priorité nationale, p.53

[20]Source : http://www.huffingtonpost.com/2011/11/02/london-conference-on-cyberspace_n_1071242.html consulté le 26 septembre 2012
[21] NOCETTI J, Introduction au dossier « Internet, outil de puissance », in Politique Etrangère, vol. 77, été 2012, IFRI, p.248
[22] BOCKEL JM, 2012, Rapport d'information du Sénat - La cyberdéfense : un enjeu mondial, une priorité nationale, p.67

même, une confiance absolue est accordée à son interlocuteur, le transfert et la duplication des informations partagées constituent en elles-mêmes un risque supplémentaire de fuite.

Dans un rapport sur les défis du partage de l'information en matière de sécurité de l'information, l'ENISA explique que la confiance ne peut être continue et absolue mais elle constitue néanmoins le point de départ à toute mise en place d'un réseau de partage de l'information[23]. La question de la confiance n'est pas nouvelle en matière de relations internationales. A ce titre, les Etats-Unis ont souhaité relancer l'action de l'Organisation pour la sécurité et la coopération en Europe (OSCE) considérée comme une véritable « *machine à fabriquer de la confiance* » dans la mise en place de coopération en matière de cyberdéfense[24].

[23]ENISA, « Incentives and Challenges for Information Sharing in the Context of Network and Information Security », septembre 2010
[24] BOCKEL JM, 2012, Rapport d'information du Sénat - La cyberdéfense : un enjeu mondial, une priorité nationale, p.56

CONCLUSION

De l'avis général, la coopération internationale est primordiale et absolument nécessaire pour un cyberespace plus sûr tant pour les états que pour leurs citoyens. Cependant les nombreux freins et notamment les enjeux de souveraineté et de sécurité nationale tendent à réduire toute tentative de coopération en une collaboration a minima.

De surcroit, si les États sont des acteurs incontournables dès lors qu'il est question de sécurité, ils ne peuvent l'assurer à eux seuls dans le cyberespace. En effet, ce domaine est avant tout constitué d'acteurs privés (entreprises et société civile) qui ont contribués à le façonner. Le cyberespace et son fonctionnement leur sont en partie soumis. Les entreprises de l'internet et de l'informatique comme Google, Apple ou Microsoft font partis des acteurs qui, de part leur présence mondiale et leur influence, sont capables de mener des réformes importantes sur les pratiques quotidiennes du réseau. Or si la sécurité ne constitue pas forcément pour eux une priorité, ils doivent tout de même être intégrés à ces débats à l'échelle internationale. William Hague, secrétaire d'état aux Affaires Étrangères britanniques invitait d'ailleurs le secteur privé à participer activement auprès des États aux initiatives de coopération : « *Vous devez être nos alliés pour assurer que le cyberespace de demain reste fidèle à sa nature* »[25]. Cependant, l'introduction de ces acteurs dans les débats ne risque-t-elle pas de complexifier davantage la mise en œuvre d'accords de coopération internationale ?

[25] Source : Foreign Secretary's closing remarks at the London Conference on Cyberspace (Foreign and Commonwealth Office) http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=685672482 – consulté le 8 août 2012

BIBLIOGRAPHIE

- ARPAGIAN N., 2010, *La cybersécurité*, Que-sais-je, PUF, Paris
- BOCKEL JM, 2012, Rapport d'information du Sénat - La cyberdéfense : un enjeu mondial, une priorité nationale
- QUEMENER M., FERRY J. et al., 2009, *Cybercriminalité: Défi mondial*, 2ème édition, Economica, Paris
- QUEMENER M., 2008, *Cybermenaces, Entreprises et Internautes*, Economica, Paris
- VAZQUEZ D., ACOSTA O. et al, 2012, « Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships », *4th International Conference on Cyber Conflict*, CCD COE Publications, Tallinn
- VATIS M., 2003, « International cyber-security cooperation – informal bilateral models », Cyber Security – Turning National Solutions into International Cooperation, Center for Strategic and International Studies, Washington