RETEX de la conférence : « *Construire la paix et la sécurité internationales de la société numérique* » (#SecNumConf)

Table des matières

Panel 1 : Prévention des attaques informatiques et protection : qui doit faire quoi ?

Inventio

Karine Bannelier, Université Grenoble-Alpes

Après avoir souligné que le cyberespace est une source de tension importante, elle rappelle que des règles existantes dans le droit international s'appliquent déjà (Jurisprudence de l'Affaire de Corfou, ICJ 1949 ; l'obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats.[1]), c'est le concept de cyber-diligence. Elle explique ensuite que c'est une obligation de faire et non de résultat, qu'on n'attendra pas d'un État en voie de développement les mêmes moyens que ceux que pourrait produire un pays développé. Elle fait un point aussi sur la résolution du conseil de sécurité des Nations en date du 13 Février 2017 portant sur la protection des infrastructures critiques contre les attaques terroristes[2]. Elle explique ensuite l'importance des partenariats public-privé et met un accent sur leur nécessité. Elle finit son discours avec sa proposition de légiférer sur les vulnérabilités Zéro Day (Vulnérabilités qui, lorsqu'elles sont divulguées, aucun correctif n'existe à ce moment).

Claude Kirchner, INRIA

L'intervenant insiste dès les premières minutes de son discours sur l'importance de cette révolution la comparant ainsi à celles de l'écriture et de l'imprimerie. Il s'attarde ensuite sur le fait que le cyberespace est un monde réel, omniprésent et inexploré. Il explique ensuite qu'il y a du bon dans le cyber mais qu'il y a aussi du mauvais. Il explique quels axes de prévention peuvent être envisagés notamment sur l'éducation numérique et le développement de l'interdisciplinarité des recherches. Concernant la protection, il évoque les pistes du chiffrement homomorphe et de la chaîne de blocs, entre autres. Il demande aussi à ce que les procédures de certifications soient réévaluées relativement aux aspects juridiques et/ou techniques. Enfin, il termine avec la notion de responsabilité qu'il voit triple : Une responsabilité Internationale, une collective et une éthique. Il incite les auditeurs à aller contribuer à une initiative de mémoire publique du logiciel nommée Software Heritage [3]!

Elocutio

Nicola Bonucci, OECD

Il commence son discours en rappelant que la cyber sécurité est un point crucial. Il explique après son travail sur le développement de nouveaux indicateurs de cyber sécurité. Puis, poursuit sur l'existence d'un cadre juridique déjà présent sur lequel il n'y a pas de consensus. Il expliquer ensuite sa vision qui est celle d'une équivalence fonctionnelle qui consiste à avoir les mêmes objectifs, mais pas avec les mêmes moyens. Il termine en affirmant qu'il aimerait moins de NATO (No Actions, Talks Only) mais plus d'actions concrètes !

Moctar Yedaly, Union Africaine

Après s'être présenté, l'intervenant nous faire part de sa joie de voir l'Afrique enfin représentée. Il insiste surtout sur la nécessité d'avoir de nouveaux Frameworks et de la définition d'un vocable

[1] http://www.icj-cij.org/docket/files/1/1645.pdf ; Affaire du Détroit de Corfou, Arrêt ICJ 9 Avril 1949, p22
[2] http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2341(2017)
[3] https://www.softwareheritage.org/

commun. Il annonce aussi que l'Union Africaine a adopté la Convention de Malabo du 27 juin 2014[4] préconisant des principes de bonne gestion de la cyber sécurité et des données personnelles.

Francesca Bosco, UNICRI

Après avoir présenté plusieurs études mettant en évidence l'augmentation des attaques, elle insiste plus particulièrement sur le manque d'études sur le nombre d'incidents déclarés en raison d'une culture du secret dans le milieu. Cela complique la compréhension des dommages et des coûts réels résultant de ces attaques. Elle rappelle ensuite des attaques marquantes : Ministère des Affaires étrangères, Ashley Madison, Yahoo. Puis elle expose les challenges : Attribution, développement rapide, l'aspect transnational des attaques et des poursuites. Pour terminer, elle souligne que les attaques informatiques ne se traduisent pas que par vol d'information, mais qu'elles affectent aussi l'image, la réputation et le chiffre d'affaires.

Disputatio

Sergei Boeke, Université de Leiden (Pays Bas) ; Céline Castets-Renard, Université Toulouse Capitole / Institut Universitaire de France ; Fabien Terpan, Sciences-Po Grenoble

Lors des débats plusieurs thèmes sont abordés successivement, que ce soit celui de la cyber sécurité à 3 niveaux : International, national et local ; la réaffirmation de la nécessité d'un vocable commun, l'idée de normaliser et la signature des armes informatiques des États ou encore que le partage d'information ait une limite, celle de la sécurité nationale. Enfin, il fait aparté sur la proposition aux États de la part d'un acteur privé, Microsoft, de normes de sécurité.

Ouverture

Dr Tobias Feakin, Ambassadeur de l'Australie pour les affaires Cyber

L'ambassadeur commence par indiquer la position de l'Australie sur la coopération internationale en expliquant qu'il faudrait davantage de mécanismes de coopération transnationaux. Puis il expose la stratégie de l'Australie et son budget de 230 millions de dollars pour 2017. Il termine sur la nécessité de développer des nouveaux Frameworks et stratégies pour réguler cet espace numérique.

Anatoly Streltsov, Directeur adjoint de l'institut de la sécurité de l'information à Moscou

Il rappelle que les conflits dans le cyberespace sont une chose nouvelle pour les tribunaux internationaux. Il explique ensuite que les Technologies de l'Information et de la Communication ont longtemps été oubliées par les législateurs, que le principe de souveraineté des territoires n'est plus valable dans l'espace numérique du fait que ce monde est intangible. Ensuite, il demande quelles pourraient-être les preuves pour ces conflits, quels peuvent être les témoins, sur quoi s'appuyer pour trancher en faveur d'une ou de l'autre partie ? A cette fin, il se questionne sur la mise en place de processus reconnus internationalement, la définition précise d'une cyberattaque et la normalisation contraignante ou non de ce nouveau champ de bataille. Il pointe aussi l'impartialité contestable de certaines infrastructures d'Internet, plus précisément en exposant le cas de l'ICANN. Il recommande une approche commune de la question mais qui sera adaptable aux différents États. Il recommande fortement une culture du cyber enseignée dès que possible à chaque être acteur du numérique.

[4] http://www.afapdp.org/wp-content/uploads/2014/07/CONV-UA-CYBER-PDP-2014.pdf

Panel 2 : Réponse aux attaques informatiques : qui peut faire quoi ?

Inventio

Théodore Christakis, Université Grenoble-Alpes / Institut Universitaire de France

Après être revenu sur le caractère transnational des attaques informatiques, il détaille les deux possibilités d'attribuer les actes d'un acteur privé à un État et les conditions qui sont nécessaires à cette attribution :

- La première est celle qui consiste à ce que l'État reconnaisse les faits comme siens ou qu'il s'agisse d'actes perpétrés par un tiers sur directives, instructions ou contrôle de l'État.

- La seconde est plus méconnue, il s'agit de l'« obligation pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États. » Cette obligation est d'ailleurs consacrée par l'arrêt du 04 Avril 1949 dite Affaire du Détroit de Corfou par la Cour Internationale de Justice. Il y a des conditions à cette responsabilité : L'État ne peut être tenu responsable que s'il a manqué à une de ses obligations de notification (dès que l'État a connaissance de l'attaque, il doit informer), de vigilance (prévention, protection, surveillance) et de réponse (l'État doit essayer de mettre un terme à l'attaque).

Il est donc possible d'imputer une responsabilité des faits d'un tiers à un État seulement sous de strictes conditions. Puis, il développe les réactions qui peuvent être entreprises en l'absence de violation du Droit International par un autre État et les réactions qui peuvent être utilisées en cas de violation du Droit International par un autre État. L'élément clé est qu'il n'est pas nécessaire à un État de prouver qu'il y a eu attaque pour réagir. Il alerte aussi sur le fait que ce soit des acteurs privés qui attribuent maintenant les attaques et que cela pose un problème diplomatique avec tous les risques d'escalade indus. Tous les éléments de son intervention sont tirés de son étude[5] que je vous invite à lire.

Claude Castellucia, INRIA

Après avoir rappelé l'importance des TIC dans notre écosystème actuel, il attire notre attention sur les pratiques de Hack-back[6] mais surtout sur le côté primordial de la défense, qu'il vaut mieux se doter de capacités défensives qu'offensives. Enfin, il demande à ce que les informations soient plus partagées et qu'augmente les mécanismes de coopération internationale dans ce domaine.

Elocutio

Ken Hu, Membre du conseil d'administration de Huawei®

Après avoir présenté la dernière innovation technologique de chez Huawei, la 5G, il explique que le futur c'est un monde tout connecté, tout le temps. Il pointe donc les nouveaux problèmes qui émergent de ce nouveau monde tout connecté comme l'augmentation de la surface d'attaque de l'entreprise et l'augmentation des vulnérabilités et des divulgations de données des entreprises. Il résume tout cela par une expression « Toute médaille a son revers ». Il donne son opinion sur la sécurité et à quel niveau elle doit être mise en œuvre, préférant une gouvernance au niveau de l'exécutif des entreprises. Il revient sur la création en 2010 d'un comité de sécurité global chez Huawei, comité qui a le pouvoir de bloquer la sortie des produits si ces derniers ne sont pas conformes aux exigences internes de Huawei. Il explique la position de Huawei sur l'intégration de la sécurité dès la

[5] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988

[6] Action qui consiste après la survenance d'une attaque informatique à contre-attaquer informatiquement l'attaquant.

conception du produit et le mécanisme de vérification indépendant de leurs produits, notamment l'évaluation de la sécurité chez les fournisseurs du fabricant. Il dit ensuite que la sécurité informatique est un critère de recrutement des équipes travaillant au sein de Huawei. Sur le côté coopération, il indique travailler avec les gouvernements mais veut plus de coopération notamment pour les aider à diriger des standards de sécurité unifiés, rappelant ici la nécessité de travailler ensemble et non chacun de son côté en mettant l'accent sur l'exemple Français. Enfin, il annonce que Huawei investit dans des projets à sources ouvertes et incite d'autres entreprises et gouvernements à faire de même.

Scott Charney, Membre du conseil d'administration de Microsoft®

Il évoque tout d'abord la militarisation de l'espace numérique. Depuis qu'internet est devenu un champ de bataille où se livrent des affrontements numériques mais qui ont des incidences sur le monde physique, il tire la sonnette d'alarme en tenant compte de l'augmentation des attaques dites destructrices, ce qui ne présage rien de bon pour la suite. Il alerte ensuite sur l'acquisition d'armes informatiques destructrices par des pays et des groupuscules en énonçant le sabotage du programme nucléaire iranien, qui a pour objectif de se doter de l'arme atomique et qui a été retardé par le logiciel malveillant Stuxnet[7]. Puis il dit que si nous devons nous entretuer, faisons-le de manière civilisée. Pour cela, il propose trois types de normes :

- Défensives : les gouvernements sont d'accords sur le principe d'une défense commune
- Offensives : les gouvernements se restreignent d'eux-mêmes sur l'usage des armes numériques
- Industrielles : par l'édiction de normes de sécurité contraignantes pour l'industrie sur la sécurité du numérique.

Puis il évoque la position de Microsoft® sur le chiffrement, l'entreprise veut du chiffrement très fort, il insistera sur ce point-là. Il veut aussi que les gouvernements signent leurs armes numériques en temps de guerre. Il pose ensuite la question à qui incombe la charge de la preuve et de la difficulté d'attribution. Il militera ensuite sur la création d'une agence internationale des crimes et délits dans le cyberespace. Enfin, il pense que l'usage des armes numériques sera à l'origine de leur processus d'interdiction.

Disputatio

Sarah Heathcote, Université Nationale d'Australie

Elle rappellera que le hack-back unilatéral non-réglementé est interdit. Que seul l'État est en droit de riposter et seulement sous certaines conditions, elle citera l'État de nécessité pour étayer sa démonstration.

Nicolas Tsagourias, Université de Sheffield

Il exposera rapidement que les contremesures sont différentes de l'auto-défense et quels sont les buts politiques et juridiques d'attribuer une attaque. Il posera aussi la question à qui revient la charge de la preuve et dans quelle dimension le secret et la confidentialité ont des conséquences sur celle-ci. Il expliquera que s'il doit y avoir hack-back, il faut qu'il soit proportionnel et qu'il y aura sûrement des dommages collatéraux, rappelant par la même occasion la nécessité de réduire au maximum ces derniers. Il demandera aussi à ce que soit défini le caractère imminent d'une attaque.

[7] Stuxnet est un ver informatique découvert en 2010 qui aurait été conçu par la NSA en collaboration avec l'unité 8200 pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. (Wikipédia)

Liis Vihul, NATO Cooperative Cyber Defence Centre of Excellence

Elle déclare qu'on se pose beaucoup trop de questions inutiles ou futiles et qu'il vaudrait mieux se recentrer sur des questions plus techniques et concrètes. Elle explique aussi la situation dans laquelle sont actuellement les organisations internationales comme l'UNESCO qui ne peuvent pas dire quelles sont attaquées au niveau international. Elle incite à protéger les fonctions clés d'internet en citant le DNS. Enfin, elle réaffirme qu'il faut renforcer les droits humains et ceux de la vie privée et mieux les respecter.

Ouverture

David Martinon, Ambassadeur français de la Cyber diplomatie et de l'économie numérique

Tout d'abord, il explique que nous ne pouvons pas parler de relents de la guerre froide car nous sommes dans une situation où il y a plus que deux parties qui s'affrontent dans le cyberespace avec notamment la présence d'acteurs non-étatiques qui sont parfois bien plus puissants que les États eux-mêmes. Il rappelle que jusqu'à récemment les attaques informatiques consistaient essentiellement à des défacement de sites internet. Il met ensuite un accent à expliquer la difficulté pour un État d'imputer une attaque informatique à un autre État car ce dernier passe par des tiers ou des proxies pour mener des campagnes d'attaques numériques. Il confirme la position de la France sur la réponse à ces attaques d'un nouveau genre en expliquant que celle-ci pourra être faite en utilisant les moyens informatiques comme les moyens traditionnels. Il croît au concept de cyber-diligence et affirme qu'il sera la base pour créer une chaîne de responsabilité et des normes de comportement. Il pointe aussi le manque d'enthousiasme de certains États qui craignent de freiner les avancées technologique et l'innovation dans ce domaine en légiférant. Enfin, il expose la position de la France sur les pratiques de Hack-back qui sont interdites actuellement du fait de leur potentiel hautement déstabilisateur sur la diplomatie en mettant un accent sur le projet de légalisation de Hack-back des USA nommé AC-DC pour « Active Cyber Defense Certainty Act [8] ».

Panel 3 : Gouvernance et régulation de la sécurité numérique : quel rôle pour chacun ?

Inventio

Nicolas Tsagourias, Université de Sheffield

Il commence par exposer l'état actuel du modèle de cyberdéfense où c'est les acteurs privés qui attribuent les attaques. Puis, il explicite le caractère contraignant de la résolution du conseil de sécurité des Nations Unies. Il s'interroge aussi sur la nécessité d'avoir une organisation internationale pour s'occuper de ces problèmes. Pour s'occuper du rôle des acteurs privés, il voit trois solutions qui peuvent être envisagées :

- Les acteurs privés régulent le marché et font leurs normes.
- Les acteurs privés sont consultés pour l'établissement des normes par les États.
- Les États légifèrent et forcent les acteurs privés à appliquer les normes étatiques.

[8] https://tomgraves.house.gov/uploadedfiles/discussion_draft_ac-dc_act.pdf

Kavé Salamatian, Université de Savoie Mont Blanc

Il débute son discours sur la difficulté qu'a connu le domaine pour financer les recherches, arguant que ces dernières tenaient la plupart du temps de bidouilles académiques. Il se remémore ensuite que France Telecom avait banni le mot IP et que l'Internet japonais a été déployé par une association à ses débuts. Le retard d'intérêt des Etats fait que ces derniers ont peu d'autorité sur ce moyen de communication. Il explique ensuite les cycles de centralisation / décentralisation successifs que connaît Internet et de la durée moyenne de ces cycles qui s'amenuisent, les dernières mesures donnant trois ans pour un cycle total. Il revient sur le fait qu'actuellement nous observons des changements mais que nous ne comprenons pas les nouvelles règles qui se développent avec eux. Enfin, il donne les thèmes des nouveaux chantiers dans le domaine du numérique qui sont les défis de demain : éthique du Big Data et le transhumanisme

Elocutio

Richard Stallman, Président-bénévole de la Free Software Foundation

Il commence par critiquer les médias véhiculant une mauvaise image du hacker du fait qu'ils font l'amalgame entre Crackers et Hackers. Il s'en prend ensuite aux créateurs de base de données en expliquant les différents abus qui peuvent être fait de ces dernières par l'organisation détentrice de la base, par des personnes malveillantes dans l'entreprise, par des agences de renseignement et par les crackers. Il s'élèves contre les lois qui sont passées dernièrement dans le monde qui autorise nombre de violation de la vie privée au nom de la sécurité et de la lutte contre le terrorisme. Il alerte l'assistance sur les dangers du tout connecté et de la surveillance des masses qu'il dénonce également et demande à ce que l'État soit limité dans les données qu'il peut collecter. Il dénonce ensuite la compromission de la chaîne d'approvisionnement des États-Unis et de la Chine. Il donne sa vision d'une cyberattaque qui serait la prise de contrôle de votre système à votre insu, taclant au passage Microsoft et Apple, allant jusqu'à qualifier les deux fournisseurs de système d'exploitation de cyber malveillants. Il rappelle aux utilisateurs de bien lire le Contrat de Licence Utilisateur Final de chaque logiciel utilisé. Il dénonce ensuite l'apprentissage des technologies de l'information et de la communication au plus jeunes via des tablettes aux systèmes propriétaire et la gestion des données personnelles des enfants en considérant les tablettes comme des dispositifs d'espionnage. Enfin, il s'alarme que la censure prenne chaque jour plus de place dans le numérique et que cela attente à nos droits fondamentaux.

Dan Shefet, Président de Association for Accountability and Internet Democracy

Après avoir présenté son association et ses membres, il dit qu'il faut que tous les acteurs, privés comme publics, rendent des comptes. Après avoir insisté sur la nécessité d'avoir des obligations juridiques contraignantes, il pense que les fournisseurs d'accès à Internet sont les mieux placés pour mettre en place des mesures contre la cyber malveillance. Pour lui, il ne fait aucun doute que le consommateur est manipulé par astroturfing[9]. Il milite pour la création d'un médiateur Internet qui ne pourra être saisi uniquement par les acteurs privés et l'idée d'une immunité si celui-ci respecte la décision du médiateur, sinon il perd son immunité et devient justiciable. Enfin, il demande la création d'une COP21 du Numérique et la création d'une liste des paradis numériques.

[9] L'astroturfing désigne une technique de propagande utilisée à des fins publicitaires ou politiques ou encore dans les campagnes de relations publiques, qui ont pour but de donner une fausse impression d'un comportement spontané ou d'une opinion populaire. Elle consiste à simuler un mouvement citoyen, venu de la base. (Wikipédia)

Ingolf Pernice, fondateur de l'Institut Alexander von Humboldt pour l'Internet et la Société

Il prône une gouvernance partagée et régie par des règles reconnues internationalement. Il rappelle que la gouvernance c'est une forme de coopération et qu'il faut intégrer les acteurs privés dans celle-ci. Il pointe le succès des organisations internationales comme l'IETF, l'ISO, IGF, UIT et Tallinn 2.0. Il pense qu'on peut réagir aux cyberattaques par la défense ou même le Hack-back mais pas tant qu'on n'a pas attribué les attaques, sinon c'est une non-solution avec tous les risquent qui peuvent en découler. Enfin, il interpelle sur la nécessité d'utiliser des solutions résilientes face aux nouvelles menaces.

Kim Aumonier, Membre de Peace Brigades International

Elle explique l'opportunité que présente le numérique pour faire connaître leur cause. Quel voit aussi les dangers qui viennent de ce nouveau moyen de communication notamment contre l'intégrité physique et psychologiques des lanceurs d'alertes. Elle milite pour des outils de chiffrement forts pour défendre le secret des communications des défenseurs. Elle demande aussi à ce qu'on garantisse la sécurité des ONG car si les lanceurs d'alerte ne peuvent pas avoir confiance dans les ONG, alors ils ne feront pas confiance aux représentants de ces dernières.

Disputatio

Frédérick Douzet, Université Paris 8 / Chaire Castex

Elle rappelle que la sécurité est une prérogative régalienne des États mais que les acteurs privés sont de nouvelles puissances émergentes. Elle demande une vraie coopération entre les États, les chercheurs et les acteurs privés. Pour elle, la solution se trouverait entre les acteurs privés et les chercheurs car ils ont intérêt à ce que tout le monde se fasse confiance. Elle voudrait qu'on définisse ce qu'est une cyberattaque et quelles sont les infrastructures critiques à protéger. Enfin, elle demande une vraie diversité dans les groupes de discussion sur ces questions.

Théodore Christakis, Université Grenoble-Alpes / Institut Universitaire de France

Il rappelle tout d'abord que les États ont pris beaucoup trop de temps avant de se saisir de la question cyber et de réglementer le cyberespace. Il pense que nous avons besoin de lois peu voire non-contraignantes et d'une coopération internationale entre les acteurs privés et publics afin de créer et diriger la cyber paix.

Pål Wrange, Université de Stockholm

Il croît que pour qu'il existe la paix dans le cyberespace, il faut que tout le monde s'y attelle mais l'échange sera sûrement perdant-perdant et c'est là que réside la difficulté. Il explique aussi que malgré l'écriture de d'une version 2.0 du Manuel de Tallinn, celui-ci n'a que peu de légitimité au niveau politique.

Le rôle des États : deux points de vue

Qi XiaoXia, Directrice générale du Bureau de Coopération Internationale, Cyberspace Administration of China

Après avoir exposé les principaux points de la Stratégie Internationale de Coopération dans le Cyberespace de la Chine[10], elle détaille les mesures chinoises pour le cyberespace :

- Renforcement des protections des infrastructures sensibles

[10] http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

- Combattre la cyber criminalité
- Augmenter le niveau d'information à la cyber sécurité des chinois en créant une semaine d'information dédiée
- Lutter contre les biens contrefaits et les violations de droits d'auteurs
- Encourager les publics et les organisations à la gouvernance d'Internet
- Adhérer à un Internet ouvert et transparent

Enfin, elle s'arrête sur trois points clés de la Stratégie Nationale de la Sécurité du Cyberespace Chinois[11] :

- La volonté de paix
- Respect et la garantie de la souveraineté
- Utiliser le cyberespace pour la paix et non la guerre

Guillaume Poupard, Directeur Général de l'Agence Nationale de la Sécurité des Systèmes d'Information

Il commence par dresser un bilan des actions faites par l'ANSSI et remarque que le niveau technique chez les attaquants augmente, il explique qu'il voit de la recherche et du développement chez eux comme chez nous. Il expose ensuite ses craintes sur de possibles attaques par alliance de cause et craint que celle-ci aient lieux au vu de la géopolitique actuelle. Il attire l'attention sur le développement des villes intelligentes connectées et la difficulté qu'il y a à gérer et faire travailler ensemble un nombre considérable d'acteurs différents. Il continue en demandant à ce que les populations comprennent les conséquences et comment le cyber influe-t-il dans leurs vies.

Puis, il revient sur les erreurs qui peuvent être commises lors du processus d'attribution, expliquant que les attaquants cherchent à contrer les techniques de forensique légale. Il alerte aussi sur le fait qu'un pays A pourrait monter le pays B contre le pays C en se faisant passer pour le pays B et expose quelles pourraient-être les conséquences d'une telle cybercrise internationale. Il rappelle aussi que la diffusion des codes sources de logiciels malveillants une fois ces derniers utilisés est un bon moyen pour brouiller les pistes et donc rendre plus pénible voire impossible une attribution, c'est pourquoi actuellement la France n'a pas attribué d'attaque. Il pense que le numérique n'a pas vocation à remettre en cause le rôle de l'État.

Concernant le Hack-back, il donne la position de la France et explique qu'il n'y a actuellement que des agents de l'État Français qui sont autorisés à en user. Il est pour un armement avec des capacités offensives mais elles doivent aller avec une doctrine, une éthique et un usage raisonné de cette nouvelle force de frappe.

Il explique ensuite pourquoi en France l'ANSSI et les services de renseignement sont différenciés car pour lui il est important que les acteurs tiers puissent faire confiance à une structure qui ne les espionne pas en retour. En cela, la position de l'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale et ne dépend d'aucun ministère, ce qui laisse la latitude nécessaire à l'agence pour mener à bien ses missions.

Il croît très fort dans un chiffrement robuste car c'est un outil de paix et s'alarme de la volonté des États de vouloir le limiter car cela pourrait fragiliser la défense mais aussi l'économie numérique. Il rappelle par la même occasion la nécessité de former les populations au numérique et à la cyber

[11] https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

sécurité afin que les bonnes pratiques soient connues et respectées, arguant au passage que l'ANSSI produit plusieurs documents pour expliquer de manière simple et rapide celles-ci.

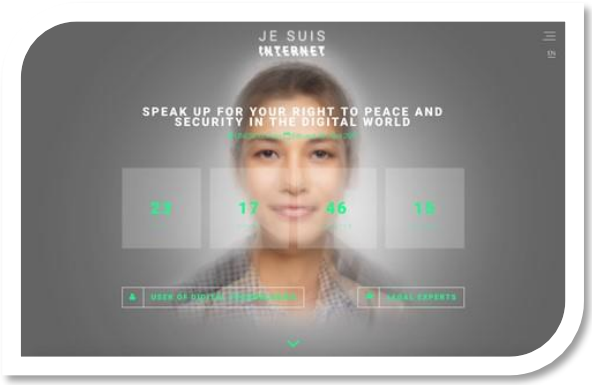
Au final, le constat est unanime, on voit une augmentation de la menace et un gros déficit de normes encadrant le cyber. Il conclue par expliquer le changement de paradigme pour le cyberespace où traditionnellement on considère que l'attaque est la meilleure défense, alors que dans ce nouveau monde numérique, la meilleure défense c'est la défense !

Conclusion

Louis Gautier, Secrétaire général de la défense et de la sécurité nationale

Après avoir rappelé l'importance d'avoir un tel débat et salué l'UNESCO de bien avoir voulu accueillir cette conférence, il explique que la mise en place d'un droit international n'a rien d'aisé dans un système traditionnellement constitué et organisé par des acteurs du secteur privé. Il salue ensuite l'ensembles des intervenants des deux jours de discussions et donne rendez-vous à l'assistance dans deux ans pour la suite des débats.

L'initiative JeSuisInternet.today



C'est une plateforme mise à disposition, traduite ne 11 langues, qui permet à tous de s'exprimer sur les sujets débattus dans les deux jours de conférences. A travers deux parcours, expert légal et utilisateur du numérique, vous êtes invité à répondre à ces questions. Une vidéo d'un intervenant est disponible pour expliquer plus en détails quelles sont les attentes sur chaque question.

Parcours Utilisateur du numérique :

- Quels seraient, d'après vous, les critères permettant d'identifier de manière précise une attaque informatique ?
- Peut-on définir des frontières dans l'espace numérique dans lesquelles seraient applicables les droits nationaux ou ceux définis par les organisations intergouvernementales (protection des données, liberté d'expression, sécurité informatique, etc.) ?
- De quelle manière les entreprises, les ONG et l'ensemble des acteurs peuvent participer à l'élaboration de la paix dans un monde qui se numérise ?
- Est-il nécessaire de créer une nouvelle structure internationale et multi-acteurs dans le domaine du numérique ? Si oui, quels en seraient les missions et moyens ?
- Doit-on accorder aux entreprises, aux ONG et à l'ensemble des acteurs du monde numérique le droit de répondre à une attaque informatique par une autre attaque informatique ?
- Faut-il une « Charte des droits de l'être humain et du citoyen dans le monde numérique » ? Quels seraient les grands principes de cette Charte ?

Parcours Expert légal :

- Quelle place accorder aux acteurs privés dans l'élaboration d'un cadre normatif applicable au cyberespace, à l'échelle nationale et à l'échelle internationale ?
- Quel est/devrait être le rôle des organisations internationales existantes dans le domaine de la sécurité du numérique ?
- Comment universaliser les normes agréées dans le cadre du GGE ?
- Est-il nécessaire de créer une nouvelle structure inter-gouvernementale ou multi-acteurs dans ce domaine ?
- Quelles mesures les Etats devraient-ils adopter en matière de sécurité de l'espace numérique afin d'éviter les actes malveillants affectant les droits d'autres Etats ?
- Les acteurs privés peuvent-ils unilatéralement déclencher des mesures de « cyber-défense active » ?

Pour contribuer, vous pouvez cliquer sur ce lien ou vous rendre sur la page en entrant l'adresse suivante : https://jesuisinternet.today/

A propos de l'auteur

Professionnel de la sécurité informatique, passionné par tout ce qui touche directement et indirectement à ce domaine : Législations (nationales et internationales), logiciels malveillants, actualités, vie privée, géopolitique, etc.

@SwitHak