DGRIS
Direction générale des relations internationales et de la stratégie
MINISTÈRE DE LA DÉFENSE

ETUDE PROSPECTIVE ET STRATEGIQUE

DESCRIPTION DE LA MANIERE DONT LA CYBERCRIMINALITE ET LA LUTTE INFORMATIQUE SONT ABORDEES PAR LES ACTEURS POUVANT INFLUENCER LE DOMAINE

Mars 2015

N° 2014 1050029622 – EJ court 1505280001

Compagnie européenne d'intelligence stratégique
CEIS

Le ministère de la Défense fait régulièrement appel à des études externalisées auprès d'instituts de recherche privés, selon une approche géographique ou sectorielle, visant à compléter son expertise interne. Ces relations contractuelles s'inscrivent dans le développement de la démarche prospective de défense qui, comme le souligne le dernier Livre blanc sur la défense et la sécurité nationale, « *doit pouvoir s'appuyer sur une réflexion stratégique indépendante, pluridisciplinaire, originale, intégrant la recherche universitaire comme celle des instituts spécialisés* ».

Une grande partie de ces études sont rendues publiques et mises à disposition sur le site du ministère de la Défense. Dans le cas d'une étude publiée de manière parcellaire, la Direction générale des relations internationales et de la stratégie peut être contactée pour plus d'informations.

AVERTISSEMENT : Les propos énoncés dans les études et observatoires ne sauraient engager la responsabilité de la Direction générale des relations internationales et de la stratégie ou de l'organisme pilote de l'étude, pas plus qu'ils ne reflètent une prise de position officielle du ministère de la Défense.

ceis

Description de la manière dont la cybercriminalité et la lutte informatique sont abordées par les acteurs pouvant influencer le domaine

EPS n°2013-36

EPS 2013-36

Mars 2015

Table des matières

Introduction

1.1. Le contexte

Devenues aujourd'hui des thèmes « grand public », la lutte contre la cybercriminalité et la cyberdéfense suscite les réactions de plusieurs catégories d'acteurs. Qu'il s'agisse de la société civile (représentée par les particuliers, mais aussi les ONG et associations se réclamant de la défense des droits de l'Homme, ainsi que les hacktivistes et hackers) ou des acteurs du tissu économique, tous prennent position sur les sujets façonnant l'actualité et souhaitent influencer les politiques engagées par les Etats.

Comment appréhender avec le recul nécessaire le flot d'annonces officielles et non officielles issues d'acteurs étatiques ? Quels ***enseignements*** *tirer de ces annonces* ***sur les concepts et doctrines*** *des pays en question ? Ces déclarations sont-elles annonciatrices de risques majeurs, ou surfent-elles uniquement sur un effet d'annonce dissuasif ?*

1.2. Les objectifs

Objectif : Comprendre comment seraient traitées d'éventuelles attaques informatiques avec les conséquences envisageables en matière de ripostes.

L'étude a pour objectif de fournir au ministère de la Défense les moyens d'appréhender les différentes postures des acteurs prenant part au débat sur le cyberespace et les affrontements qui s'y déroulent. Au travers des différentes annonces et déclarations des différents acteurs impliqués (autorités constituées, monde politique, société civile, milieu économique), il s'agit avant tout d'analyser la perception que ces acteurs ont du sujet et leur capacité d'influence respective. Pour nombre d'entre elles, ces déclarations s'inscrivent en effet dans une démarche plus globale de **guerre psychologique** ou de guerre de l'information, visant différents objectifs : justifier et faire accepter par les opinions publiques l'éventualité de conflits dans le cyberespace, contribuer à la stratégie de dissuasion « floue » développée par les Etats, développer au sein des populations nationales une nouvelle forme de citoyenneté et d'enracinement patriotique…

Pour répondre à cette question, il est nécessaire de disposer de plusieurs éléments :

- Quelle est la posture officielle du pays ou de l'organisation ?
- Comment communique-t-il dessus ?
- Comment la perçoivent les acteurs tiers ?
- Quels facteurs ou critères ont pu influencer par le passé les postures des uns et des autres, dans des situations similaires ?
- Quelles sont les perspectives d'évolution de ces facteurs ?
- Est-il possible de conjuguer :
    - Posture des Etats ;
    - Réactions effectives des Etats face aux cyberattaques ;
    - Influence des acteurs tiers sur ces réactions étatiques ;

- Et, en dernier lieu, une liste des facteurs « leviers » pouvant influencer l'issue de chaque scénario ?

1.3. La méthodologie

Pour réaliser cette étude et répondre à ces questions, nous procédons en trois étapes.

1.3.1. Etape 1, l'échantillonnage

Cet échantillonnage a pour objectif de disposer d'une base de données suffisante afin d'identifier les positions de chaque acteur dans des situations passées, proches de celles que nous souhaitons anticiper.

Afin d'offrir l'exhaustivité et le recul nécessaire, l'étude s'appuiera sur une démarche structurée de recueil d'informations auprès d'un panel d'acteurs et de sources d'information représentatifs. Il s'agira ainsi de confronter les postures officielles avec celles d'autres acteurs (société civile, monde politique, milieux économiques), d'analyser les interactions entre chacun de ces acteurs et leur capacité d'influence respective.

1.3.2. Etape 2, l'identification des arguments, leviers et facteurs d'influence

Mais la transposition pure et simple de ces réactions ne suffit pas. Il faut également identifier les éléments de contexte ainsi que les rôles des acteurs tiers, voir comment ils sont susceptibles d'évoluer dans le temps – en fonction des intérêts, rapports de force ou des opinions publiques -, et les intégrer aux scénarios afin de rendre ces derniers plus réalistes.

1.3.3. Etape 3, l'évaluation des risques et des conséquences de la LIO

En dernier lieu, il sera possible d'envisager les risques et les conséquences d'une action offensive de la part d'un Etat, en mettant en perspective les postures étatiques actuelles et les facteurs d'influence identifiés.

Partie 1. Etat des lieux des postures

Postures officielles vs. Jeux d'influence

Suite à nos travaux de recherche et d'échantillonnage, nous sommes aujourd'hui en mesure de dresser un panorama des postures des acteurs étatiques sur la problématique de la lutte informatique offensive. L'analyse de quelques évènements jugés structurants met en lumière une stratégie de communication spécifique à chaque Etat, plus ou moins en phase avec la posture officielle de ces derniers. Enfin, il est essentiel de rappeler le rôle qu'ont pu jouer les acteurs tiers. Ont-ils entraîné un changement du message étatique ? Y ont-ils participé ou s'y sont-ils opposés ? Avec succès ou sans écho ? Et, surtout, leur posture influencera-t-elle, en cas de cyberattaque, la gestion, par l'Etat, de la situation de crise ?

Cas d'étude

Certaines affaires sont révélatrices de nombreuses postures étatiques, industrielles, mais aussi hacktivistes ou de la société civile. Ces cas ont pu fédérer tous ces acteurs et susciter chez eux différents types de réactions.

1.1. Daesch et la guerre de l'information

1.1.1. Résumé

La problématique que l'on perçoit chez tous les acteurs, même si la solution donnée n'est pas la même, est le souci de contrer le monopole que détiennent les djihadistes sur les réseaux sociaux et internet.

La société civile se saisit de la question, grâce à un mouvement général de dépréciation des activités du groupe islamiste :

- Soit en condamnant leurs actes via les réseaux sociaux,
- Soit en promouvant la non-diffusion de vidéos ou images publiées par DAESH, comme le préconise par exemple l'opération « #ISISMediaBlackout » ou encore le phénomène « #daeshbags hashtag ».

Ce « Daesh bashing » sur les réseaux sociaux est largement fédérateur.

Du point de vu académique et médiatique, on essaie de comprendre quelles sont les tendances et les stratégies de communication de l'Etat Islamique sur internet. On constate tout d'abord que le groupe s'est doté d'anglophones au sein même de son organisation et que son discours n'est pas le même pour le public occidental que pour le public du Moyen-Orient. Par ailleurs, il existe deux types de communication :

- Le premier est destiné aux potentiels combattants, il vise à recruter de nouveaux membres dans les rangs de DAESH. Ce discours s'adapte aux personnes et pays. Il se base sur l'attrait du combat et de l'idéologie et la mise en valeur de principes (anti-corruption, vie saine et pieuses).

- Le second type de discours s'adresse aux « ennemis », il vise à choquer et instaurer un sentiment de terreur.

D'un point de vue étatique, on constate un renforcement global du système législatif, pour donner les outils pour une plus grande surveillance sur internet. Par ailleurs, des campagnes anti-radicalisation sont initiées pour sensibiliser les jeunes et contrer les campagnes de recrutement des groupes djihadistes.

Le gouvernement irakien a décidé le blocage de la majorité des réseaux sociaux pendant plusieurs jours. Les Etats-Unis, le Canada, le Royaume-Uni et la France ont tous décidé le renforcement de leurs dispositifs de sécurité sur l'internet. Il s'agit de mesures en partie « d'affiche » car la plupart disposait déjà de systèmes de surveillance sur internet très poussés. Par ailleurs les gouvernements mettent en place des plateformes de « contre-propagande » ou bien, effectue des campagnes de désinformation contre DAESH.

En parallèle de ces actions étatiques, les Etats demandent une plus grande responsabilisation des acteurs industriels et de la société civile. Les entreprises sont appelées à améliorer leur sécurité, les individus sont appelés à dénoncer tout comportement considéré comme suspect.

Du point de vue du secteur industriel, on constate une tendance modératrice. Si la stratégie de communication de DAESH est perçue comme très efficace et dangereuse, on refuse de parler de « cyberguerre » et l'on considère que la majorité des hackers du groupe sont des « skrip skiddies ». Par ailleurs, les réactions législatives sont estimées non adaptées.

1.1.2. Focus sur les réactions

Pays	Date	Acteur	Type d'acteur	Source	Traduction/Résumé FR
	mai2014	Quilliam trending, think tank spécialisé dans le contre-terrorisme	Acteur Académique	http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf p. 120	Il est important d'identifier les faiblesses et les incohérences des récits des extrémistes pour finalement les exploiter contre eux. Les initiatives de contre-extrémisme devraient chercher à renverser le monopole que détiennent actuellement les extrémistes sur certains sujets afin de rendre l'idéologie "démodée". Le défi de la lutte contre l'extrémisme devrait être un effort conjoint entre le secteur public, privé et le secteur des services.
	17 juin 2014	Erin Marie Saltman, journaliste	Presse	http://www.independent.co.uk/voices/comment/isis-have-used-social-media-to-wreak-havoc-in-iraq-and-syria-but-we-can-stop-them-9542838.html	Les mesures négatives (telles que le blocage, la censure ou de filtrer les comptes djihadistes) sont peu efficaces pour remédier au problème, s'attaquant souvent au symptôme plutôt qu'à la cause. L'information sur des sites comme Twitter doit être utilisée comme une source essentielle pour la collecte de renseignements. La campagne médiatique d'ISIS est basée sur une propagande trompeuse et une exagération des fausses victoires. Pour cette raison, les gou-

					vernements devraient être transparents et clairs pour expliquer leurs prises de position politiques".
	13 juin 2014	Craig Timberg	Presse	http://www.washingtonpost.com/business/technology/iraq-tries-to-censor-social-media-but-its-success-is-limited/2014/06/13/19e1e918-f325-11e3-bf76-447a5df6411f_story.html	"Bloquer l'accès à Facebook, Twitter et YouTube dans le but de perturber les outils de médias de communication des insurgés est une technique."; "Perdre du terrain physique signifie aussi perdre le contrôle du cyberespace"
	13 juin 2014	Doug Madory, analyste chez Renesys	Industriel	http://www.washingtonpost.com/business/technology/iraq-tries-to-censor-social-media-but-its-success-is-limited/2014/06/13/19e1e918-f325-11e3-bf76-447a5df6411f_story.html	"Cette action fait écho au peu de contrôle que le gouvernement irakien possède sur le pays."
	13 juin 2014	Collin Anderson, chercheur à l'Université de Pennsylvanie	Acteur Académique	http://www.washingtonpost.com/business/technology/iraq-tries-to-censor-social-media-but-its-success-is-limited/2014/06/13/19e1e918-f325-11e3-bf76-447a5df6411f_story.html	En plus des effets sur Facebook, Twitter et YouTube, les interruptions réduisent les accès à WhatsApp et Viber, applications qui fournissent des messageries en temps réel.
	13 juin 2014	Minister of Communication d'Irak	Acteur Etatique	https://twitter.com/CDA/status/477504734115692544	Site internet bloqué par décision du MoC irakien.
	25 juin 2014	J. M. Berger, journaliste chez The Atlantique	Presse	http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/	ISIS utilise les réseaux sociaux pour diffuser des photos violentes, attirer de nouveaux combattants, et d'inciter les loups solitaires. [..]. ISIS possède une légitimité en ligne, mais inférieure à ce qu'il pourrait sembler et il doit beaucoup de ce soutien à une campagne calculée pour humilier les groupes, ou "gourous", marketing américains sur les réseaux sociaux

	26 sept. 2014	Richard A. Stengel, sous-secrétaire d'Etat pour la diplomatie des Etats-Unis	Acteur Etatique	http://www.nytimes.com/2014/09/27/world/middleeast/us-vividly-rebuts-isis-propaganda-on-arab-social-media.html	Nous devons être plus sévères et nous devons riposter, plus particulièrement dans l'espace informationnel.
	31 août 2014	Emerson Brooking, chercheur associé au Council on Foreign Relations	Acteur Académique	http://www.thedailybeast.com/articles/2014/08/31/isis-s-use-of-social-media-to-reach-you-its-new-audience.html	Le premier grand tournant était Mossoul : ISIS a beaucoup misé sur la préplanification de cette offensive sur les réseaux sociaux, et cet effort a été payant. Après Mossoul, on constate un pic important de vidéos et images d'ISIS en anglais."
	31 août 2014	Clint Watts, chercheur au Foreign Policy Research Institute	Acteur Académique	http://www.thedailybeast.com/articles/2014/08/31/isis-s-use-of-social-media-to-reach-you-its-new-audience.html	ISIS a appris comment atteindre le public américain et à le rendre favorable à leur cause.
	31 août 2014	Peter Neumann, directeur du Centre for the Study of Radicalisation at King's College à Londres	Acteur Académique	http://www.thedailybeast.com/articles/2014/08/31/isis-s-use-of-social-media-to-reach-you-its-new-audience.html	"La grande différence est que désormais, ISIS a, dans ses rangs, ses propres anglophones"
	?	Douglas Wade, professeur à l'Université d'Oxford, blogueur	Société civile	http://www.academia.edu/9081141/Daesh_is_losing_the_propaganda_war	"Le vent a tourné de façon décisive contre Daesh dans la guerre des mots, images et discours et les effets sont déjà ressentis par les commandants de Daesh avec la baisse du nombre de nouvelles recrues. L'émergence de phénomènes tels que la tendance #daeshbags hashtag sur Twitter joue: Ces lieux d'échanges servent de moquerie générale contre Daesh et ses followers, et deviennent très populaires."
	04 fév. 2015	#SVURenewed	Société civile	https://twitter.com/search?q=%23ISISMediaBlackout%20&src=typd	Vous voulez faire votre part pour arrêter ISIS? NE PAS diffuser leur propagande. Ou les images de leur cruauté. #ISISMediaBlackout

	12 janv. 2015	Premier Ministre britannique	Acteur Etatique	http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks	"Les agences de renseignements ont besoin de plus de pouvoir" "Les données issues des communications sont cruciales, non pas seulement pour combattre le terrorisme, mais pour identifier des personnes disparues et des meurtriers" " Une législation supplémentaires donnerait accès aux services à un ensemble de communication téléphoniques plus conséquent."
	12 janv. 2015	Simon Hughes, Ministre Lib Dem de la Sécurité au Royaume Uni	Etatique	http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks	Il faut s'accrocher à nos libertés et ne pas les abandonner dans la défense de la nation. C'est le mauvais message à envoyer. Nous n'avons aucune raison de croire qu'augmenter les pouvoirs (des autorités) est nécessaire.
	15 janv. 2015	Gérôme Billois, expert en sécurité informatique au cabinet Solucom et administrateur du Club de la sécurité de l'information français (Clusif).	Acteur Industriel	http://www.francetvinfo.fr/monde/terrorisme-djihadistes/faut-il-craindre-une-cyber-guerre_796909.html	"Ce serait exagéré de parler de "guerre". Aujourd'hui, nous parlons d'actes qui n'ont pas d'effets dans le monde réel. Il n'y a pas d'explosions, pas d'interruptions de services essentiels comme l'énergie ou les transports. Il n'y a pas non plus de pertes humaines. On reste dans le monde virtuel. Il n'existe pas vraiment de mot pour déterminer ces actes.
	16 janv. 2015	Loïc Guezo, expert en sécurité chez Trend Micro	Acteur Industriel	http://www.zdnet.fr/actualites/cyberattaques-en-france-un-succes-de-com-avant-tout-39813119.htm	"C'est très habile, en termes de communication, de la part des attaquants"; "jeunes, voire très jeunes". "Leur profil est plutôt celui de personnes avec des compétences de base, au sens de la gestion du PC et de certains outils"
	19 janv. 2015	ASIC, association d'entreprises technologiques	Acteur Industriel	http://www.wsj.com/articles/france-germany-seek-help-from-tech-firms-in-policing-terrorism-online-1421766194	Les ajouts législatifs récents - certains pas encore en vigueur - dotent la France d'un des plus grands arsenaux juridiques dans le monde. Toute nouvelle loi ou mesure doit respecter les libertés, à la fois publiques et privées.
	20 janv. 2015	Thomas de Maizière, Ministre de l'Intérieur allemand	Etatique	http://www.wsj.com/articles/france-germany-seek-help-from-tech-firms-in-policing-terrorism-online-1421766194	Moins de gens prennent compte de leur responsabilité, plus les législateurs devront prendre d'initiatives.

	28 janv. 2015	Gouvernement français	Acteur Etatique	http://www.education.gouv.fr/cid85796/lancement-du-site-internet-www.stop-djihadisme.gouv.fr.html	"#StopDjihadisme : contre le terrorisme, tous unis et tous vigilants. Découvrez le site dédié >> https://cards.twitter.com/cards/18ce53vx8vu/bek4 ..." ; http://www.stop-djihadisme.gouv.fr/
	04 fév. 2015	Stephen Harper, Premier Ministre canadien	Acteur Etatique	http://www.army-technology.com/news/newscanada-announces-anti-terrorism-legislation-4503736	Notre gouvernement comprend que les djihadistes ont déclaré la guerre aux peuples libres et au peuple canadien en particulier. Le projet de loi vise à fournir à nos agences de sécurité et à la Justice les outils et la modularité dont ils ont besoin, pour ainsi efficacement détecter et perturber les menaces nationales avant qu'elles ne surviennent, en persévérant la sécurité des Canadiens.
	04 fév. 2015	Ministre Candice Bergen	Acteur Etatique	http://www.portageonline.com/index.php?option=com_content&task=view&id=41526&Itemid=662	Cette nouvelle législation va fournir des outils législatifs nécessaires pour protéger le peuple canadien. Notre but n'est pas de combattre le terrorisme sur notre territoire mais aussi à l'extérieur.
	04 fév. 2015	Michael Steinbach, chef de la division spécialisée dans le contre-terrorisme du FBI	Acteur Etatique	http://edition.cnn.com/2015/02/03/politics/fbi-isis-counterterrorism-michael-steinbach/	"Le recrutement des femmes par ISIS est beaucoup plus important que ce que nous avons vu pour toute autre organisation terroriste." Nous avons identifiés de nombreux lieux d'échanges qui appelaient au combat et dont les personnes isolées répondaient favorablement, non exclusivement par des attaques sophistiquées." "Nous ne voulons pas ébranler la liberté d'expression, tout le monde a droit d'exprimer son opinion mais quand cette opinion se transforme en un violent discours puis en action, c'est différent."

1.2. LPM et l'échec de la mobilisation de la société civile

1.2.1. Résumé

Contexte

La loi de programmation militaire (LPM) 2014-2019 a été adoptée en décembre 2013 mais, conformément à la loi, la LPM a fait l'objet d'une révision en décembre 2014. Suites aux attentats contre Charlie Hebdo, il a été évoqué une modification de ces textes dans le but d'augmenter les capacités des autorités, notamment sur internet. Un article en particulier, l'article 20 (anciennement 13) a déclenché une forte polémique. Cet article organise une possibilité de collecte de données en temps réel sur les réseaux des FAI, sans contrôle judiciaire. Cet article est accusé d'entraver la liberté d'expression et la liberté à la vie privée.

Réactions

On constate, au sein des **acteurs étatiques**, des réactions hétérogènes concernant l'article, signes que la mesure ne fait pas entièrement consensus. Le gouvernement actuel observe une certaine réserve. Il insiste sur la nécessité d'un renforcement des mesures de sécurité, le respect de la loi et des engagements pris dans le cadre du vote de la LPM mais a effectué très peu de communications sur l'article 20 en lui-même. Les autorités ont affirmé vouloir prendre des mesures proportionnées et adaptées insistant sur la prévention des crimes, la lutte contre le recrutement et la nécessité d'obtenir ces données.

Du côté de l'opposition, les critiques vont dans des sens contradictoires: certains demandent un « *Patriot Act* à la française » (cf. la loi de renseignement de mars 2015), mettant justement le doigt sur les critiques concernant le document ; d'autres estiment qu'il ne faut pas faire la même erreur que les Etats-Unis. L'opposition politique, si elle s'est effectivement mobilisée pour que la LPM soit soumise au Conseil Constitutionnel, ils n'ont pas réussi à obtenir le minimum requis de personnes (60).

De manière assez unanime, les industriels, la presse, la société civile et les académiques sont opposés au projet.

Du point de vue du **secteur industriel**, c'est surtout le scepticisme sur l'utilité de la mesure qui prime. La France disposant déjà d'un arsenal législatif très sévère, le renforcer semble plutôt être un effet d'annonce qui aura un impact négatif sur la population.

La **presse** critique, quant à elle, le processus par lequel la loi a été votée. Certains éléments ont soulignés notamment la non consultation de la CNIL et le vote en procédure accélérée.

La **société civile** poursuit sa mobilisation à l'encontre du texte (e.g. la pétition#StopArt20 adressée au Président du Groupe UMP au Sénat ou encore la campagne #PasEnNotreNom) mais l'on remarque que cette mobilisation se ralentit fortement après le vote de la loi. Certaines associations en revanche comptent déclencher le mécanisme de la question prioritaire de constitutionnalité, ce qui pourrait remettre en cause les dispositions de la loi.

Impact

Le vote de la LPM en l'absence de consultation ni de communication, a alimenté l'opposition déjà existante à l'encontre du texte. L'annonce par le gouvernement de nouvelles mesures pour renforcer la sécurité en ligne accentue l'opposition. De nombreux éléments tels que la non consultation de nombreux acteurs concernés, le manque de clarté sur de nombreux points (e.g. les « documents » et « in-

formations » concernés, le dédommagement des opérateurs de communication recenseraient des données de connexion etc..), ainsi que l'absence de contrôle judiciaire posent problème.

1.2.2. Focus sur les réactions

Pays	Date	Acteur	Type d'acteur	Source	Citation VO
France	08 déc. 2013	Gilles Babinet, Digital champion" auprès de Neelie Kroes	Société civile	http://www.lesechos.fr/08/12/2013/lesechos.fr/0203176354634_gilles-babinet-----nous-sommes-a-deux-doigts-de-la-dictature-numerique--.htm	"Cette loi (art 13 LPM), c'est le plus grand coup porté au fonctionnement de la démocratie depuis les lois d'exceptions pendant la guerre d'Algérie [...] Nous sommes à deux doigts de la dictature numérique."
France	19 déc. 2013	Stéphanie Lamy, participante de la pétition #StopArt20	Société civile	https://www.change.org/p/cap-sur-un-internet-libre-en-2014-stopart20	"Devant la défaillance manifeste de nos représentants, c'est à nous d'exploiter tous les recours démocratiques possibles pour stopper ces atteintes à nos droits au nom du "tout sécuritaire" ; "Signez pour rejoindre le mouvement #StopArt20 !" ; "La loi sur la programmation militaire vient d'être adoptée et avec elle un article controversé instaurant un « *Patriot Act* à la française » qui étend l'accès de l'État à nos données téléphoniques et informatiques, sans l'avis d'un juge."
France	07 août 2014	Fabrice Epelboin, spécialiste des médias et du Web social	Société civile	http://www.lefigaro.fr/vox/monde/2014/08/07/31002-20140807ARTFIG00096-piratage-sur-internet-la-fin-de-la-vie-privee.php	"la simple arrivée de ces technologies de surveillance change radicalement l'équilibre du pouvoir entre les grandes composantes de la démocratie. Ce changement se fait au profit de l'exécutif de façon presque exclusive – le pouvoir judiciaire pouvant avoir recours, de façon très encadrée, aux technologies de surveillance ciblée. Par ailleurs, la population, elle, est la grande perdante en termes de libertés individuelles et, à terme, de libertés publiques."
France	07 sept. 2014	Tyler Durden, correcteur et journaliste	Presse bretonne		"La Stasi en a rêvé, la république française l'a fait. La loi est passée. "

France	11 sept. 2014	Guillaume Poupard, directeur de l'ANSSI	Etatique	http://pro.01net.com/editorial/626682/la-loi-de-programmation-militaire-au-service-de-l-anssi/	" La LPM est un véhicule important pour moderniser nos questions de sécurité avec plusieurs articles qui concernent l'ANSSI [...] Une réaction rapide est obligatoire. L'ANSSI doit avoir un rôle de coordination à froid comme à chaud [...] Hier, quand on détectait un attaquant, nous nous interdisions de faire quoi que ce soit vis-à-vis de lui. Maintenant nous pouvons chercher à savoir ce qu'il veut faire et quels sont ces objectifs"
France	29 oct. 2014	La Quadrature du net, association de défense des droits et libertés des citoyens sur Internet.	Société civile	http://www.nextinpact.com/news/90674-le-projet-loi-sur-terrorisme-deja-menace-dune-qpc.htm	"Chaque député, chaque sénateur qui rejettera ce texte prendra date comme étant l'un de ceux qui se seront opposés à l'instrumentalisation des risques terroristes pour porter atteinte aux droits fondamentaux et à l'État de Droit, dans des domaines qui vont très au-delà de la seule lutte antiterroriste"
France	29 oct. 2014	Asic, association des sites internet	Société civile	http://www.lasic.fr/?p=666	"au cours des prochains mois, le Gouvernement publiera les décrets d'application de ces lois portant une atteinte, sans précédent, aux libertés. L'ASIC sera vigilante à ce que ceux-ci fassent l'objet d'un contrôle de leur légalité par le Conseil d'État et puissent être soumises à l'examen du Conseil constitutionnel par l'intermédiaire de la procédure de la Question prioritaire de constitutionnalité (QPC) [...] le Conseil constitutionnel a eu l'occasion de rappeler la nécessité de limiter les atteintes à la liberté de communication. Celle-ci inclut notamment la liberté d'accéder à des informations [...] le blocage de sites internet, tout comme leur déréférencement, constitue par nature une atteinte à cette liberté.

France	04 déc. 2014	CNIL, Commission nationale de l'informatique et des libertés	Etatique	http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029959443	" appelle dès lors l'attention du gouvernement sur les risques qui en résultent pour la vie privée et la protection des données à caractère personnel et sur la nécessité d'adapter le régime juridique national en matière de conservation et d'accès aux données personnelles des utilisateurs de services de communications électroniques."
France	26 déc. 2014	Éric Poncet, journaliste Le Point	Presse	http://www.les-crises.fr/le-cadeau-de-noel-de-manuel-valls-aux-internautes-la-surveillance/	"La loi de programmation militaire a mis en place un outil de surveillance de la population française qui aurait fait pâlir d'envie les pires dictateurs de l'histoire. Si nous sommes très loin d'un régime totalitaire en France, il n'est pas exclu que des leaders extrémistes disent demain merci au gouvernement Valls pour leur avoir fourni un tel outil clé en main"
France	28 déc. 2014	Nicolas Bourgoin, docteur de l'Ecole des Hautes Etudes en Sciences Sociales, auteur de livres	Académique	https://bourgoinblog.wordpress.com/2014/12/27/la-loi-de-programmation-militaire-va-legaliser-la-surveillance-dinternet/	"La dernière loi de Programmation militaire va légaliser la surveillance de la totalité du Net et des télécommunications [...]. Véritable sésame pour vaincre les résistances aux lois liberticides, la « guerre contre le terrorisme » ou contre la « criminalité organisée » donne lieu à une militarisation de l'espace public, un panoptisme social intrusif et la mise en œuvre d'une politique de contrôle intérieur basée sur la peur. [...] L'adoption du projet par le Sénat s'est faite malgré une forte mobilisation des acteurs du numérique et sans consultation de la CNIL. Il ouvre la voie à une surveillance totale des communications et des déplacements. Véritable loi martiale numérique, la LPM rend encore un peu plus réel le cauchemar d'une société de sécurité maximale "

France	09 oct. 2014	Internet Sans Frontières	Société civile	https://www.change.org/p/cap-sur-un-internet-libre-en-2014-sto-part20/u/8381499	"lance sur le réseau social Twitter la campagne #PasEnNotreNom visant à demander aux sénateurs de refuser de sacrifier les libertés sur l'autel de la sécurité lors de leur vote sur le projet de loi contre le terrorisme. " [...] Projet de loi terrorisme : Sénateurs, la plus grande victoire du terrorisme serait de mettre en péril l'état de droit !"
France	13 janv. 2015	Jean-Yves Le Drian, Ministre de la Défense	Etatique	http://www.zamanfrance.fr/article/drian-evoque-renforcement-role-reservistes-13944.html	"les missions de déploiement de 10 000 hommes pour protéger le territoire français "sont tout à fait inscrites dans la loi de programmation militaire" ; "Il est prévu en 2015 que le parlement soit saisi d'une actualisation (de la loi) [...] Cette question sera abordée au moment où il le faudra, quand le parlement sera saisi, c'est-à-dire dans quelques semaines" ; "Je crois qu'un des sujets qui doit être posé demain, c'est le rôle des réserves pour l'avenir, en particulier pour la protection du territoire".
France	14 janv. 2015	Eleusis Bastiat, journaliste, Le Parisien Libéral	Presse	http://www.agoravox.fr/tribune-libre/article/jesuischarlie-onfaitquoi-162055	" la France vient déjà de se doter d'un corpus législatif liberticide, l'article 20 de la loi de programmation militaire (4), dont les effets porteront sur tous, et non pas juste sur les terroristes présumés. Voulons-nous vraiment d'une police autorisée à faire n'importe quoi au nom de la lutte contre le terrorisme, pour que dans 10 ans nous soyons comme les américains actuellement, à ouvrir le dossier de la violation des libertés civiles ? Et sans même faire parler les morts, est-ce que les journalistes de Charlie Hebdo auraient approuvé un *Patriot Act* ? "

France	15 janv. 2015	Guy Mamou-Mani, président du Syntec numérique	Industriel	http://www.lesechos.fr/tech-medias/hightech/0204085278928-la-grogne-monte-face-aux-ambitions-de-la-cyberpolice-1083682.php	" C'est légitime que l'on se pose des questions. Je ne suis pas un libertaire bisounours. Mais aller écouter internet sans l'intervention d'un juge, non ». "la loi de programmation militaire votée en décembre dernier élargit déjà les pouvoirs de la police et des services de renseignement en leur permettant d'accéder aux données de connexion des internautes sans décision judiciaire."
France	21 janv. 2015	Elysée	Etatique	http://www.elysee.fr/communiques-de-presse/article/conseil-de-defense-3/	L'Elysée "a décidé de réduire de 7 500 les déflations d'effectifs prévues pour le ministère de la défense sur la période de 2015 à 2019 par la loi de programmation militaire, dont 1 500 dès l'année 2015
France	15 janv. 2015	François Hollande, président français	Etatique	http://www.lemonde.fr/politique/article/2015/01/15/hollande-pret-a-revoir-la-baisse-des-effectifs-militaires_4557026_823448.html#U2s1IYJSVUcK2C3g.99	"Je me suis engagé à la (la LPM) respecter pour 31,4 milliards d'euros, et ce chiffre-là est sanctuarisé »
France	11 janv. 2015	Valérie Pécresse, UMP, ancienne ministre	Etatique	http://www.franceinfo.fr/emission/france-info-numerique/2014-2015/y-aura-t-il-un-patriot-act-francais-12-01-2015-22-10	"Il faudra bien entendu *un Patriot Act* à la française. Il faut une réponse ferme et globale #renseignement #securité"

1.3. OpFrance, la bataille sémantique

1.3.1. Résumé

L'Opération Charlie Hebdo, lancée par Anonymous directement après les attentats contre le journal, a obtenu une grande couverture médiatique et a rallié de nombreux acteurs : en deux jours, on comptait plus de 22 000 abonnés sur le compte twitter des Anonymous[1].

En revanche cette action a été vivement critiquée : les **autorités françaises**, la **presse** ainsi que les **experts en sécurité** des systèmes d'informations ont été nombreux à remettre en cause l'utilité de la manœuvre. Ceux-ci ont fait remarquer que malgré les centaines de sites djihadistes bloqués, Anonymous risquait de perturber les enquêtes policières en forçant les djihadistes à changer de comportement ou en supprimant des comptes qui servaient de sources de renseignements pour les forces de l'ordre.

OpFrance a pour sa part été menée par près d'une trentaine de groupes venant de Tunisie, Maroc, Indonésie, Algérie, Malaysie, Mexique[2]. Citons : United Islamic Cyber Force, FallaGa team, Anon Ghost, APoca-DZ[3], Abdellah Elmaghribi[4], CrashBandicot, Hani Xavi et Lootz etc… Ces groupes d'islamistes opèrent selon une technique de « filet » : ils recherchent, par le biais d'outils automatisés, des sites n'ayant pas appliqué des mises à jour de sécurité et donc vulnérables. La plupart sont des sites personnels, de PME ou d'associations, mais sont également touchés certains sites à l'audience beaucoup plus importante.

Gouvernement français

Dans l'urgence, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a envoyé un manuel aux ministères, qui résume les étapes de base à prendre en matière de cyber-sécurité. Il est donc nécessaire d'éviter d'utiliser le même mot de passe sur plusieurs sites pour stocker tous vos mots de passe en un seul endroit. L'**ANSSI** a mis à disposition des entreprises et des particuliers des documents concernant à la fois la prévention et la réaction aux menaces cybernétiques: une fiche destinée à tout internaute et une fiche destinée aux administrateurs de sites internet, le guide d'hygiène informatique et la note sur la sécurisation des sites web.

Pour faire face au cyberterrorisme, le gouvernement français a également fourni une version numérique du Plan Vigipirate. Les recommandations visent en priorité les opérateurs d'importance vitale, les ministères et les forces de l'ordre.

Afin de contrer les cyberattaques, « une cellule de crise opérationnelle 24h sur 24 » a été mise en place[5].

Politiquement, la posture adoptée est à la relativisation : il s'agit d'attaques sur des « cibles faciles », « de faible niveau », et pouvant être perpétrées par « n'importe quel geek ». La priorité est donnée aux

---

[1] Proâme.net *La cyberguerre est déclarée*, 11 janvier 2015 : http://www.proame.net/la-cyberguerre-est-declaree-upmagazine (consulté le 24 mars 2015).
[2] RAFATI Mohamed, *Several Thousands French Websites are under Cyber Attacks and Hacked,* Cyberwarzone.com, 13 janvier 2015 : http://cyberwarzone.com/several-thousands-french-websites-cyber-attacks-hacked (consulté le 24 mars 2015).
[3] France24.com, « *Cyberjihadists » hack hundreds of French websites,* 14 janvier 2015 : http://www.france24.com/en/20150114-cyberjihadists-hack-hundreds-of-french-websites (consulté le 24 mars 2015).
[4] LORRIAUX Aude, *Des dizaines de sites internet français piratés par des islamistes,* Metronews.fr, 11 janvier 2015 *:* http://www.metronews.fr/info/des-dizaines-de-sites-internet-francais-pirates-par-des-islamistes/moak!cmZFDn64y6fw (consulté le 24 mars 2015).
[5] RP Defense blog : http://rpdefense.over-blog.com/tag/arnaud%20coustilliere (consulté le 24 mars 2015).

opérateurs d'importance vitale, à savoir, 12 secteurs d'activités et 218 entités françaises à protéger en priorité.

Autres acteurs

Pour la plupart des **experts en sécurité** des systèmes d'information, cette attaque n'a rien d'exceptionnelle si ce n'est la quantité des victimes et la rapidité à laquelle les infections ont été menées. En revanche, les moyens techniques sont faibles (DDoS, défiguration) et ils estiment que les conséquences de ces attaques sont moindres.

Au niveau des **victimes**, la réaction est plus importante. Les attaques ont souvent perturbé pendant quelques jours les plateformes des localités, même s'il ne semble pas y avoir eu de vol de données. Beaucoup de municipalités ont choisi de porter plainte. Certaines sont cependant financièrement pénalisées par ces attaques (cf. Le Monde).

La société civile s'inquiète quant aux réactions législatives et politiques dans l'urgence qui, au contraire de renforcer la sécurité des citoyens, auraient pour conséquences une perte de libertés individuelles[6].

1.3.2. Focus sur les réactions dans le cadre d'OpFrance

Pays	Date	Acteur	Type d'acteur	Source	Citation VO
UK, France	12 janv. 2015	David Cameron, Premier ministre UK	Acteur étatique	http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg	"New legislation would be needed in two areas: the collection of communications data – information about when a call is made, by whom and to whom; and the interception of calls and online communications, known as accessing content".
France	14 janv. 2015	ASIC (Association des services internet communautaires)	Société civile	http://www.lasic.fr/?p=698	"Nos membres travaillent activement avec tous les services d'enquêtes afin de les aider à procéder à l'identification des divers auteurs de crimes ou délits ou de lutter contre la propagation de ces contenus manifestement illicites."; "toute nouvelle mesure législative et réglementaire devra respecter l'ensemble des libertés, qu'il s'agisse des libertés publiques mais aussi des libertés individuelles."; "le Gouvernement devrait rapidement, comme ont pu le faire ses homologues européens, s'engager dans une vraie campagne de 'contre-discours' "

[6] POLLONI Camille et KRISTANADJAJA Gurvan, *Mesures terroristes : « Si on doit borner le liberté d'expression, c'est la loi qui doit le faire, par des entreprises privées »*, Nouvel Observateur, 21 janvier 2015 : http://rue89.nouvelobs.com/2015/01/21/mesures-antiterroristes-si-doit-borner-liberte-dexpression-cest-loi-doit-faire-entreprises-privees-257234 (consulté le 14 mars 2015).

France	15 janv. 2015	Arnaud Coustillière, Vice-amiral, Officier général cyberdéfense à l'EMA	Acteur étatique	http://www.20minutes.fr/societe/1517927-20150115-cyberdjihad-19000-sites-internet-francais-attaques-islamistes-quatre-jours	«c'est la première fois que le pays est confronté à une telle cyber contestation» ; «hackers islamistes»; « Nous prenons cette crise au sérieux mais nous ne sommes absolument pas inquiets »; «C'est une attaque de faible niveau» ; «une cellule de crise opérationnelle en H24» a été mise en place.
France	15 janv. 2015	Frédéric Valette, responsable du pôle sécurité des systèmes d'informations au sein de la Direction général de l'armement	Acteur étatique	http://www.20minutes.fr/societe/1517927-20150115-cyberdjihad-19000-sites-internet-francais-attaques-islamistes-quatre-jours	«Ces attaques sont de type opportunistes»; «De faible niveau» et menées par «n'importe quel geek», ces attaques, qui ont ciblé «des écoles ou encore une pizzeria», exploitent les failles de ces sites faiblement protégés.
France	21 janv. 2015	Elodie, rédactrice pour Le Journal du Geek	Presse	http://www.journal-dugeek.com/2015/01/21/le-monde-pirate-armee-electronique-syrienne/	" 3,3 millions d'abonnés ont pu voir défiler sur leur timeline des messages et images en liens avec les attentats de Paris" ; "Ce piratage a également eu d'autres conséquences, puisqu'en quelques heures, Lemonde.fr a perdu quelques 326 000 abonnés."
France	21 janv. 2015	Martin Untersinger, journaliste pour Le Monde	Presse	http://www.lemonde.fr/pixels/article/2015/01/21/le-compte-twitter-du-monde-piraté_4560072_4408996.html#3FcvqyJHHdwke7CJ.99	"Le Monde avait fait l'objet d'une tentative très élaborée d'attaque, dimanche et lundi, que nos équipes étaient parvenues à contrer et à circonscrire. Les pirates avaient accédé à notre outil de publication, sans parvenir à publier d'article. Ils ont également eu accès à certaines boîtes électroniques. Une plainte sera déposée dans les prochaines heures, notamment pour intrusion et maintien frauduleux dans un système informatique"
France	20 janv. 2015	Guillaume Poupard, directeur de l'ANSSI	Acteur étatique	http://www.01net.com/editorial/641992/selon-l-anssi-les-hackers-djihadistes-sont-de-faible-niveau/	" Sur le plan de la communication, l'impact est parfois réel. Mais au niveau technique, ces attaques sont de faible niveau. Il s'agit essentiellement de défigurations de sites peu sécurisés: des écoles, des mairies, etc. Ces actions sont accessibles à n'importe quel étudiant en informatique motivé"; les cyber djihadistes sont de l'ordre de "quelques dizaines, grand maximum"; "opérateurs d'importance vitale [...] C'est vraiment la priorité de l'ANSSI. Ces attaques peuvent avoir des conséquences sur le fonctionnement même de la Nation »: "cibles faciles"

France	20 janv. 2015	Thibaud Signat, responsable ingénierie système chez FireEye	Acteur industriel	http://www.01net.com/editorial/641992/selon-l-anssi-les-hackers-djihadistes-sont-de-faible-niveau/	"Globalement, les hackers du Moyen-Orient sont techniquement moins sophistiqués qu'en Occident ou en Asie, mais ils utilisent davantage d'ingénierie sociale pour atteindre leur but" ; "Mais attention, ces groupes ont aujourd'hui les moyens de recruter. Il y a aussi des étudiants brillants qui partent faire le jihad"
Allemagne, France	20 janv. 2015	Thomas de Maizière, ministre de l'Intérieur allemand	Acteur étatique	Forum International de la Cybersécurité (FIC2015)	"There is an' urgent action' terrorist efforts in the' virtual world";
France	13 janv. 2015	Manuel Valls, Premier ministre de la République française	Acteur étatique	http://www.liberation.fr/societe/2015/01/13/manuel-valls-et-la-reforme-securitaire-qui-s-esquisse_1179984	"Dans les huit jours des propositions de renforcement [qui] devront concerner notamment internet et les réseaux sociaux, plus que jamais utilisés pour l'embrigadement, la mise en contact et l'acquisition de techniques permettant de passer à l'acte " + sortie accélérée d'un des décrets d'application de la loi contre le terrorisme adoptée en octobre 2014 qui permet le blocage administratif des sites 'provoquant des actes de terrorisme ou en faisant l'apologie'
France	13 janv. 2015	Adrienne Charmet-Alix, Coordinatrice des campagnes de la Quadrature du Net	Société civile	http://rue89.nouvelobs.com/2015/01/21/mesures-antiterroristes-si-doit-borner-liberte-dexpression-cest-loi-doit-faire-entreprises-privees-257234 ; http://www.lemonde.fr/pixels/article/2015/01/13/patriot-act-a-la-francaise-il-est-important-de-garder-la-tete-froide_4555146_4408996.html#kKv7Bw5BXPCi9kC0.99	"Des cyberpatrouilles, ça veut tout et rien dire. Qu'est-ce qu'elles auront le droit de faire ?" ; "Appeler à la responsabilité morale des acteurs du Web, c'est un biais dangereux, parce que c'est demander à des entreprises privées d'exercer elles-mêmes une censure plus lourde. Si on doit borner la liberté d'expression, c'est la loi qui doit le faire, et non des entreprises privées." : " il y a déjà ce qu'il faut dans la loi. Simplement, c'est un choix à faire : choisit-on de surveiller massivement la population en espérant y trouver des renseignements, ou choisit-on de mettre des moyens humains sur les moyens de renseignement et de logistique. A priori, ce qui manque, ce sont les moyens humains. C'est ce que l'on préconise, afin de mieux suivre les personnes que l'on pense dangereuses, plutôt que toute la population."

France	21 janv. 2015	Manuel Valls, Premier ministre de la République française	Acteur étatique	http://www.lemonde.fr/pixels/article/2015/01/13/patriot-act-a-la-francaise-il-est-important-de-garder-la-tete-froide_4555146_4408996.html#kKv7Bw5BXPCi9kC0.99	"Les grands fournisseurs de services internet, les réseaux sociaux ont aujourd'hui une responsabilité juridique incontestable en droit français", a appuyé Manuel Valls, leur imposant des "obligations légales" ; "une responsabilité morale encore plus grande". "Je les appelle de manière solennelle à coopérer avec les autorités", notamment "pour répondre aux signalements" ou "déréférencer des sites illégaux".

1.3.3. Focus sur les réactions dans le cadre d'OpCharlie

Pays	Date	Acteur	Type d'acteur	Source	Citation VO
France	09 janv. 2015	Olivier Laurelli, bloggeur spécialiste de la sécurité informatique	Société civile	http://www.20minutes.fr/high-tech/1513775-20150109-attaque-charlie-hebdo-riposte-anonymous-peut-etre-bonne-idee	«A partir du moment où on attaque les réseaux où ils [les djihadistes] communiquent entre eux, on interfère dans le travail des enquêteurs»
France	12 janv. 2015	Olivier Bogaert, Commissaire de la Computeur Crime Unit de la police fédérale belge.	Acteur étatique	http://www.journaldugeek.com/2015/01/12/opcharliehebdo-anonymous-ripostent/	« en s'attaquant au serveur, les pirates d'Anonymous risquent de bloquer des données ou de faire disparaître les traces d'accès aux sites par les criminels. Traces qui pourraient être utilisées pour identifier d'autres terroristes »
France	09 janv. 2015	Pascal Samama, journaliste 01net	Presse	http://www.01net.com/editorial/640257/opcharliehebdo-l-operation-antidjihadiste-des-anonymous-sous-la-critique/	"Problème, en attaquant ces plateformes, ils incitent les islamistes à se réorganiser et, ainsi, ils risquent de saper le travail des policiers chargés de l'enquête. Et cette fois, au lieu d'approuver, la toile critique ouvertement l'initiative."
France	13 janv. 2015	Le Switcheur, bloggeur	Société civile	http://www.phonandroid.com/charlie-hebdo-anonymous-ferme-plusieurs-sites-djihadistes.html#comment-1788084917	"#opJaipasdecerveau. Pourquoi refuser d'utiliser les outils mis à notre disposition par le gouvernement comme Pharos ? Ce qu'ils font est tout sauf productif. Quitte à lutter, faites-le intelligemment, messieurs !"

France	13 janv. 2015	Fred, bloggeur	Société civile	http://www.phonandroid.com/charlie-hebdo-anonymous-ferme-plusieurs-sites-djihadistes.html#comment-1788084917	"ils bougent eux contrairement à certains qui ne font que du bruit avec leur bouche depuis des années."
France	12 janv. 2015	Graham Cluley, auteur d'articles sur Tripwire Inc.	Acteur industriel	http://www.tripwire.com/state-of-security/off-topic/anonymous-attacks-jihadist-websites/	"Of course, there is no shortage of irony in the fact that Anonymous rails against attacks on freedom of expression, but appears to have no problem with launching denial-of-service attacks to silence websites. […] And, if you believe that someone is breaking the law online, the best thing you can do is inform the authorities so they can take appropriate action. The answer, I believe, is not to take the law into your own hands by taking down websites, and potentially disrupting the infrastructure and communications of innocent individuals and companies."
France	01 août 2015	Police Nationale, compte Twitter	Acteur étatique	https://twitter.com/pnationale/status/553153469755170816	"[#CharlieHebdo] Ne perturbez pas le travail des policiers enquêteurs en diffusant de fausses informations ou #rumeurs "
France	11 janv. 2015	Olivier Chicheportiche journaliste de ZDNet.fr	Presse	http://www.proame.net/la-cyberguerre-est-declaree-upmagazine/	« Sous des airs louables, les Anonymous n'ont pas peur de la contradiction puisqu'il s'agit d'empêcher certains de s'exprimer pour défendre la liberté d'expression. Curieuse approche car quand on défend la liberté d'expression, en théorie, on la défend pour tous. Ce genre de vengeance à chaud risque de jeter de l'huile sur le feu, de creuser les lignes de fracture. Et de ne servir à rien puisque les personnes à l'origine de ces sites sont parfaitement capables de remonter des infrastructures, encore plus discrètes et donc encore plus difficiles à localiser. »

1.4. Sony, un cas d'étude structurant et regroupant des réactions de divers acteurs

1.4.1. Résumé

L'affaire Sony est un cas d'espèce très représentatif de la palette de réactions et d'outils d'influence utilisables lors de cyber conflits.

- Pression humoristique et soft power via création artistique
- Pression cyber par l'outil de l'arme informatique
    - Intrusion
    - Diffusion d'information
    - Etc.
- Pression économique par le ralentissement de l'activité d'une entreprise structurante
- Pression en termes d'image pour l'entreprise
- Pression en termes d'image pour le pays dont cette entreprise est l'avatar (Hollywood et USA) : s'attaquent à un symbole du soft power américain
- Pression humaine sur les salariés de l'entreprise : données personnelles + licenciements et démissions
- Pressions juridiques et judiciaires de la part des Etats-Unis
- Présentation de faisceau d'indices pour l'attribution désignée
- Usage des entreprises tiers pour justifier l'attribution (Taia global, etc.)
- Riposte informatique : usage de l'attaque DDoS pour sanctionner la Corée du Nord et démonstration de force
- Riposte diplomatique avec des sanctions à l'échelle internationale par les Etats-Unis

1.4.2. Focus sur les réactions

Pays	Date	Acteur	Type d'acteur	Source	Traduction/Résumé FR
Etats-Unis / Corée du Nord	27 juin 2014	Ja Song-Nam, représentant de la Corée du Nord au Nations Unies	Acteur étatique	http://www.reuters.com/article/2014/07/09/us-northkorea-un-film-idUSKBN0FE21D20140709	Une lettre adressée au Secrétaire général des Nations Unies Ban Ki-moon, de l'ambassadeur de la Corée du Nord, Ja Nam Song, datée du 27 juin 2014 mais rendue publique début juillet accuse les Etats-Unis de soutenir le terrorisme et de commettre un acte de guerre en permettant la production d'un film qui 'implique d'insulter et d'assassiner le leader suprême'.
Etats-Unis	24 nov. 2014	[deleted]	Société civile	http://www.reddit.com/r/hacking/comments/2n9zhv/i_used_to_work_for_sony_pictures_my_friend_still/	I used to work for Sony Pictures. My friend still works there and sent me this. It's on every computer all over Sony Pictures nationwide.

Etats-Unis	24 nov. 2014	GOP	Société Civile	http://www.business2community.com/tech-gadgets/sony-pictures-hacked-gop-mean-01077919	"Hacké par #GOP, nous vous avions avertis et ceci est juste le début" Message présent sur les écrans des ordinateurs de SONY Pictures le 24/11/2014 au matin
Etats-Unis	25 nov. 2014	Charles Lim, Senior Analyst at ICT, Frost & Sullivan Asia Pacific	Acteur industriel	http://www.bbc.com/news/technology-30189029	Charles Lim annonce que les pirates du #GOP revendiquent avoir eu accès aux données sensibles des employés de SONY
Chine	25 nov. 2014	Hua Chunying, porte-parole du Ministère des affaires étrangères	Acteur étatique	http://www.shanghaidaily.com/national/Call-for-restraint-over-Sony-incident/shdaily.shtml	Hua Chunying souhaite que les parties impliquées dans cette affaire s'astreignent de toute accusation sans fondement et que l'enquête doit se poursuivre sans entraves.
Etats-Unis	25 nov. 2014	Wee Teck Loo, Head Consumer electronic research at Euromonitor	Acteur industriel	http://www.bbc.com/news/technology-30189029	Le piratage de SONY d'il y a 3 ans était conséquent. Cette fois-ci, je ne crois pas qu'il y ait de dégâts importants, même si le piratage est bien réel.
Etats-Unis / Corée du Nord	28 nov. 2014	Arik Hesseldahl	Presse	http://recode.net/2014/11/28/sony-pictures-investigates-north-korea-link-in-hack-attack/	Les équipes de Sony annoncent que les pirates à l'origine de l'attaque seraient localisées en Corée du Nord ou en Chine, le timing de l'attaque coïncide avec la sortie imminente du film THE INTERVIEW, évoquant un attentat contre le dirigeant Nord-Coréen.
Etats-Unis	01 déc. 2014	Jean Guérin, porte-parole de Sony	Acteur industriel	http://www.scpr.org/news/2014/12/01/48394/sony-hack-fbi-confirms-it-s-investigating-hack-lea/	Sony Pictures continue de travailler sur les problèmes liés à ce qui était manifestement une cyber-attaque. La société a rétabli un certain nombre de services importants pour assurer la continuité des activités en cours et travaille en étroite collaboration avec les responsables de l'application de la loi pour enquêter sur l'affaire.

Etats-Unis / Corée du Nord	01 déc. 2014	Porte-parole de la mission de l'ONU de la Corée du Nord	Acteur étatique	http://www.reuters.com/article/2014/12/01/us-sony-cybersecurity-northkorea-idUSKCN0JF2UJ20141201	Les forces hostiles ont tendance à tout lier à la RPDC (Corée du Nord). Je conseille d'attendre et de voir. La Corée du Nord attribue régulièrement le termes de "forces hostiles" les États-Unis et la Corée du Sud.
Etats-Unis	02 déc. 2014	Clifford Neuman, directeur de l'USC Center for Computer Systems Security	Acteur académique	http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hacked-spreadsheet-salaries-ssns-email-up-20141202-story.html	Pour regagner la confiance dans l'intégrité de son réseau, Sony aura besoin de reconstruire les systèmes de sécurité de l'ensemble de sa structure.
Corée du Nord	04 déc. 2014	Porte-parole du Ministre des Affaires étrangères Nord-Coréen	Acteur étatique	http://www.scmp.com/news/asia/article/1673631/new-us-sanctions-over-sony-cyberattack-hostile-act-says-north-korea	"The persistent and unilateral action taken by the White House to slap 'sanctions' [on North Korea] patently proves that it is still not away from inveterate repugnancy and hostility [toward it]," a Foreign Ministry spokesman was quoted as saying by the state-run Korean Central News Agency. The Foreign Ministry spokesman quoted on Sunday by KCNA said Sony Pictures "produced a disgusting movie openly agitating terrorism against a sovereign state only to invite bitter censure and criticism of public at home and abroad."
Corée du Nord	04 déc. 2014	Officiel Nord Koréen	Acteur étatique	http://time.com/3612132/sony-hack-north-korea-interview/	La publication de ce film serait un acte de guerre et de terrorisme et des sanctions pourraient être entreprises contre la sortie de ce film.
Etats-Unis	05 déc. 2015	Kazuo Hirai, PDG de Sony	Acteur industriel	http://www.techtimes.com/articles/24874/20150106/sony-ceo-condemns-vicious-and-malicious-hack-proud-of-employees-and-partners.htm?exe=reporter	Les anciens employés et employés actuels de Sony sont les victimes d'une des plus vicieuses et malicieuses cyber attaques connues. La liberté de parole, d'expression, d'association, sont des principes fondamentaux de Sony et de l'industrie du divertissement.

Etats-Unis	06 déc. 2014	Kévin Mandia, directeur de Fire Eye's Mendiant, entreprise engagée pour enquêter sur l'attaque	Acteur industriel	http://recode.net/2014/12/07/sony-describes-hack-attack-as-unprecedented/	Cette attaque est d'une nature sans précédent. La portée de cette attaque dépasse tout ce qui a été connu dans le passé. Son but était la destruction de biens et la divulgation de renseignements confidentiels au public. Ce crime était bien planifié et a été réalisé par un groupe organisé pour lequel aucune entreprise n'aurait pu être entièrement prête.
Japon	07 déc. 2014	Kazuo Hirai SONY Corp. CEO	Acteur industriel	http://www.scmp.com/news/asia/article/1675905/sony-ceo-kazuo-hirai-says-company-was-victim-vicious-cyberattack	Le PDG de SONY Corp. a pris la parole au CES de Las Vegas pour parler de la liberté d'expression. Première apparition en public du PDG de SONY depuis l'attaque en novembre dernier.
Etats-Unis	07 déc. 2014	Jordan Robertson, Dune Lawrence and Chris Strohm	Presse	http://www.bloomberg.com/news/2014-12-07/sony-s-darkseoul-breach-stretched-from-thai-hotel-to-hollywood.html	Faits relatant la possible présence de hackers dans des hôtels à Bangkok. Ceux même qui auraient participés à l'attaque contre SONY Pictures.
Etats-Unis	08 déc. 2014	SONY	Acteur industriel	http://www.huffingtonpost.com/2014/12/01/fbi-sony-hack_n_6248120.html	Les équipes de SONY Pictures ont décidé de faire appel aux experts de Mendiant et Fire Eye pour une expertise du réseau de SONY et de l'attaque produite.
Etats-Unis	08 déc. 2014	SONY PICTURES	Acteur industriel	http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf	Lettre de la direction de SONY Pictures aux employés sur le vol des données sensibles: numéros de sécurité social, numéro de permis de conduire, mots de passe,etc.
Etats-Unis	08 déc. 2014	FBI	Acteur étatique	http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation	Le FBI annonce pour la PREMIERE FOIS l'implication de la Corée du NORD dans l'attaque de SONY Pictures.
Corée du Nord	08 déc. 2014	Porte-Parole non identifié du NDC Nord-Coréen	Acteur étatique	http://www.shanghaidaily.com/world/NK-denies-cyberattack-on-Sony/shdaily.shtml	De nombreuses rumeurs ont été diffusées sur les réseaux et la Corée du Nord nie toute implication dans l'attaque contre SONY Pictures.

Etats-Unis	09 déc. 2014	Kévin Levine, président du fournisseur de services en sécurité Digital Guardian	Industriel	http://arstechnica.com/security/2014/12/unprecedented-cyberattack-no-excuse-for-sony-breach-pros-say/	L'annonce de Kevin Mandia et de l'équipe FireEye est une façon de déresponsabiliser Sony en leur offrant l'opportunité de se cacher derrière le prétexte des menaces persistantes avancées.
Etats-Unis	10 déc. 2014	Philip Lord, directeur de film	Presse	https://deadline.com/2014/12/sony-hack-amy-pascal-e-mails-1201318234/	L'attaque contre Sony est une attaque terroriste. Publier des informations aide les terroristes. Sony et les cinéastes sont victimes, nous devons les soutenir.
Etats-Unis	10 déc. 2014	Ryan Johnson, directeur de film	Presse	https://deadline.com/2014/12/sony-hack-amy-pascal-e-mails-1201318234/	Ce qui est arrivé contre Sony est très grave. Il ne faut pas cliquer sur le lien des hackers et il faut reporter toute personne qui poste des emails volés.
Etats-Unis	11 déc. 2014	Seth Rogen, acteur américain	Presse	http://variety.com/2014/film/news/the-interview-seth-rogen-amy-pascal-1201377101/	Lors de l'Avant-Première du film "The Interview", Seth Rogen a déclaré remercier Amy Pascal, co-directrice de Sony, d'avoir eu le courage de faire ce film.
Etats-Unis	16 déc. 2014	Groupe d'hackers, probablement responsables de l'attaque contre Sony	Société civile	http://variety.com/2014/film/news/sony-hackers-threaten-911-attack-on-movie-theaters-that-screen-the-interview-1201380712/	Attention à ceux qui souhaitent voir le film "The Interview". Rappelez-vous le 11 septembre 2001. Nous vous conseillons de vous éloigner des lieux de diffusion du film. Ce qui arrivera dans les prochains jours est le résultat de la cupidité de Sony Pictures Entertainment. Le monde va bientôt détester Sony.
Etats-Unis	16 déc. 2014	John Miller, commissaire adjoint du renseignement et de la lutte contre le terrorisme du NYPD	Acteur étatique	http://nypost.com/2014/12/16/sony-hackers-issue-creepy-warning-to-moviegoers/	Les menaces concernant le film "The Interview" n'ont rien d'exceptionnelles. De telles menaces ont été faites pour d'autres films sur Ben Laden par exemple. La sécurité sera renforcée à tous les lieux de potentielle diffusion.

Etats-Unis	17 déc. 2014	Dan Sterling, Scénariste de "L'Interview"	Presse	http://www.scpr.org/programs/the-frame/2014/12/15/40758/how-the-interview-scribe-dan-sterling-became-Sony/	On ne sait toujours pas si la Corée du Nord est derrière cette attaque ni qui en sera affecté et de quelles manières.
Etats-Unis / Chine / Corée du Nord	18 déc. 2014	George Clooney, acteur américain.	Presse	https://deadline.com/2014/12/george-clooney-sony-hollywood-cowardice-north-korea-cyberattack-petition-1201329988/	Le nom Gardiens de la Paix est une référence à la phrase que Nixon a utilisée durant une visite en Chine: lorsqu'on lui a demandé pourquoi il aidait la Corée du Sud, il a dit que c'était parce que nous étions les gardiens de la paix. Il s'agit dans cette attaque menée par un pays, la Corée du Nord et qui dépasse largement le cadre du cinéma mais affecte tous les intérêts des Etats-Unis. Sony n'a pas diffusé le film parce que les cinémas ont dit qu'ils n'allaient pas le passer et parce que si quelqu'un mourrait dans cette affaire, ils seraient responsables. George Clooney a lancé une pétition auprès des grands représentants du cinéma qui n'a reçu aucune signature par peur de se mettre les hackers à dos.
Etats-Unis / Corée du Nord	19 déc. 2014	FBI	Acteur étatique	http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation	Suite à son enquête, le FBI possède suffisamment d'informations pour conclure que le gouvernement nord-coréen est lié à l'attaque contre Sony. La nature destructrice et coercitive de cette attaque la distingue de toute autre cyber attaque. Les actions de la Corée du Nord visaient à infliger des dommages importants aux entreprises américaines et à supprimer le droit des citoyens américains de s'exprimer. Ces actes d'intimidation dépassent les limites d'un comportement acceptable de la part d'un Etat.
?	19 déc. 2014	Guardians of Peace, groupe de hackers	Société civile	https://twitter.com/guardiansgop/status/545997922241085441	Nous ne sommes pas Coréens.
Mexique	19 déc. 2014	Susana Moscatel, journaliste mexicaine	Presse	http://www.milenio.com/firmas/susana_moscatel/Ganaron-terroristas_18_430337003.html	Céder aux menaces signifie une victoire des terroristes. Sony Pictures aurait dû diffuser le film dans le monde grâce aux canaux piratés qui peuvent échapper au contrôle des hackers.

Etats-Unis	19 déc. 2014	Guy Delisle, auteur de la BD Pyongyang	Presse	http://www.guydelisle.com/divers/farewell-hollywood/	Ce qui est désolant ce sont les raisons qui ont conduit à cette annulation. On aurait pu imaginer qu'une grosse multinationale résisterait devant les menaces d'une bande de hackeurs nord-coréens. Apparemment, ils ont su toucher là où ça fait mal.
Etats-Unis	21 déc. 2014	John Mc Cain, Sénateur US	Acteur étatique	http://www.huffington-post.com/2014/12/21/sony-north-korea-war_n_6362454.html	Il s'agit d'une nouvelle forme de guerre et non de cyber vandalisme comme le dit le Président Obama. Nous devons réagir et réagir fortement. Les Etats-Unis devraient rétablir les sanctions contre la Corée du Nord qui ont été levées au cours de l'administration de George W. Bush.
Etats-Unis	21 déc. 2014	Stuart McClure, directeur général de la société de cybersécurité Cylance	Acteur industriel	http://www.billboard.com/articles/business/6413955/sony-security-kevin-mitnick-electronic-frontier	Il s'agit de la plus grande attaque de vol de données qu'est connue l'industrie du cyber mais elle n'est pas particulièrement technique. Il n'y a rien de nouveau dans cette attaque: c'est la même technique qu'on utilise encore et encore, car elle fonctionne. Certaines technologies basiques auraient pu empêcher une grande partie de ce vol de données. Le niveau d'atteinte d'une entreprise américaine est sans précédent, mais un enfant aurait pu perpétrer cette attaque. Cette attaque marque l'aube de l'âge de cyber-terrorisme.
Etats-Unis	21 déc. 2014	Tor Ekeland, avocat de New York spécialisé en droit de l'internet	Société civile	http://www.billboard.com/articles/business/6413955/sony-security-kevin-mitnick-electronic-frontier	Ne pas avoir un bon système de sécurité de l'information quand on est un groupe aussi important que Sony, c'est de la négligence et il semble que la sécurité de Sony ait été très bâclée.
Etats-Unis	21 déc. 2014	Kévin Mitnick, directeur de Mitnick Security Consulting	Acteur industriel	http://www.billboard.com/articles/business/6413955/sony-security-kevin-mitnick-electronic-frontier	Ce n'est pas de la faute à Sony de n'avoir pas su empêcher cette attaque mais c'est de sa faute d'avoir été incapable de la détecter pendant plusieurs mois. Le gouvernement américain devrait publier toutes les preuves de l'attaque dans le monde du cyber, pour construire une certaine confiance.

Etats-Unis / Corée du Nord	22 déc. 2014	Bruce Schneier, écrivain et directeur en technologie à Co3 Systems	Acteur industriel	http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/	Je doute fortement de la véracité des propos du FBI concernant l'implication nord-coréenne dans l'attaque contre Sony. Il y a de nombreuses possibilités à envisager comme par exemple: un militaire nord-coréen, un individu indépendant nord-coréen, des hackers qui ont fait cette attaque pour s'amuser, un employé de Sony, une agence aidée par la Corée du Nord etc...
Chili / Etats-Unis	22 déc. 2014	Raúl Sohr, analyste international	Acteur académique	http://radio.uchile.cl/2014/12/22/caso-sony-abre-debate-sobre-terrorismo-y-derechos-digitales	Cette attaque ne représente pas un nouveau type d'attaque terroriste envers les Etats-Unis mais du piratage. L'intervention personnelle du Président américain pour une entreprise privée est le signe de pressions internes des partis conservateurs.
Etats-Unis	22 déc. 2014	David Boies, avocat de Sony Pictures Entertainment	Industriel	http://motherboard.vice.com/read/sony-threatens-to-sue-twitter-unless-it-removes-tweets-containing-hacked-emails	Sony demande à Twitter de prendre toutes les mesures possibles pour empêcher la diffusion d'informations volées et menace de poursuivre en justice le réseau social le cas échéant.
Etats-Unis	22 déc. 2014	Art House Convergence, la coalition des cinémas d'art et d'indépendants des Etats-Unis	Acteur industriel	https://www.change.org/p/sony-we-the-undersigned-support-sony	La coalition des cinémas Art House Convergence soutient Sony ainsi que ses employés partout dans le monde. Elle défend l'intégrité artistique et les libertés individuelles qui sont menacées par cette attaque. Art House Convergence promeut la diffusion du film même si la décision appartient à Sony et aux cinémas.
Chili / Etats-Unis	22 déc. 2014	Claudio Ruiz, directeur de l'ONG Derechos Digitales	Société civile	http://radio.uchile.cl/2014/12/22/caso-sony-abre-debate-sobre-terrorismo-y-derechos-digitales	Les entreprises détenant des informations personnelles devraient avoir des mesures de sécurité très élevées. Lors de fuites, la notification aux clients ainsi que la mise en place de sanctions devraient être prévues par la loi.
Etats-Unis	23 déc. 2014	Ken Levine	Presse	http://kenlevine.blogspot.de/2014/12/how-sony-hacking-has-impacted-its.html	Sony aurait dû chiffrer toutes les données de ses employés actuels et anciens et les conserver sur un réseau sécurisé. Sony n'a pas été assez regardant sur la sécurité et ses propositions de protection des données des employés sont insuffisantes. Des fraudes liées à cette attaque pourront avoir lieu pendant plusieurs années.

Etats-Unis	23 déc. 2014	Sony Pictures	Acteur industriel	http://rt.com/news/217019-sony-threat-sue-twitter/	Les équipes de SONY Pictures veulent poursuivre Twitter pour avoir laissé des pirates.
Etats-Unis	23 déc. 2014	Porte-Parole Twitter	Acteur industriel	http://motherboard.vice.com/read/sony-threatens-to-sue-twitter-unless-it-removes-tweets-containing-hacked-emails	Twitter's legal department told Broeksmit that it would be unable to provide him with "legal advice" saying he "may wish to contact your own attorney about this matter." A Twitter spokesperson told Motherboard that while it did not allow users to post the private information of other people directly in tweets, linking to such information is allowed. In at least three separate tweets, however, Broeksmit directly posted photographs containing the hacked information.
Russie	24 déc. 2014	Oleg Demidov Program Director, International Information Security and Global Internet Governance	Acteur académique	http://fr.ria.ru/presse_russe/20141224/203299697.html	Oleg Demidov du centre PIR souligne qu'il n'y a pour le moment aucune raison d'évoquer un "conflit interétatique dans l'espace cybernétique" car les auteurs potentiels des attaques contre Sony et la Corée du Nord sont nombreux. De plus, cette rupture provisoire d'accès en Corée du Nord ne peut en aucune façon constituer une réponse "proportionnée" par rapport aux pertes de Sony Pictures, qui se chiffrent à des millions de dollars: "La Corée du Nord est en réalité autosuffisante par rapport au web global. Mais si les hackers attaquaient le réseau intérieur nord-coréen, Kwangmyong, cela serait vraiment une réponse proportionnée".
Etats-Unis / Corée du Nord	25 déc. 2014	IntelCrawler, entreprise américaine spécialisée sur les menaces cyber	Acteur Industriel	https://twitter.com/intelcrawler	La Corée du Nord a peut-être reçu de l'aide des hackers qui ont attaqué Sony en 2011. C'est le Lizard Squad qui est lié à l'attaque contre Sony.
Russie / Etats-Unis / Corée du Nord	25 déc. 2014	Alexander Lukashevich, diplomate russe	Acteur étatique	http://itar-tass.com/en/russia/769186	L'idée même de ce film est agressive et scandaleuse. La réaction de la Corée du Nord est complètement compréhensive. Les menaces des Etats-Unis sur leur revanche et leur appel envers les autres nations à condamner la Corée du Nord sont contreproductives et dangereuses dans une région où il existe déjà de multiples tensions.

Corée du Nord	08 déc. 2014	Porte-Parole non identifié du NDC Nord-Coréen	Acteur étatique	http://www.shanghaidaily.com/world/NK-denies-cyberattack-on-Sony/shdaily.shtml	Lettre de la direction de SONY Pictures aux employés sur le vol des données sensibles : numéros de sécurité social, numéro de permis de conduire, mots de passe,etc.
Etats-Unis / Corée du Nord	27 déc. 2014	Porte-parole de la Commission de défense nationale nord-coréenne	Acteur étatique	http://article.joins.com/news/article/article.asp?total_id=16796597 ; http://www.reuters.com/article/2014/12/27/us-northkorea-cybersecurity-idUSKBN0K502920141227	(Traduction via translate Google du coréen au français) Les Etats-Unis sont directement liés aux coupures récentes d'internet. Il s'agit d'un nouvel exemple de l'impérialisme américain. Le film "The Interview" est contraire au droit international et est diffamatoire.
Etats-Unis	29 déc. 2014	Anthony M. Freed, bloggeur pour Norse Corp., société d'intelligence stratégique	Acteur industriel	http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/?utm_content=buffer20cd7&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer	Une enquête sur l'attaque a abouti à l'identification de six suspects dont au moins un ex-employé de Sony qui avait le savoir-faire technique et la connaissance du système pour mener cette attaque. Il s'agit donc peut-être d'une attaque faite de l'intérieure.
Etats-Unis	29 déc. 2014	Mark Rasch, ancien procureur fédéral	Etatique	http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/?utm_content=buffer20cd7&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer	Il y a toujours eu de gros doute sur l'implication de la Corée du Nord. Ce n'est pas impossible mais douteux. Cela a beaucoup plus de sens qu'ils s'agissent de personnes appartenant à l'entreprise, intégrées à ses rouages qui ont prétendu être la Corée du Nord.

Etats-Unis	30 déc. 2014	Mark Rasch Ancien procureur fédéral pour les cybercrimes	Société civile	http://www.scmp.com/news/world/article/1670667/north-korea-may-have-hired-foreign-help-hack-sony-pictures-us	"I think the government acted prematurely in announcing unequivocally that it was North Korea before the investigation was complete," said Mark Rasch, a former federal cybercrimes prosecutor. "There are many theories about who did it and how they did it. The government has to be pursuing all of them."
Etats-Unis	30 déc. 2014	Kevin Mandia Chief operating officer pour FireEye Inc.	Acteur industriel	http://www.scmp.com/news/world/article/1670667/north-korea-may-have-hired-foreign-help-hack-sony-pictures-us	"I don't have the data that they have to come up with that conclusion [about FBI allegation]," Mandia, chief operating officer of FireEye Inc, said in a video interview. "Every attack loops through numerous machines," he said. "You have to peel that onion all the way back. It isn't an easy thing to do." "Nobody expected when somebody breaks in to absolutely destroy all your data, or try to anyway, and that's just something that no one else has seen," he said.
Chine / Corée du Nord / Etats-Unis	05 janv. 2015	Hua Chunying, Ministre chinois des Affaires Etrangères	Acteur étatique	http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1225723.shtml	Toutes les parties concernées doivent agir avec prudence et éviter de prendre des mesures pouvant aggraver la situation déjà précaire dans la péninsule coréenne. Par ailleurs, la Chine a exprimé son opposition à toute forme de cyber-attaques par tout pays y compris les cyber-attaques menées par des individus en Chine ou grâce à l'utilisation des installations chinoises.
Japon / Etats Unis	06 janv. 2014	Fumio Kishida Ministre des affaires étrangères du Japon	Acteur étatique	http://itar-tass.com/en/world/770391	The Japanese side appreciates the U.S. support in the cyber security issue and welcomes Washington's stance on North Korea in connection with hacking of Sony Pictures Entertainment Inc., Japanese Foreign Minister Fumio Kishida said on Tuesday after a telephone conversation with U.S. Secretary of State John Kerry. Japan "strongly condemns" the cyber-attack against Sony Pictures Entertainment Inc. attributed to North Korea, Kishida told Kerry. Speaking to journalists after telephone talks with Kerry, Kishida said he told his U.S. counterpart that Japan "appreciates" the firm U.S. response to North Korea over the cyber-attack, in an apparent reference to Washington's imposition Friday of new sanctions on Pyongyang, Kyodo news agency reported.

Etats-Unis	?	Bob Rudis, co-auteurs du blog Data Driven Security	Société civile	http://sony.attributed.to/ ; http://www.silicon.fr/qui-pirate-sony-pictures-site-repond-humour-105176.html	Le site, construit par trois personnes, attribue de façon aléatoire le piratage des studios hollywoodiens à un groupe arménien, à un administrateur système de Sony, à un employé Sony situé en Corée du Nord ou en Chine (les deux versions existent), à un personnel de la direction financière du groupe au Brésil, à une organisation cybercriminelle syrienne, à des hackers américains, à des hacktivistes, etc. Il suffit de recharger la page pour avoir une nouvelle hypothèse (le plus souvent assez plausible, les données de base provenant d'informations collectées sur des piratages dans 95 pays). Le site parodie astucieusement (avec tracking d'IP, carte, indicateurs de compromission, timeline des événements…) les communications des sociétés de sécurité, qui se servent abondamment de leurs recherches en sécurité sur ce type d'événements pour se faire de la publicité. Le site ne se prive d'ailleurs pas de citer ces entreprises.

Postures par pays

Certains pays présentent une posture originale en matière de lutte informatique offensive. Quel discours tiennent-ils ? Comment réagissent-ils aux postures des autres Etats ? Quels sont leurs outils et leviers d'influence ?

1.1. Allemagne

1.1.1. Abstract

L'Allemagne est une cible privilégiée de la **cybercriminalité**. Mais sa réponse apportée est en cohérence avec sa stratégie nationale et sa posture officielle. Le pays est également ciblé en raison de ses engagements géopolitiques (hacktivisme de haut niveau : Cyber-Berkut et question de l'Ukraine). L'Allemagne parle peu de ses capacités offensives, et préfère axer son discours sur la défense de la vie privée et des libertés sur internet. Son action en ligne est donc perçue comme positive, et non militariste.

La posture traditionnelle allemande est de communiquer sur la protection de la vie privée et des libertés en ligne. Mais ce message est en réalité (voir « Mise en œuvre et rôle des acteurs tiers) brouillé par les faits (lancement de son propre système de collecte, etc.). Il est aussi battu en brèche par les Etats-Unis et le Royaume-Uni qui disposent, comme moyen de pression, de l'accord de partage de renseignement préexistant entre les trois pays. Ainsi, les désirs d'investigations, par les parlementaires allemands, sur l'espionnage massif mené par la NSA risquent de ne pas se concrétiser, et les annonces risquent de rester au stade de simple annonce.

Fort est à parier que l'Allemagne continuera de soutenir son discours en se positionnant sur le terrain plus « mou » de la gouvernance, où les Etats-Unis notamment, semblent prêts à lâcher du lest (cf. récentes annonces de l'ICANN et NetMundial).

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale		
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale	Gouvernance internet	Coopération régionale
	Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée)	Protection du secteur économique	
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Etats-Unis	Royaume-Uni	France	Brésil	Europe
Cibles potentielles/ pays ennemis	-				

1.1.2. Mise en œuvre et rôle des acteurs tiers

L'Allemagne **contribue énormément à communiquer** sur la cyber (criminalité, défense, etc.) dans les médias. Le pays prend régulièrement position, qu'il s'agisse de l'affaire du cyberespionnage américain révélé par E. Snowden, que pour afficher sa place prépondérante dans la coopération internationale.

En matière de **coopération internationale**, c'est la récente opération menée contre le botnet Ramnit qui permet à l'Allemagne de communiquer sur sa gestion de la cybercriminalité.[7]

La publication par le BSI, en décembre 2014, d'un rapport[8] admettant qu'une usine métallurgique allemande a subi des dégâts matériels conséquents suite à une cyberattaque est une révélation sans précédent. Cela a été considéré par les analystes comme le deuxième **exemple historique d'une cyberattaque ayant causé des dommages physiques**, après Stuxnet. Si le rapport ne donne pas d'informations sur la date de l'attaque et l'usine concernée, il précise tout de même que les pirates informatiques ont usé de méthodes avancées. La diffusion d'un tel rapport fait partie intégrante de la stratégie de communication allemande. **Se positionnant sur le terrain de l'information et de la vérité, tout en ne diffusant que très peu d'informations sensibles sur le sujet, l'Allemagne espère ainsi convaincre de la gravité de la situation.**

L'Allemagne a eu l'occasion d'exploiter d'autres situations, comme **outil de persuasion de la société civile** d'une part, mais aussi de **tremplin pour l'affirmation d'une nouvelle position stratégique** et géopolitique d'autre part. Elle s'est, par exemple, présentée en **chef de file, avec le Brésil, d'un nouvel ordre de gouvernance se positionnant contre l'hégémonie américaine**.

> *"In an angry conversation, recently reelected German Chancellor Angela Merkel (shown) told President Obama that the surveillance tapping of her cellphone by the National Security Agency (NSA) was "like the Stasi," the infamous East German secret police."*
>
> 16/12/2013, NY Times

Par exemple, des discussions sont actuellement en cours pour suspendre l'accord nommé *Safe Harbor* entre les Etats-Unis et l'Allemagne[9]. Une dynamique qui se poursuit encore, notamment avec l'annonce de la création d'une *task force* de l'Union Européenne, destinée à enquêter sur les violations, par Facebook, de la législation européenne en matière de vie privée, menée par la Belgique, les Pays-Bas, et l'Allemagne.[10] Aussi, suite à la révélation du programme de la NSA baptisé *TREASURE MAP* (permettant de cartographier la totalité du réseau allemand), l'Allemagne a annoncé la création d'une commission parlementaire d'investigation sur les allégations d'E. Snowden et sur les activités de la NSA.

> *"NSA whistleblower Edward Snowden has told German officials he is prepared to testify over the extent to which the U.S. government tapped Angela Merkel's phone, it is claimed."*
>
> 01/11/2013, Daily Mail

---

[7] WAQAS, *Europea, Cyber Police Shuts Down World's Biggest « Ramnit » Botnet,* Hackread.com, 3 mars 2015 : https://www.hackread.com/european-cyber-police-shuts-down-worlds-biggest-ramnit-botnet (consulté le 24 mars 2015).

[8] Bundesamt für Sicherheit in der Informationstechnik, *Die Lage der IT-Sicherheit in Deutschland 2014* : https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile (consulté le 24 mars 2015).

[9] ZASKE Sara, *Germany-s privacy leaders gather to discuss suspending US Safe Harbor,* ZDNet.com, 27 janvier 2015 : http://www.zdnet.com/article/germanys-privacy-leaders-gather-to-discuss-suspending-us-safe-harbor (consulté le 24 mars 2015).

[10] ESSERS Loek, *EU data protection authorities get serious about Facebook's privacy policy,* PCWorld.com, 4 février 2015 : http://www.pcworld.com/article/2879872/eu-data-protection-authorities-get-serious-about-facebooks-privacy-policy.html (consulté le 24 mars 2015).

Mais cette position ambitieuse parait difficile à tenir. Premièrement, des révélations montrent que l'Allemagne s'attelle à **développer ses propres capacités d'interception** pour rivaliser avec les Etats-Unis.

> *"The magnitude of the eavesdropping is what shocked us,"…"Let's be honest, we eavesdrop too. Everyone is listening to everyone else. But we don't have the same means as the United States, which makes us jealous."*
>
> Bernard Kouchner, Former French foreign minister, 22/10/2013

L'attachement allemand pour le respect de la vie privée se heurte aux réalités de son système de renseignement. Le média *Die Zeit* a en effet révélé que le BND allemand collecterait plus de 220 millions de métadonnées de téléphones par jour, et en stockerait plus de 11 milliards (contre 6 milliards pour les Etats-Unis). Le BND collecterait ces données via satellites et câbles réseaux.[11]

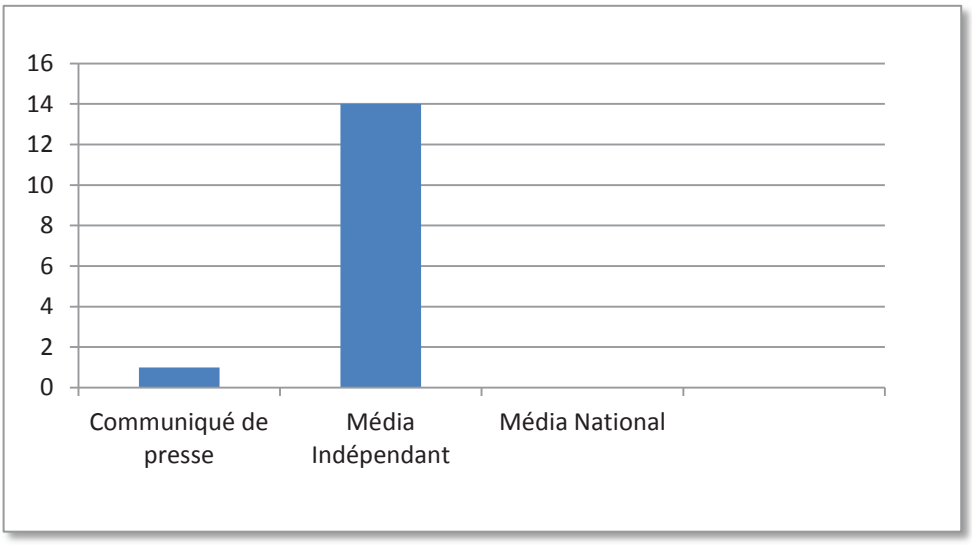
Deuxièmement, parce que l'Allemagne se heurte à une **quasi-indifférence de la part des Etats-Unis, ils** ne semblent pas prêts à fléchir sur leurs positions. Détaché, le Président des Etats-Unis Barack Obama a notamment encouragé la Chancelière Allemande Angela Merkel à relativiser la situation. Cette demande de « ne pas imaginer le pire » sur le programme d'espionnage de la NSA semble balayer d'un revers de main les exigences et la fermeté du clan d'en face, et montre bien que les Etats-Unis sont très peu affectés (ou souhaitent délibérément afficher l'indifférence) vis-à-vis des positions et de l'indignation du Brésil et de l'Allemagne.[12] Indifférence confirmée par les récentes annonces des Etats-Unis : le programme de surveillance de la NSA ne subira que des changements mineurs.[13]

Cette indifférence de façade se comprend mieux lorsque l'on sait que, suite à l'annonce, par les Allemands, de la création de la commission parlementaire susmentionnée, des officiels britanniques auraient menacé l'Allemagne de mettre fin à la coopération trilatérale entre l'Allemagne, le Royaume-Uni et les Etats-Unis.[14] Cette posture sous-entend donc que **le renseignement allemand dépendrait fortement, en termes de collecte, des puissances américaines et britanniques**.

En troisième lieu, l'Allemagne doit composer avec les pressions internes de son important écosystème hacktiviste, mais aussi venues de l'extérieur.

---

[11] BIERMANN Kai, *BND stores 220 million telephone data every day*, Zeit online, 2 février 2015 : http://www.zeit.de/digital/datenschutz/2015-02/bnd-nsa-mass-surveillance (consulté le 24 mars 2015).
[12] VOLZ Dustin, *Germany Can Stop „Assuming the Worst"About NSA Spying, Obama Says*, Defense one.com, 9 février 2015 : http://www.defenseone.com/politics/2015/02/germany-can-stop-assuming-worst-about-nsa-spying-obama-says/104928 (consulté le 24 mars 2015).
[13] SANGER David E., *President Tweaks the Rules on Data Collection*, The New York Times, 3 février 2015 : http://www.nytimes.com/2015/02/03/world/president-tweaks-the-rules-on-data-collection.html?_r=0 (consulté le 24 mars 2015).
[14] HUFELSCHULTE Josef, *Briten drohen mit Abbruch aller Kontakte zu Deutschland*, Focus online, 5 février 2015 : http://www.focus.de/politik/deutschland/geheimdienst-eklat-briten-drohen-mit-abbruch-aller-kontakte-zu-deutschland_id_4454261.html (consulté le 24 mars 2015).



Analyse des réactions collectées lors de l'étape d'échantillonnage - La place prépondérante de la presse indépendante en Allemagne.

L'Allemagne fut l'un des premiers pays à compter des hacktivistes très actifs. L'affaire dite du « *hack* KGB », révélée en 1989 en témoigne : un groupe de *hackers* de Hanovre avait réussi à pénétrer les réseaux informatiques de nombreuses sociétés occidentales et avait revendu les informations obtenues au KGB. Aujourd'hui, l'écosystème hacktiviste y est encore actif, comme le démontrent les attaques de plusieurs groupes, dont le « n0n4m3 *crew* », sur des sites gouvernementaux allemands.

Cet écosystème dispose d'une vitrine officielle particulièrement développée, à l'image du « *Computer Chaos Club* »[15] ou du parti politique des « Pirates »[16].

Cette communauté présente un message audible par la société civile. Selon un sondage international mené en janvier 2015 par YouGov[17], la figure Edward Snowden serait plus admirée que le président américain Barack Obama en Allemagne. Cette mouvance, sur laquelle l'Allemagne s'efforce de surfer grâce à une législation très protectrice des libertés et de la vie privée, risque pourtant de lui porter préjudice.

Enfin, **les médias locaux ont une portée considérable en Allemagne et dans le monde**. L'exemple de *Der Spiegel*, chef de file des médias révélant les documents collectés par E. Snowden, confirme ce point. Des contributeurs au journal, tels que l'expert en cybersécurité et hacker Jacob Appelbaum, soulignent l'engagement de *Der Spiegel* envers la communauté activiste et hacktiviste. Cette implication du principal média allemand dans l'affaire Snowden témoigne de l'existence d'un contrepoids en matière de communication grand public sur le thème de la cybersécurité.

L'Allemagne s'efforce donc de communiquer en mettant en valeur son engagement pour une autre voie que celle proposée par les Etats-Unis et leur vaste programme de cyberespionnage. Mais les révélations sur les propres programmes allemands mettent à mal cette posture, et exposent le pays aux critiques de son propre écosystème hacktiviste.

[15]CCC website : http://www.ccc.de/de (consulté le 24 mars 2015).
[16] Piraten partei website : http://www.piratenpartei.de (consulté le 24 mars 2015).
[17] YouGov UK, *World's most admired 2015 : Angelina Jolie and Bill Gates*, 17 février 2015 : https://yougov.co.uk/news/2015/01/30/most-admired-2015/ (consulté le 24 mars 2015).

L'Allemagne est également fortement exposée en raison de ses prises de position à l'échelle internationale. En janvier 2015, le groupe d'hacktivistes pro-russes CyberBerkut s'en prend aux sites gouvernementaux allemands. Ils opèrent par défiguration et y postent des messages pro-russes. Ils reprochent notamment à l'Allemagne d'aider l'Ukraine dans le conflit.[18]

[18] MARTIN Michelle, *Pro-Russian group claims cyber attack on German government websites,* Reuters.com, 7 janvier 2015 : http://www.reuters.com/article/2015/01/07/us-germany-cyberattack-idUSKBN0KG15320150107 (consulté le 24 mars 2015).

1.2. Brésil

1.2.1. Abstract

Le Brésil a profité des récents évènements (Coupe du Monde et NSA) pour affirmer ses positions en matière cyber. La Coupe du Monde a été l'occasion d'annoncer une forte montée en puissance des capacités de lutte informatique défensives et offensives du pays. En dépit de la disproportion de réaction, l'objectif était de montrer que le pays anticipe les risques. Suite à l'espionnage mené par la NSA, le Brésil a adopté une posture relativement ferme à l'égard des Etats-Unis. Le discours assez virulent a été suivi d'actes entérinant certaines mesures, notamment politiques, diplomatiques et juridiques, mais dont la plupart n'est pas concrétisée et certaines mêmes abandonnées. L'impact des GAFA, et notamment de Google, est ici essentiel. De plus, le Brésil semble faire face à la même indifférence américaine, à l'image de l'Allemagne. Cette réaction américaine de façade signerait-elle l'échec de la dissuasion cyber ?

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale		
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme				
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale	Gouvernance internet	Coopération régionale
	Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée)	Protection du secteur économique	

Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile
Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Allemagne	BRICS	Région Amérique Latine		
Cibles potentielles/ pays ennemis	Etats-Unis	Royaume-Uni			

1.2.2. Mise en œuvre et rôle des acteurs tiers

Le Brésil est régulièrement victime de la cybercriminalité. Récemment, le pays a subi une campagne importante de pharming, ciblant les routeurs domestiques[19]. Le pays a également sur son territoire des cybercriminels actifs, à l'image de ceux ayant mené l'opération « Boleto »[20].

Deux faits récents ont permis aux officiels brésiliens de communiquer sur le sujet de la lutte informatique et la lutte contre la cybercriminalité. Le gouvernement a proposé une stratégie de sécurité poussée, intégrant la protection des infrastructures critiques du pays[21].

La Coupe du Monde

Le Brésil a beaucoup communiqué pendant la Coupe du Monde, évènement ayant provoqué un véritable boom de la cybercriminalité du pays. **La coupe du Monde a été un véritable tremplin pour le Brésil, qui en a largement profité pour exposer sa stratégie de cyberdéfense**. Cette stratégie place les forces armées au cœur de la cyberdéfense du pays et de ses infrastructures critiques[22]. La Police fédérale étant, quant à elle, peu valorisée. Cette dynamique a été confirmée par les récentes annonces. Mais cette stratégie de placer la cyberdéfense et la cybersécurité (même civile) entre les mains des

[19] MIMOSO Michael, *Pharming attack targets home router DNS settings, Threat post.com,* 27 février 2015 : http://threatpost.com/pharming-attack-targets-home-router-dns-settings/111326 (consulté le 24 mars 2015).

[20] PAOLIERI NETO Fernando, *DNS Poisoning Used In Boleto* Fraud, RSA.com, 9 février 2015 : https://blogs.rsa.com/dns-poisoning-used-boleto-fraud (consulté le 24 mars 2015).

[21] Portal da Copa, *Planejamento Estrategico de Segurança para a Copa do Mundo de 2014 é publicado no DOU,* 30 août 2012 : http://www.copa2014.gov.br/pt-br/noticia/planejamento-estrategico-de-seguranca-para-copa-do-mundo-de-2014-e-publicado-no-dou (consulté le 24 mars 2015).

[22] Ministerio da Defesa, Defesa MD aprova Politica Cibernetica de Defesa, 28 décembre 2012 : http://www.defesa.gov.br/index.php/noticias/4205-28-12-2012-defesa-md-aprova-politica-cibernetica-de-defesa (consulté le 24 mars 2015).

forces armées est parfois critiquée[23], est dénoncée une militarisation du cyberespace. Les critiques portent également sur le fait que les problématiques cyber ne sont pas toutes équivalentes. La cybercriminalité, ou encore le hacktivisme, ne se gèrent pas de la même façon que la cyberdéfense des infrastructures critiques. Selon certains observateurs, le Brésil ne se positionne pas ouvertement sur le renseignement d'intérêt cyber, l'attribution des cyberattaques, etc. Mais le pays s'appuie sur de solides infrastructures de cyberdéfense. Et les menaces potentielles amenées par la Coupe du Monde ont été largement anticipées par le ministère de la Défense[24].

La Coupe du Monde a d'ailleurs vu le nombre de **revendications hacktivistes** exploser, en raison des manifestations à fondements économique et social ayant précédé l'évènement[25]. Les menaces proférées par certains pirates informatiques ont été nombreuses[26]. Les Anonymous ont lancé de nombreuses campagnes en amont, telles que #OpHackingCup ou encore #OpWorldCup. L'une des revendications hacktivistes était de critiquer les dépenses astronomiques engagées pour la Coupe du Monde, dans un contexte économique et social difficile.

"The hacker group Anonymous is preparing a cyber-attack on corporate sponsors of the World Cup in Brazil to protest the lavish spending on the soccer games in a country struggling to provide basic services, said a hacker with knowledge of the plan on Friday."

Reuters.com, 31/05/2014

Mais le fait est qu'elles n'ont pas engendré le chaos annoncé. L'évènement s'est en effet déroulé sans incident majeur.

Autre élément fort de communication : l'armée brésilienne a annoncé, avant la coupe du Monde, tester un **simulateur de cyberguerre** afin de se préparer à toute éventualité.

"The Brazilian Army has a new weapon to fight the cyber war: the National Simulator for Cyber Operations. This software, known by its Portuguese acronym SIMOC, builds training environments that simulate known virtual threats — as well as threats not yet discovered."

Dialogo Americas, 23-03-2013

Il s'agit ici clairement d'une stratégie de communication, **la réaction étant ici disproportionnée** face aux risques de hacktivisme. L'objectif était de présenter les avancées et le renforcement des capacités de l'armée brésilienne comme une réponse effective aux menaces, et non comme une démarche de militarisation.

Les révélations d'E. Snowden

Autre évènement ayant servi au Brésil de contexte idéal pour l'annonce d'une véritable stratégie cyber : les révélations, par Edward Snowden, de l'espionnage massif réalisé par la NSA sur le territoire brésilien.

---

[23] MUGGAH Robert, *Why Brazil Put Its Military In Charge of Cyber Security*, Defense one.com, 13 janvier 2015 : http://www.defenseone.com/technology/2015/01/why-brazil-put-its-military-charge-cyber-security/102756 (consulté le 24 mars 2015).

[24] El Economista, *Brasil se prepara para ataques cibernéticos durante el Mundial*, 26 février 2014 : http://eleconomista.com.mx/tecnociencia/2014/02/26/brasil-se-prepara-ataques-ciberneticos-durante-mundial (consulté le 24 mars 2015).

[25] MCKENZIE Jessica, *Protests in Brazil Turn Digital*, Tech President.com, 28 juin 2013 : http://techpresident.com/news/wegov/24107/protests-galvanize-brazilian-hacktavists (consulté le 24 mars 2015).

[26] ISRAEL Esteban et BOADLE Anthony, *Hacker group threatens cyber-attack on World Cup* sponsors, Reuters.com, 31 mai 2014 : http://in.reuters.com/article/2014/05/30/us-brazil-worldcup-hackers-idINKBN0EA29M20140530 (consulté le 24 mars 2015).

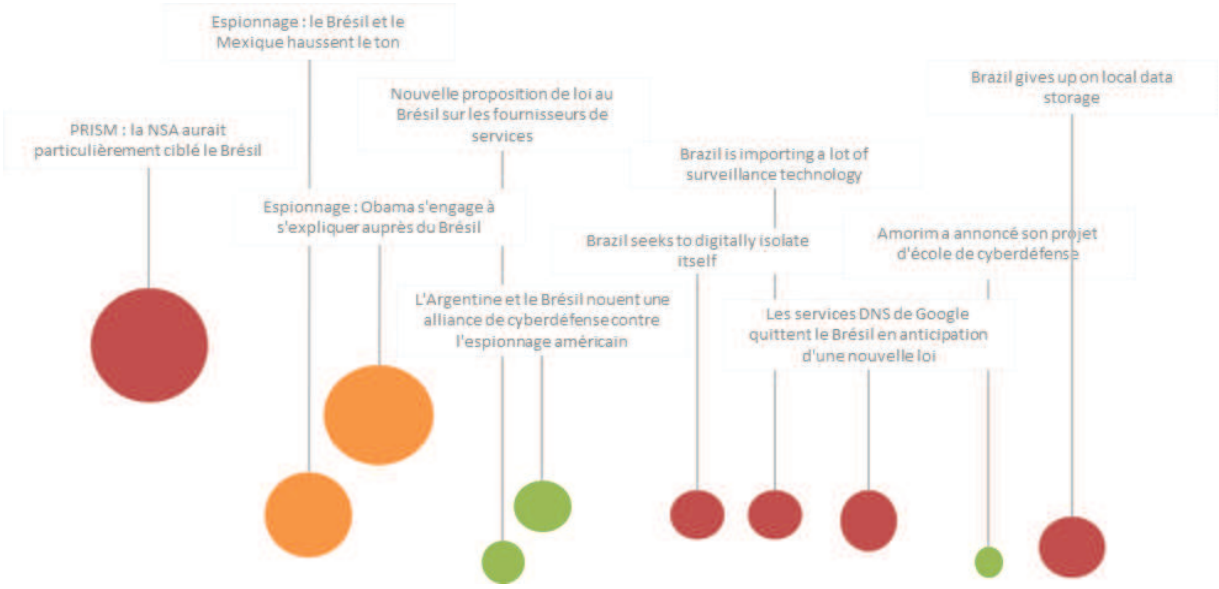


Schéma : enchaînement des réactions sur l'affaire NSA/Brésil

Les réactions du Brésil ont été virulentes : mise en place d'une commission d'enquête sur ces révélations, alliances régionales contre l'espionnage américain, mais aussi vote de mesures structurelles juridiques.

« Le Sénat brésilien a mis en place mardi une commission pour enquêter sur des faits présumés d'espionnage des États-Unis au Brésil et a réclamé la protection du journaliste à l'origine de leur révélation. La première mesure approuvée par cette Commission parlementaire d'enquête (CPI) a été de demander à la police fédérale que le journaliste du quotidien britannique The Guardian, Glenn Greenwald, qui vit au Brésil et a divulgué des documents appuyant ces accusations, reçoive une protection policière tout comme son compagnon brésilien, David Miranda. »

Lapresse.ca, 03/09/2013

Les ambassadeurs des États-Unis au Brésil et au Mexique ont été convoqués par les ministères des Affaires étrangères respectifs des deux pays pour s'expliquer sur des accusations d'espionnage par les États-Unis de communications de la présidente brésilienne Dilma Rousseff et de son homologue mexicain Enrique Peña Nieto.[27]

"*Si ces faits sont avérés, ce serait une situation inadmissible, inacceptable, qui pourrait être qualifiée comme une claire atteinte à la souveraineté de notre pays*", a réagi dimanche soir le ministre de la Justice José Eduardo Cardozo. [28]

Par la suite, Barack Obama s'est engagé à s'expliquer auprès de Dilma Roussef, présidente brésilienne, au sujet des accusations d'espionnage portées contre les Etats-Unis. Il s'est engagé à assumer la responsabilité directe et personnelle de l'enquête sur ces accusations.

Peu de temps après, une proposition de loi, obligeant les sociétés à localiser les informations recueillies au Brésil dans le pays, a été présentée au Parlement brésilien[29]. Aussi, les ministères de la Défense d'Argentine et du Brésil se sont alliés pour améliorer mutuellement leurs capacités de cyberdéfense[30].

[27] Le Point.fr, *Espionnage : le Brésil et le Mexique haussent le ton*, 2 septembre 2013 : http://www.lepoint.fr/monde/snowden-les-presidents-rousseff-et-pena-nieto-espionnes-par-washington-02-09-2013-1720153_24.php *(consulté le 24 mars 2015).*
[28] Le Point.fr, *Espionnage : le Brésil et le Mexique haussent le ton*, 2 septembre 2013 : http://www.lepoint.fr/monde/snowden-les-presidents-rousseff-et-pena-nieto-espionnes-par-washington-02-09-2013-1720153_24.php *(consulté le 24 mars 2015).*

"We need to reflect on how we cooperate to face these new forms of attack," Brazil's defense minister, Celso Amorim, said at a conference in Buenos Aires.[31]

Cette démarche globale a été critiquée par la société civile, accusant l'Etat brésilien de s'isoler numériquement.[32] Surtout, la posture brésilienne a été mise à mal suite aux révélations selon lesquelles le Brésil se serait doté d'importantes capacités d'espionnage à la veille de la Coupe du Monde[33].

Face à cette dynamique d'isolement numérique, les entreprises privées ont réagi, à l'image de Google. En réaction, certains services DNS de Google ont en effet commencé à quitter le pays tout comme ils l'avaient fait en Chine. Aucune décision officielle n'a encore été prise cependant de la part du géant d'internet américain[34].

Ces nombreuses critiques ont eu raison du projet, et la proposition de loi sur l'hébergement local des données a été abandonnée, en cause, la difficile réalisabilité du projet, et la fuite potentielle des grandes entreprises, à l'image de Google.

Seul le projet de Marco Civile, texte assurant la garantie de la confidentialité de l'usager contre toute violation ou utilisation indue des données des internautes brésiliens, a abouti. Quoi qu'il en soit, le Brésil s'est engagé comme chef de file de la dynamique de renforcement des BRICS, notamment au niveau des infrastructures internet (construction d'un câble BRICS hors de portée, en théorie, de l'espionnage américain). Cette volonté de créer un câble se situe dans le droit fil du projet vite abandonné d'Angela Merkel de créer un internet européen. Au-delà du caractère fantaisiste de la proposition, cela reflète toutefois la volonté claire de s'isoler et de se protéger de l'espionnage américain au niveau de la couche physique du cyberespace car, c'est en effet au niveau de la gouvernance internet que le Brésil a plus de chance de s'imposer.

---

[29] WINTER Brian, *Brazil's Rousseff targets internet companies after NSA spying,* Reuters.com, 12 septembre 2013 : http://www.reuters.com/article/2013/09/12/net-us-usa-security-snowden-brazil-idUSBRE98B14R20130912?feedType=RSS&feedName=technologyNews (consulté le 24 mars 2015).

[30] RT.com, *Argentina, Brazil agree on cyber-defense alliance against US espionage*, 15 septembre 2013 : http://rt.com/news/brazil-argentina-cyber-defense-879 (consulté le 24 mars 2015).

[31] RT.com, *Argentina, Brazil agree on cyber-defense alliance against US espionage*, 15 septembre 2013 : http://rt.com/news/brazil-argentina-cyber-defense-879 (consulté le 24 mars 2015).

[33] FONSECA Bruno, MOTA Jessica, BODENMÜLLER Luiza et VIANA Natalia, *Com a Copa, Brasil vira mercado prioritario da vigilancia*, Publica.com, 6 septembre 2013 : http://apublica.org/2013/09/copa-brasil-vira-mercado-prioritario-da-vigilancia (consulté le 24 mars 2015).

[34] MADORY Doug, *Google DNS Departs Brazil Ahead of New Law*, DYN.com, 22 novembre 2013 : http://research.dyn.com/2013/10/google-dns-departs-brazil-ahead-new-law (consulté le 24 mars 2015).

1.3. Chine

1.3.1. Abstract

Les annonces et réactions chinoises récentes en matière de cybersécurité sont fermes. Leur impact et les réactions des autres acteurs montrent que la communauté internationale ne dispose pas de réel levier ou moyen de pression pour contraindre les chinois, ou éluder leurs annonces/critiques. Cela témoigne aussi de l'importante indépendance de la Chine vis-à-vis de cette communauté internationale. La Chine semble assumer sa stratégie agressive d'appropriation de la propriété intellectuelle, en s'illustrant dans des opérations de cyberespionnage industriel étatique. L'indépendance de la chine s'illustre également en termes d'infrastructures réseau, grâce au Grand Pare-feu Chinois, et d'écosystème de marché (blocus à l'encontre des produits numériques américains). La Chine fait donc aujourd'hui partie des pays dont la riposte serait la plus radicale et violente.

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation

	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile
Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	OCS	Russie	Corée du Nord	Iran	
Cibles potentielles/ pays ennemis	Occident				

1.3.2. Mise en œuvre et rôle des acteurs tiers

Depuis quelques années déjà, la chine a été **désignée comme ennemi principal des Etats-Unis** en matière cyber. Avec la Russie et la Corée du Nord, la Chine concentre l'essentiel des critiques américaines.

Récemment encore, la Chine a été la cible de nombreuses actions de communication de la part des Etats-Unis. De nombreux rapports (Mandiant, Crowd Strike…) tentent de démasquer l'identité et la localisation géographique des pirates informatiques chinois. Ces entreprises publient ainsi des rapports extrêmement détaillés, assortis de documents personnels et de photos de ces supposés pirates informatiques, marquant ainsi une véritable **privatisation de la démarche d'attribution**.

La Chine a également été la cible de procédures judiciaires américaines, marquant ainsi la **judiciarisation de conflits de cyberespionnage**, jusque-là restés clandestins. Lundi 19 mai 2014, le département américain de la Justice annonce qu'un grand jury a inculpé cinq officiers de l'armée chinoise accusés d'avoir piraté les systèmes informatiques de six entreprises américaines œuvrant dans les secteurs de l'énergie - nucléaire, énergie solaire - et de la métallurgie.

En réponse**, la stratégie de communication de la Chine est rigoureuse et contrôlée extatiquement**. **Très peu de voix dissidentes** se font entendre, et il n'y a pas d'écosystème cybercriminel ou hacktiviste audible en la matière.

Selon le communiqué de presse publié par le ministère Chinois des Affaires Etrangères, Zheng Zeguang a exprimé à Max Baucus, ambassadeur des Etats-Unis, « la protestation solennelle » de la Chine et déclaré que « les Etats-Unis ont gravement violé les normes régissant les relations internationales, nuit à la coopération sino-américaine en matière de cybersécurité et porté atteinte aux liens bilatéraux en fabriquant des informations et en accusant des officiers chinois de cyber vol ».[35] On assiste ensuite à une véritable **escalade des réactions**.

[35] French Xinhuanet.com, *La Chine convoque l'ambassadeur américain après les poursuites à l'encontre d'officiers chinois*, 20 mai 2014 : http://french.xinhuanet.com/chine/2014-05/20/c_133347931.htm (consulté le 24 mars 2015).

La Chine décide d'arrêter l'utilisation du système d'exploitation Windows 8 pour tous les nouveaux ordinateurs commandés par les pouvoirs publics[36], ordonne aux entreprises publiques de ne plus utiliser les services de firmes de consulting américaines et prépare un nouveau « *cybersecurity vetting system* » pour tous les produits d'ICT entrant dans son territoire[37]. Par la suite, le gouvernement chinois rejettera en bloc les accusations américaines et dénoncera une tentative d'instrumentalisation[38]. Et c'est ainsi que l'administration américaine entame un bras de fer "commercial" - et non une "guerre froide" - avec la Chine[39]. La Chine est en effet dans **une logique de réponse diplomatique et économique de « *no business* »**.[40]

Elle se révèle le pays le plus ferme à l'égard des Etats-Unis, et le pays dont les réactions ont le plus d'impact. Cet impact peut s'expliquer par l'indépendance incontestable de la Chine vis-à-vis des Etats-Unis, en matière commerciale, diplomatique, juridique, mais aussi en matière de renseignement. Les Etats-Unis se retrouvent donc dans une position conflictuelle plus complexe à gérer qu'avec le Brésil ou encore l'Allemagne.

La Chine fait d'ailleurs partie de ces pays où la démarche cyber offensive est assumée. Sa stratégie de communication est, en ce sens, sans concessions. Sans pour autant admettre ou revendiquer ses actes, la Chine entretient le mystère et semble bénéficier d'une cyber dissuasion collatérale, grâce aux nombreuses accusations proférées à son égard. Il est par exemple avantageux en termes de dissuasion et de démonstration de capacités, pour la Chine, d'être accusée d'avoir apporté son soutien à la Corée du Nord parce que cette dernière ne disposerait pas des infrastructures nécessaires à une attaque cyber de grande ampleur.

[36] DENYER Simon, *As cyber rift deepens, China bans use of Windows 8 on government computers*, The Washington Post, 21 mai 2014 : http://www.washingtonpost.com/world/asia_pacific/as-cyber-rift-deepens-china-bans-use-of-windows-8-on-government-computers/2014/05/21/11bdb4b6-597e-4afe-ba16-ce27afa7a7d7_story.html (consulté le 24 mars 2015).
[37] KAN Michael, *China to block IT products that don't pass cybersecurity vetting,* ComputerWorld.com, 22 mai 2014 : http://www.computerworld.com/article/2489773/security0/china-to-block-it-products-that-don-t-pass-cybersecurity-vetting.html (consulté le 24 mars 2015).
[38] WEIHUA Chen et XIAOKUN Lia, *China outraged over US charges*, Chinadaily USA, 21 mai 2014 : http://usa.chinadaily.com.cn/2014-05/21/content_17531950.htm (consulté le 24 mars 2015).
[39] FINKLE Jim, MENN Joseph et VISWANATHA Aruna, *US accuses China of cyber spying on American companies*, Reuters.com, 20 mai 2014 : http://in.reuters.com/article/2014/05/20/us-cybercrime-usa-china-announcement-idINKBN0DZ1HV20140520 (consulté le 24 mars 2015).
[40] WHITTAKER Zack, *It's official: NSA spying is hurting the US tech economy,* ZDNet.com, 25 février 2015 : http://www.zdnet.com/article/another-reason-to-hate-the-nsa-china-is-backing-away-from-us-tech-brands (consulté le 24 mars 2015).

1.4. Corée du Nord

1.4.1. Abstract

La Corée du Nord ne dispose que de très peu de faits d'armes à son compte. Le plus récent, l'affaire Sony, fait encore l'objet de contestations. En cause, la faiblesse de ses infrastructures et de ses capacités internes. Mais si la Corée du Nord nie être à l'origine du piratage, force est de constater que lui attribuer ce piratage ne peut que renforcer sa position, à l'échelle internationale, d'« ennemi à craindre » sur le plan cyber.

En somme, la Corée du Nord, seule, ne semble pas être un Etat à risque sur le plan cyber. Mais la puissance de ses alliés et soutiens que sont la Chine et la Russie en font un pays avec lequel il faudra composer dans les années à venir.

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique

Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	OCS	Russie	Chine	Iran	
Cibles potentielles/ pays ennemis	Occident				

1.4.2. Mise en œuvre et rôle des acteurs tiers

Il y a très peu d'informations sur la façon dont la Corée du Nord communique sur la cybersécurité. Seules des allégations existent quant à l'attribution, à la Corée du Nord, du piratage de la firme japonaise Sony Entertainment, dont le studio emblématique, Hollywood, se situe aux Etats-Unis. Mais cette affaire souligne toutefois l'importance du volet « communication » au sein de la problématique de cybersécurité. Ainsi, l'outil cyber semble avoir été utilisé comme outil de riposte suite à l'annonce d'un film portant un jugement négatif sur le dirigeant de la Corée du Nord. L'acte s'inscrit donc clairement au cœur d'une guerre de l'information, visant à décrédibiliser Sony Entertainment, par la divulgation de données, etc. Toujours dans cette démarche de communication, les Etats-Unis ont pu désigner, grâce à un faisceau d'indices, la Corée du Nord comme auteur de cette cyberattaque. Cette annonce a été très critiquée, les observateurs dénonçant le manque de preuves. Même si la Corée du Nord a pu nier les faits, les Etats-Unis ont mis en œuvre des sanctions économiques et diplomatiques fortes à l'encontre du pays.

Finalement, la Corée du Nord n'a que très peu de raisons de nier catégoriquement avoir été à l'origine de l'attaque. Cette paternité lui attribue en effet des capacités cyber extrêmement importantes, et très éloignées des faibles capacités et du retard technologique qui lui étaient jusque-là associés.

Mais les incertitudes pesant sur les réelles capacités du pays sont encore très présentes. Le pays a en effet aisément été coupé d'internet plusieurs heures, et plusieurs fois de suite, rappelant la faiblesse de ses infrastructures.

La Corée du Nord semble en effet avoir besoin de ses alliés (Iran, Syrie, Russie ou Chine), pour mener des attaques de grande ampleur. Ainsi, les motivations de la Corée du Nord couplées aux capacités techniques de ses alliés peuvent potentiellement représenter une menace majeure.

Dans un article du *Washington Times*[41], un dissident nord-coréen explique d'ailleurs en ce sens, que la Corée du Nord s'entraînerait régulièrement au piratage informatique des infrastructures critiques occidentales. La situation de la Corée du Nord est donc idéale :

- Le pays dispose de capacités internes avec des profils mobilisés et dédiés à la cybersécurité offensive ;
- Le pays peut faire appel aux soutiens et aux infrastructures alliées afin de palier ses lacunes internes ;
- Le pays ne dispose pas d'une surface de vulnérabilité importante :
    - Pas d'infrastructures sensibles connectées et avancées technologiquement vulnérables,
    - Pas de dépendance accrue aux systèmes d'information connectés au quotidien.
    - Ainsi, une riposte informatique contre le pays n'aurait que très peu de conséquences sur le quotidien et la continuité des services publics.

[41] GERTZ Bill, *Defector: North Korean hackers threaten* West, Washington Times, 4 mars 2015 : http://www.washingtontimes.com/news/2015/mar/4/inside-the-ring-north-korea-cybersecurity-hackers- (consulté le 24 mars 2015).

1.5. Etats-Unis

1.5.1. Abstract

Handicapés par l'affaire Snowden, les Etats-Unis semblent opter pour une stratégie de « laisser couler ». En dépit des excuses présentées à l'Allemagne et au Brésil, les Etats-Unis ne modifient pas leur système d'espionnage massif. Mieux encore, ils demandent aux Etats, de façon triviale, de ne pas se faire d'idées sur la réalité des activités menées par la NSA. Cette posture témoigne du fait qu'en dépit de l'affaire Snowden, les Etats-Unis restent confiants dans leur influence et leur prépondérance sur de nombreux terrains : économique, marché, renseignement, etc.

Leur stratégie de communication est globale, et se positionne tant sur le soft power (lancement de jeux vidéo cyber, mais aussi de séries TV dédiées à la cybercriminalité) que sur le hard power (annonce de riposte aux cyberattaques par des moyens conventionnels, etc.). Les Etats-Unis souhaitent prendre les devants et influencent les plus hautes instances, dont le CCDCOE (ayant publié le manuel de Tallinn, premier manuel juridique traitant des cyber conflits), afin d'influencer la coutume internationale.

Ils usent aussi de tous les moyens d'influence plus conventionnels : secteur de la recherche, colloques et évènements, documents stratégiques… mais aussi judiciaires. La mise en accusation des officiers chinois, la récente extradition du pirate russe vers leur sol, témoignent de l'hyper activité américaine sur ce terrain.

Enfin, les Etats-Unis ne nient qu'à demi-mot la paternité des cyberattaques qui lui sont attribuées par la presse. Ceci parce que, même si ces découvertes sont appréhendées négativement par la société civile et les Etats, elles sont de véritables démonstrations de force et participent à faire des Etats-Unis un adversaire compétent en matière cyber.

Les Etats-Unis sont, enfin, l'un des pays impliquant le plus les acteurs privés au cœur de sa stratégie. Le rôle des détenteurs de contenus (Facebook, Google), de matériel (Apple, Microsoft), mais aussi celui des entreprises de cybersécurité (Mandiant, Crowdstrike) est de plus en plus important.

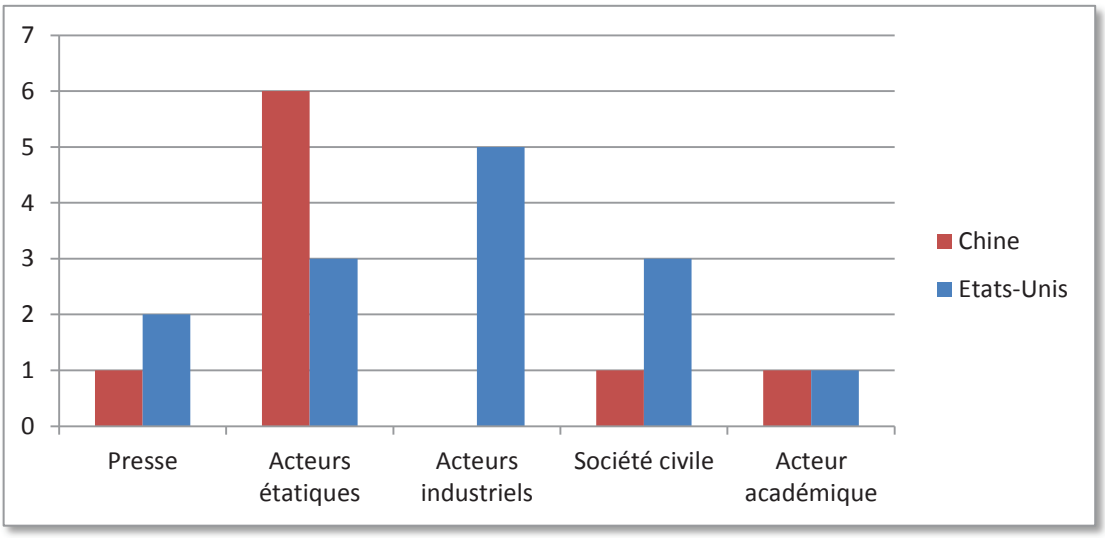
Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			

Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

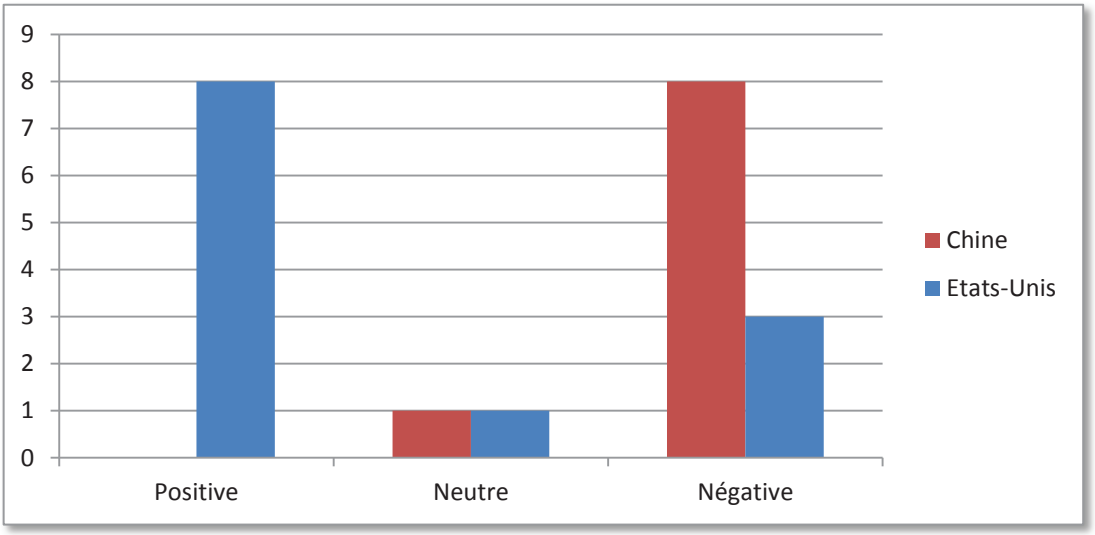
Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	OTAN	Continent américain	Europe	Israël	Japon
Cibles potentielles/ pays ennemis	Iran	Corée du Nord	Chine		

1.5.2. Mise en œuvre et rôle des acteurs tiers

Dans un contexte difficile suite aux révélations d'Edward Snowden, les Etats-Unis frappent fort en mettant en accusation des officiers chinois pour piratage informatique. Ceci est un précédent : les Etats-Unis souhaitent par cette judiciarisation de l'espionnage (acte inamical) étaler sur la place publique les méfaits de leurs ennemis chinois, rendre concrète cette menace jusque-là en deçà du seuil jusque-là réprimé. Ils souhaitent également regagner la confiance de la société civile en s'affichant comme des victimes, mais aussi comme des « justiciers » vis-à-vis du piratage informatique venant de Chine. Peu de temps après, la société privée CrowdStrike publie un rapport détaillant les activités d'un groupe proche de celui mis en cause par le DoJ. Bien que critiqué, ce rapport souhaite appuyer techniquement les affirmations du DoJ. La réaction chinoise ne se fait pas attendre tant sur les plans diplomatiques et politiques, qu'économiques : arrêt des discussions, boycott du matériel informatique américain, contre-accusations, etc.



Types d'acteurs ayant réagi



Tonalité des réactions

L'étude de cet évènement et de la cascade de réactions ayant suivi témoigne de l'importance de l'axe de la protection économique comme angle d'attaque des problématiques cyber. Elle illustre également la mise en œuvre de plusieurs types de « ripostes » en matière de cybersécurité.

- La **réponse économique** par le boycott ou l'embargo sur le matériel IT ;
- La **riposte judiciaire** en remettant dans le scope du droit pénal un acte jusque-là jugé inamical ;
- La **riposte technique** des entreprises privées se lançant dans l'investigation et dans un exercice d'attribution arbitraire et peu vérifiable ;
- La **riposte diplomatique** par l'arrêt des canaux de discussion traditionnels entre les pays concernés.

Ici, les Etats-Unis souhaitent s'engager dans une démarche qui parle à la société civile. Ils veulent en faire un exemple.

Les Etats-Unis ont opté pour une communication mettant en permanence en avant leurs capacités technologiques et offensives. La DARPA[42], agence de recherche américaine, participe grandement à cette stratégie, en diffusant régulièrement des informations sur certains projets en cours, à l'image de Memex, outil permettant de monitorer le dark net.

Les Etats-Unis ont choisi de « fabriquer » leurs ennemis en se concentrant sur quelques pays : la Chine, la Russie, l'Iran et la Corée du Nord. C'est ainsi que toutes les publications, qu'elles soient étatiques, ou d'entreprises privées sous-traitantes, vont en ce sens, et dévoilent constamment des opérations dont les auteurs sont l'un de ces quatre Etats. La stratégie de communication semble ainsi être rodée, et les entreprises privées, le relais idéal.

Le paradoxe américain réside dans le fait qu'en dépit de cette posture offensive, les Etats-Unis restent un pays avant-gardiste, et hébergeant une forte communauté hacktiviste. Leur gestion de la gouvernance est critiquée, mais acceptée car efficace. Et ils n'hésitent pas à adopter des mesures sans précédent sur, par exemple, la neutralité du net.

Les Etats-Unis disposent, enfin, d'une posture de super cyber puissance incontestable. En dépit de l'affaire Snowden, les Etats-Unis disposent encore de nombreux leviers et arguments pour maintenir leur système au *statu quo*. Leur maîtrise des données, des protocoles et des infrastructures physiques constitue un avantage considérable en faveur de leur stratégie de communication.

Autre élément clé de leur stratégie de communication : constamment exposer la menace. Cette exposition et cette diffusion de l'information vient légitimer toute action défensive.

[42] MCCANEY Kevin, *DARPA wants new tech for protecting privacy*, Defense systems.com, 3 mars 2015 : http://defensesystems.com/articles/2015/03/03/darpa-brandeis-pivacy-protection.aspx (consulté le 24 mars 2015).

1.6.Iran

1.6.1. Abstract

Les déclarations, rumeurs, et opérations attribuées à l'Iran confirment que le pays souhaite se positionner sur le terrain de l'affrontement asymétrique. Objectifs : minimiser l'influence cyber occidentale et se positionner comme puissance majeure dans sa région[43].

"Cyber warfare doesn't require a significant number of troops or a superior set of bombs [...] Iran was the first to capitalize on that."

David Kennedy, TrustedSec[44]

L'Iran a rebondi sur l'affaire Stuxnet en en faisant l'élément justifiant sa position désormais agressive dans le cyberespace. L'Iran souhaite maîtriser son cyberespace, et désormais riposter. Cette riposte peut être commerciale, diplomatique, informelle (via Twitter et la diffusion d'informations) ou cyber (voir le piratage d'Adelson Sands Corp.).

Axes de Coopération :

- ➔ Iran et Russie : les deux pays ont récemment annoncé renforcer leur coopération militaire[45]
- ➔ Iran et Irak : les deux pays ont récemment annoncé renforcer leur coopération militaire[46]
- ➔ Chine et Corée du Nord.

L'Iran semble s'empêtrer dans un cyber conflit avec l'Israël[47] et les Etats-Unis[48], ses deux principales cibles.

L'Iran se positionne dans un contexte favorable à l'escalade de conflits cyber : la transposition en ligne des considérations autour de son processus d'acquisition de l'arme nucléaire est enclenchée. Sur un autre plan, **la Russie semble prête à jouer de ses contacts avec l'Iran pour influencer l'action des américains vis-à-vis de l'Ukraine**. Récemment, un article titrait que « si les Etats-Unis arment l'Ukraine, la Russie arme l'Iran ». Cette perspective n'est pas à prendre à la légère et pourrait se transposer à la dimension cyber du conflit Russie-Ukraine.

---

[43] WALLS Mike, *Why Iran Hacks*, Darkreading.com, 29 janvier 2015 : http://www.darkreading.com/perimeter/why-iran-hacks/a/d-id/1318862 (consulté le 24 mars 2015).
[44] BERTRAND Natasha, *Iran Is Officially A Real Player In The Global Cyber War*, Business Insider UK, 8 décembre 2014 : http://uk.businessinsider.com/iran-is-officially-a-real-player-in-the-cyber-war-2014-12?r=US (consulté le 24 mars 2015).
[45] RFI, *L'Iran et la Russie renforcent leur coopération militaire*, 20 janvier 2015 : http://www.rfi.fr/europe/20150120-iran-russie-renforcent-leur-cooperation-militaire (consulté le 24 mars 2015).
[46] LAGNEAU Laurent, *L'Irak et L'Iran ont signé un mémorandum d'accord visant à renforcer leur coopération*, Zone militaire, 31 décembre 2014 : http://www.opex360.com/2014/12/31/lirak-liran-ont-signe-memorandum-daccord-visant-renforcer-leur-cooperation-militaire (consulté le 24 mars 2015).
[47] BENNETT Cory, *Israel, Iran locked in escalating cyber war*, The Hill, 4 mars 2015 : http://thehill.com/policy/cybersecurity/234489-israel-iran-locked-in-escalating-cyber-war (consulté le 24 mars 2015).
[48] WAQAS, *NSA Documents Expose Increasing Cyberwarfare Between Iran and the US*, Hackread.com, 26 février 2015 : https://www.hackread.com/nsa-document-expose-increasing-cyberwarfare-between-iran-us (consulté le 24 mars 2015).

Les nombreuses déclarations et postures de l'Iran en font un candidat idéal pour une escalade de cyberconflits. L'Iran se positionne tant sur la dimension informationnelle des cyberconflits, que sur la dimension opérationnelle, par l'acquisition de capacités offensives. Les deux aspects se croisent, lorsque l'Iran communique et tente d'influencer la communauté internationale, au sujet de sa montée en capacités cyber offensives. Enfin, l'Iran use de l'outil judiciaire pour également influencer la communauté internationale et dénoncer les exactions attribuées aux américains.

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Chine	Corée du Nord	Russie	Irak	
Cibles potentielles/ pays ennemis	Etats-Unis et alliés	Israël			

1.6.2. Mise en œuvre et rôle des acteurs tiers

Avant l'affaire Stuxnet, l'Iran communiquait peu sur la cybersécurité, et plus précisément sur sa dimension offensive. Depuis, l'Iran est devenue l'une des menaces principales pour l'occident, et plus précisément du point de vue des Etats-Unis.

L'Iran se positionne comme un acteur qui veut compter dans le domaine cyber. Et il faut souligner que la fermeté des annonces du pays reste cohérente avec d'une part les rumeurs circulant dans la presse quant aux ambitions iraniennes, que la découverte et l'attribution d'attaques de grande ampleur au pays.

Des annonces fermes et ambitieuses et l'esquisse d'une stratégie

Le piratage des infrastructures d'enrichissement nucléaire iraniennes a été l'occasion pour l'Iran de se positionner en victime au regard de la communauté internationale[49], et de communiquer sur le développement de ses capacités de riposte informatique. Certains estiment même que la vague de piratages ayant touché l'Iran aurait permis aux Iraniens d'« apprendre » et d'enrichir leurs connaissances de l'usage offensif des outils cyber[50].

Depuis, l'Iran semble avoir une stratégie ferme et assumée de riposte et de montée en puissance. Ali Khamenei appelait, dès début 2014, les étudiants du pays à se préparer à la cyberguerre, usant de métaphores religieuses pour souligner l'importance de ce nouveau terrain dans la stratégie du pays à long terme.

> *"You are the cyber-war agents and such a war requires Ammar-like insight and Malik Ashtar-like (two Prophet's Companions in early Islamic history) resistance"*
>
> Supreme Leader of Iran, Ayatollah Khamenei, 2014[51]

Ses relations avec des pays comme la Syrie, la Corée du Nord ou la Chine en font un adversaire majeur.

A cette stratégie, il faut ajouter l'ambition de créer un « internet iranien » (en réalité, un vaste intranet). Mais cette annonce initialement ferme, de quasi autarcie numérique, laisse aujourd'hui place à de nou-

[49] VAHDAT Amir, *Iran concerned by cybersecurity report*, The Salt Lake Tribune, 18 février 2015 : http://www.sltrib.com/home/2193441-155/iran-concerned-by-cybersecurity-report (consulté le 24 mars 2015).
[50] GREENWALD Glenn, *Iran's Cyber Warriors Have Learned Their Lessons From US Cyber Attacks, NSA Document,* Mattewaid.com, 11 février 2015 : http://www.matthewaid.com/post/110724833546/irans-cyber-warriors-have-learned-their-lessons (consulté le 24 mars 2015).
[51] Mehrnews.com, *Leader says soft warfare „a demanding field"*, 2 décembre 2014 : http://en.mehrnews.com/detail/News/102031 (consulté le 24 mars 2015).

velles déclarations plus ouvertes[52] à l'égard des technologies étrangères, occidentales[53], des annonces laissant penser que l'Iran aurait fait encore évoluer sa stratégie numérique[54].

Enfin, l'Iran n'hésite pas à se positionner sur la scène internationale par des prises de position claires. Le pays n'a pas hésité à communiquer, par exemple, sur les récentes révélations selon lesquelles la NSA américaine aurait piraté les clés de chiffrement des cartes SIM diffusées par l'entreprise GEMALTO.

Tweet d'un iranien, ouvertement opposé aux technologies américaines

Au final, la posture iranienne vise à exploiter à son plein potentiel les perspectives offertes par la maîtrise du cyber, qu'il s'agisse de la maitrise de l'information, des infrastructures nationales, mais aussi la maîtrise des techniques et outils offensifs. L'Iran veut affirmer sa maîtrise du réseau en refusant, puis acceptant certaines technologies étrangères, mais aussi en bloquant certains protocoles. Ce fut le cas en février 2015, lorsque le pays a blacklisté le réseau TOR sur son territoire[55].

Mieux encore, l'Iran semble, souhaiter maîtriser les outils juridiques à sa disposition : le pays aurait annoncé il y a quelques temps déjà, désirer poursuivre les Etats-Unis pour le piratage de leurs infrastructures d'enrichissement nucléaire.

Des rumeurs allant dans le sens d'une ferme volonté de peser sur le terrain cyber

L'Iran pourrait porter devant les tribunaux internationaux l'affaire Stuxnet. C'est ce qu'aurait affirmé un responsable iranien tenant à conserver l'anonymat.

« Le temps est venu d'une action en justice. Le Département d'Etat recueille actuellement des documents pour initier une action à l'échelle internationale. Les responsables américains joueront un rôle important dans cette démarche de collecte de preuves. En outre, l'Iran a pu déceler un fort consensus sur le sujet, parce que de nombreux pays se sentent aujourd'hui en danger »

Un responsable iranien, anonyme, http://irannuc.ir/content/1513

[52] MACLEAN Wiliam et KASOLOWSKY Raissa, *Rouhani urges end to Iran's isolation*, Reuters.com, 4 janvier 2015 : http://www.reuters.com/article/2015/01/04/us-iran-economy-rouhani-idUSKBN0KD0CG20150104 (consulté le 24 mars 2015).
[53] ESSERS Loek, *Iran ready to work with Google, other global internet companies*, PCWorld.com, 2 mars 2015 : http://www.pcworld.com/article/2891312/iran-ready-to-work-with-google-other-global-internet-companies.html (consulté le 24 mars 2015).
[54] BEJTLICH Richard, *Why Would Iran Welcome Western Tech ?*, Tao Security, 2 mars 2015 : http://taosecurity.blogspot.fr/2015/03/why-would-iran-welcome-western-tech.html (consulté le 24 mars 2015).
[55] HOWELL O'NEILL Patrick, *Iran blacklists tor network, knocking 75 percent of users offline*, Darkwebnews.com, 30 juillet 2014 : http://darkwebnews.com/news/iran-blacklists-tor-network-knocking-75-percent-users-offline (consulté le 24 mars 2015).

La viabilité de ce dossier face aux instances internationales a d'ailleurs été confirmée par certains experts : Stuxnet pourrait être qualifié d'agression armée[56]. Si ce projet est mené à bien, il s'agirait d'une première en la matière.

Autre rumeur, celle selon laquelle l'Iran aurait déjà riposté à l'attaque Stuxnet. Cette hypothèse n'est cependant pas vérifiée.[57]

Des opérations de grande envergure attribuées à l'Iran confirment les annonces et les rumeurs

Fin décembre 2014, la société Cylance révélait l'Operation Cleaver. Cette opération d'espionnage d'envergure aurait été menée par l'Iran, à l'encontre d'acteurs occidentaux militaires, du secteur de l'énergie, des transports, des hôpitaux, et de l'aérospatial. Si l'Iran a officiellement démenti être à l'origine de cette opération, de nombreux indices le désignent comme auteur.

> "*This is a baseless and unfounded allegation fabricated to tarnish the Iranian government image, particularly aimed at hampering current nuclear talks,*"
>
> Hamid Babaei, spokesman for Iran's mission to the United Nations, Reuters.com

Autre affaire, le piratage d'Adelson Sands Corporation, attribué à l'Iran. L'Iran aurait piraté la société suite aux déclarations de son CEO, Sheldon Adelson. Ce dernier aurait déclaré souhaiter utiliser l'arme nucléaire contre l'Iran. Ce type de réaction confirme la dynamique de riposte engagée par l'Iran.

[56] GlobalResearch, *US-Israeli Stuxnet Cyber-attacks against Iran: "Act of War",* 26 mars 2013 : http://www.globalresearch.ca/us-israeli-stuxnet-cyber-attacks-against-iran-act-of-war/5328514 (consulté le 24 mars 2015).
[57] BENNETT Cory, *Snowden file : Iran hack may have* backfired, The Hill, 10 février 2015 : http://thehill.com/policy/cybersecurity/232343-did-iran-learn-cyber-expertise-from-us-attacks (consulté le 24 mars 2015).

1.7. Estonie

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	Renforcement de la recherche
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	OTAN	Europe			Japon
Cibles potentielles/ pays ennemis					

1.8. Corée du Sud

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	-				
Cibles potentielles/ pays ennemis	Corée du Nord	Chine			

1.9.Israël

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Etats-Unis	Europe			
Cibles potentielles/ pays ennemis	Iran	Corée du Nord	Chine		

1.10. Royaume-Uni

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Etats-Unis	Europe	OTAN		
Cibles potentielles/ pays ennemis	Iran	Corée du Nord	Chine		

1.11. Russie

Stratégie de communication					
Thématiques	Cybercriminalité	Hacktivisme	Terrorisme	Espionnage	Lutte informatique
Messages principaux	Valorisation de la SSI technique	Renforcement de la législation	Identification d'un ennemi	Riposte et lutte informatique offensive	Renforcement de la dimension économique
	Protection de l'individu	Sécurité nationale	Souveraineté nationale	Propriété intellectuelle	
Emetteurs	Officiels	Politiques	Judiciaire	Société civile	Entreprises
Tonalité	Positive	Négative	Agressive	Anxiogène	Frustrée
	Ferme	Discrète			
Outils / moyens de pression	Légaliste et lutte contre la cybercriminalité	Dissuasion par démonstration de force et usage de l'offensif	Influence internationale et gouvernance internet	Guerre de l'information	Coopération régionale
	Indépendance / Position dominante préexistante (économique, renseignement, etc.)	Protection des intérêts nationaux	Protection de la société civile (vie privée) ou du secteur économique	Indépendance infrastructures physiques d'Internet	Blocus économique
Vecteurs et relais d'opinion	Culture et soft power	Outils juridiques	Evènements et conférences	Think tanks et recherche	Ecoles et formation
	Réseaux sociaux	Presse	Entreprises spécialisées	Diplomatie	
Cibles	Jeunesse	Pays rivaux	Pays alliés	Entreprises	Société civile

Dynamique cyber					
Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Chine	Corée du Nord	Iran	Irak	
Cibles potentielles/ pays ennemis	Etats-Unis et alliés	Israël	Ukraine	Certains pays d'ex-URSS	

[Page blanche]

Partie 2. Analyse des risques, conséquences et réactions

1.1. Tendances identifiées et facteurs clés d'évolution

Les risques ou les conséquences possibles d'une action d'un pays ou d'un organisme en matière de LIO et les réactions possibles de la part d'autres puissances ne peuvent être évalués qu'à l'aide de deux critères. D'une part, il est nécessaire d'identifier les postures de chaque Etat ou organisme. D'autre part, il faut tenir compte des facteurs ou leviers contextuels, pouvant influencer ces risques, conséquences et réactions. Le rôle croissant des hacktivistes, les incertitudes sémantiques et désaccords sur les définitions, la montée de l'espionnage « *as a service* » et l'usage de pirates informatiques comme intermédiaires, mais aussi la crédibilité d'un Etat ou la défiance de sa société civile, sont autant d'éléments susceptibles de faire évoluer les postures actuelles dans le temps. Les Etats ou organismes peuvent en effet tenter de s'adapter. Objectif : rester en deçà du seuil d'acceptabilité par la société civile, mais aussi du seuil de qualification juridique de la lutte informatique offensive. L'une des caractéristiques essentielles de toute cyberattaque est en effet sa discrétion première.

1.1.1. Fuites de données et guerre de l'information : rôle croissant des hacktivistes

Le hacktivisme est initialement perçu comme une activité peu nuisible. Leurs actions se situent sur le terrain de la guerre de l'information, et plus précisément de la perturbation massive, du soulèvement de foules en ligne, etc. Cela s'est vu lors de la Coupe du Monde de football au Brésil. Les manifestations en ligne ont accompagné les manifestations de rue. Les hashtags dédiés ont connu un succès considérable. Mais ce même exemple démontre le peu d'impact de ce soulèvement, bien qu'important. Les manifestations numériques n'ont pas perturbé le déroulement de l'évènement. Le hacktivisme se rapproche ainsi du concept de *script kiddies*. La majorité des acteurs – *script kiddies* – étant des novices en informatiques, considérés comme inoffensifs du point de vue de la sécurité nationale. Il n'existe en effet aujourd'hui aucun indice permettant d'affirmer que ces acteurs pourraient perturber ou atteindre des infrastructures critiques étatiques. Cela rejoint le discours tenu par les autorités françaises lors de l'#OpFrance, opération menée par le collectif AnonGh0st suite aux attentats de Charlie Hebdo. Les termes employés sont fermes et visent à minimiser – ou rétablir la vérité – sur l'impact de la vague de défiguration sans précédent ayant touché la France : « un non-évènement » (FIC 2015) ; « une menace réelle, mais à relativiser » (BFMTV) ; une opération de « guerre de l'information » (Twitter).

Mais juger l'impact de ces actions vis-à-vis de leur conséquences sur les infrastructures critiques, c'est évaluer les activités de ces groupes hacktivistes avec la mauvaise échelle d'évaluation. Car sur le terrain qui est le leur, la guerre de l'information, les actions hacktivistes sont finalement redoutables et efficaces. Leur but n'est pas de pirater les infrastructures critiques, mais bien de perturber la perception qu'ont les particuliers, les entreprises, et les institutions, de l'information. En défigurant des sites internet par milliers, les pirates informatiques du collectif AnonGh0st ont souhaité véhiculer leur message. Et cet objectif a été atteint.

L'opération menée en réaction, par le collectif Anonymous mais aussi par d'autres acteurs, #OpISIS ou par Goat Team, est également un succès sur le terrain de la guerre de l'information. Objectifs : pour les Anonymous, détruire ou fermer les plateformes de communication ou de relais des messages terroristes ou islamistes (fermeture de sites internet, de forums ou de comptes Twitter) ; et pour la Goat

Team, décrédibiliser le message des djihadistes sur Twitter, notamment, par l'humour et la dérision (création de faux comptes parodiques, parodies de vidéos diffusées par Daesch, etc.). Leur action sur ce terrain est redoutable et fait contrepoids face à des acteurs exploitant les médias sociaux à leur plein potentiel.

Autre exemple, l'affaire Snowden, située elle aussi sur le terrain de l'information, a eu un impact considérable sur la perception qu'ont les différents acteurs des opérations cyber menées par les Etats-Unis. L'impact est irréversible et la crédibilité des Etats-Unis a été atteinte. Les conséquences sur les entreprises sont considérables, ces dernières perdant des marchés, en raison de la perte de confiance générée.

La montée en puissance de le hacktivisme sur le terrain de la guerre de l'information est donc un facteur important, et à ne pas négliger. Cette montée en puissance peut influencer les postures des Etats et organisations.

1.1.2. L'incertitude de la notion de cyberterrorisme

Une des notions les plus complexes à saisir aujourd'hui est celle de « cyberterrorisme ». Que recouvre ce terme ? Les terroristes actuels peuvent-ils un jour user de l'outil cyber pour mener leurs actions offensives ? Le piratage d'une infrastructure critique (distribution d'eau, d'électricité, etc.) fera-t-il un jour partie de l'arsenal de ces acteurs, appelant généralement au meurtre et à la guerre de l'information ?

L'exemple de Daesch, groupe terroriste très penché sur les nouvelles technologies, permet d'évaluer les potentialités de l'usage de l'arme informatique à des fins de terrorisme.

> *« We've begun to see signs that rebel terrorist organizations are attempting to gain access in cyber weaponry »*
>
> David De Walt, FireEye, au sujet de l'Etat islamique (EI) pour le Financial Times[58]

L'analyse, en sources ouvertes, des capacités cyber de l'Etat islamique révèle qu'en dépit d'une presse souvent alarmiste, l'organisation ne dispose pas, aujourd'hui, des capacités de menacer par une cyberattaque les infrastructures critiques d'un Etat. Les éléments sont toutefois réunis pour envisager sur le long terme une montée en puissance, notamment en raison de l'importance des moyens financiers dont dispose l'organisation. La préparation d'une cyberattaque d'ampleur nécessite des moyens techniques, des moyens humains et une forte connaissance des systèmes ciblés (SCADAs ou autres). Cela ne signifie cependant en aucun cas l'indice que l'Etat islamique dispose de capacités permettant de réaliser une cyberattaque de grande envergure. Pirater un SCADA exige une connaissance accrue du fonctionnement du système lui-même. Un obstacle que l'Etat islamique ne pourra franchir que par trois moyens : la formation de ses propres membres ; le recrutement[59] exogène de « djihadistes en herbe » auprès des élites ou des professionnels opérant ces systèmes ; la mobilisation de hackers experts sympathisants.

L'Etat islamique[60] semble disposer de capacités de développement informatique (voir l'application de type « réseau social » intitulée « *The Dawn of Glad Tidings* »), associées à la volonté d'utiliser le chiffrement. L'organisation dispose par ailleurs des fonds nécessaires à l'achat de kits d'attaque vendus sur

[58] KUCHLER Hannah, *Warning over Isis cyber threat*, FT.com, 18 septembre 2014 : http://www.ft.com/cms/s/0/92fb509c-3ee7-11e4-adef-00144feabdc0.html (consulté le 24 mars 2015).
[59] Ces capacités de recrutement sont également soutenues et renforcées par les moyens financiers importants.
[60] Cf. OMC, note trimestrielle, Septembre 2014

les marchés noirs de la cybercriminalité. Mais, même si la prudence est de mise, ces capacités financières et l'accès aux outils des marchés noirs ne représentent pas une réelle menace pour l'instant :

- Ces outils ne sont pas suffisamment nocifs pour permettre le lancement d'attaques contre des infrastructures vitales ; ces dernières nécessitant du ciblage, du repérage et du développement dédié ;
- Les malwares vendus en kit sur les marchés noirs ne permettent que des actions de faible intensité (DDoS, vol de données, etc.) et seront, au mieux, exploitées à des fins de financement.

En conclusion, l'organisation terroriste dispose de certaines capacités de développement, notamment pour la mise à jour de son application de chiffrement des communications, ou de hacking, à l'image de Junaid Hussein. Mais ces hackers ne semblent pas – aujourd'hui - disposer des compétences et des infrastructures nécessaires au lancement d'attaques plus complexe qu'un déni de service, d'un piratage de boite email ou de cartes bancaires. Ainsi, en dépit de la volonté affichée de former ses membres aux bases du *hacking*, l'Etat islamique ne possède pas aujourd'hui les capacités de lancer une attaque contre une infrastructure critique.

Le seul scénario probable aujourd'hui est l'usage du cyber comme facteur de perturbation massive, en parallèle d'une attaque physique plus classique. Très probable, l'attaque physique semble cohérente avec la démarche agressive menée par l'Etat islamique envers les pays de la coalition ; et l'usage d'internet comme outil de déstabilisation est dans le droit fil de leur utilisation adroite faite jusque-là du cyberespace. Bien que réfutées, les récentes rumeurs[61] de préparation d'attaques du réseau électrique américain, ou de stations de métropolitain françaises ou américaines soulignent la crainte croissante d'une attaque cinétique. Les piratages de comptes Twitter par des sympathisants de l'Etat islamique illustre le potentiel de nuisance de l'organisation adossée à ses « proxies ».

1.1.3. Attribution, proxies et espionnage *as a service*

Les Etats sont nombreux à entretenir le flou sur leurs liens avec certains groupes hacktivistes. Ces groupes agissent parfois en total cohésion avec les objectifs géopolitiques de ces Etats, et sont par conséquent tolérés sur le territoire. Les Etats les cautionnant fonctionnent dans une logique d'action sur le cyberespace « par proxy ». Plusieurs niveaux de relations avec ces proxies sont identifiables : les Etats peuvent les tolérer passivement, les soutenir ou les financer activement.

Cette logique est déjà fortement présente au sein des conflits internationaux (Russie et Cyber-Berkut ; Syrie et Syrian Electronic Army, etc.). Mais elle risque de s'étendre à tout type d'acteur. En effet, la logique de mercenariat, ou encore d'espionnage *as a service* (EAAS) est une tendance croissante. Véritable business model, l'EAAS permet de faire appel à des acteurs totalement indépendants pour dérober des informations ou procéder à du piratage informatique. Cette mouvance présente la particularité de brouiller les pistes lorsqu'il s'agit d'attribuer les actes à un Etat.

1.1.4. Attribution : la dimension juridique tient un rôle essentiel

La dimension juridique joue un rôle essentiel, au cœur des stratégies cyber des Etats. La mise en œuvre du virus Stuxnet par les Etats-Unis en est la parfaite illustration. L'objectif étant justement que le virus ne soit pas perçu, démasqué par les différents acteurs.

[61] WIRE CNN et BURCH Wendy, *Officials Reject Iraqi Report of ISIS Terrorist Plot Against US Subway Systems*, KTLA 5, 25 septembre 2014 : http://ktla.com/2014/09/25/us-officials-refute-iraqi-report-of-new-york-subway-plot-by-isis (consulté le 24 mars 2015).

Dans son ouvrage « *Confront and Conceal : Obama's secret wars and surprising use of american power* », le journaliste David E. Sanger relate que le personnel chargé de l'élaboration d'Olympic Games aurait passé une majeure partie de son temps à s'assurer que le virus ne violerait pas le droit des conflits armés. Cette information surprenante n'est pas sans rappeler le débat désormais récurrent portant sur la qualification d'une cyberattaque en agression armée. Les instigateurs d'Olympic Games auraient ainsi écarté, un à un, tous les critères de cette agression, en se garantissant : l'anonymat (pas d'imputabilité à un acteur étatique) ; la discrétion des effets du virus qui, passant pour de simples dysfonctionnements, évitaient de causer des dommages suffisamment graves et quantifiables pour atteindre le seuil exigé par la qualification d'agression telle que perçue par le Conseil de sécurité de l'ONU.

Ainsi, influencer les perceptions des différents acteurs peut également passer par l'absence de perception. La discrétion et la non-attribution sont des postures clés en matière de lutte informatique offensive.

1.1.5. L'attribution et le cas de la dissuasion

Dans leur stratégie de communication, les Etats se considérant comme des cyber puissances (actuelles ou en devenir) ont un objectif commun principal : dissuader l'ennemi d'attaquer. Cette dissuasion est finalement la clé de nombreuses stratégies de communication autour de la lutte informatique offensive. Faut-il menacer, ou rassurer ? Faut-il revendiquer une cyberattaque, ou laisser planer le doute ? Mieux encore, faut-il laisser planer le doute, tout en semant les indices suffisants pour une attribution ? Faut-il mettre en avant, au contraire, la puissance de feu de l'écosystème hacktiviste pouvant être un proxy redoutable en cas de cyberconflit ?

Les Etats-Unis tiennent à cet égard une posture extrêmement intéressante. Les autorités américaines ont en effet œuvré pour que l'opération Stuxnet tienne le juste équilibre entre la force de frappe nécessaire à son efficacité, et la discrétion nécessaire à sa durée de vie. Mais cette discrétion a été mise à mal. Le virus a été découvert, et la stratégie des Etats-Unis a rapidement évolué pour tirer profit d'une situation au départ embarrassante. Les Etats-Unis ont en effet opté pour un discours dual. D'un côté, le discours public et assumé, est de nier toute implication des Etats-Unis dans la création du virus Stuxnet, en dépit du faisceau d'indices accablant. De l'autre côté, des officiels ont laissé circuler des informations extrêmement précises sur la genèse et la conception du virus dans les locaux du Président américain, par l'intermédiaire du journaliste David E. Sanger dans son ouvrage dédié.

Les Etats-Unis se dirigeraient-ils vers une stratégie plus « ouverte » consistant à assumer l'adoption de cyber capacités offensives ? La publication de ce livre, la diffusion d'offres d'emploi explicitement tournées vers l'offensif ou les récents projets de la DARPA abondent en ce sens. Certains évoquent même l'apparition d'une nouvelle « forme alternative de dissuasion, plus proche des modèles connus et conçue comme un objectif à long-terme où les instruments classiques de la diplomatie pourraient également être utilisés évacuant également les questions d'attributions des attaques[62] » ; dissuasion qui encouragerait certaines cyberpuissances émergentes à assumer, à leur tour, l'élévation de leurs capacités offensives dans le cyberespace[63].

Le général des Marines à la retraite, James Cartwright, l'a affirmé :

---

[62] Cidris, *L'Inde développe sa LIO ou comment la cyber-dissuasion évolue*, 12 juin 2012 : http://cidris-news.blogspot.fr/2012/06/linde-developpe-sa-lio-ou-comment-la.html (consulté le 24 mars 2015).
[63] JOSEPH Josy, *India to add muscle to its cyber arsenal*, The times of India, 11 juin 2012 : http://timesofindia.indiatimes.com/india/India-to-add-muscle-to-its-cyber-arsenal/articleshow/14004730.cms?referral=PM (consulté le 24 mars 2015).

« Pour que la cyber dissuasion fonctionne, il faut réunir certaines croyances : un, que nous sommes résolus à passer à l'action ; deux, que nous avons les capacités techniques de le faire ; et trois, que nous l'avons déjà fait – et tout le monde sait que nous l'avons déjà fait. »[64].

1.1.6. Le passif et la crédibilité d'un Etat : l'exemple américain et l'impact irréparable de l'affaire Snowden

L'exemple américain apporte de nombreux éléments. D'une part, nous savons que la protection de leur tissu économique justifie la judiciarisation des cyberconflits traditionnellement en-deçà du scope du juge. Ainsi, si le Brésil brandit l'argument juridique et législatif, les Etats-Unis optent pour l'argument judiciaire en traduisant leurs adversaires devant le juge.

Ensuite, cet « *indictment* » est un élément fort de communication :

- Sachant pertinemment que les officiers chinois ne seraient jamais réellement traduits devant le juge, les Etats-Unis s'exercent ici à une campagne de communication visant à exposer publiquement les agissements de l'ennemi. Objectif : l'exposer, le sortir de la traditionnelle basse intensité caractérisant les conflits informatiques. Les Etats-Unis prennent donc le parti de communiquer ouvertement sur les attaques subies.
- Cette stratégie est bien reçue des industriels qui souhaitent que l'on protège leurs activités. Elle est également moyennement bien reçue par la société civile américaine.
- Cette perception est différente en Chine, où les particuliers qualifient cette opération américaine d'absurde. Les officiels ont, quant à eux, une perception très négative, menant à des réactions sévères.

Mais cette opération n'a pas eu l'effet escompté. La perception globale de l'activité américaine dans le cyberespace reste négative et associée à la violation de la vie privée et à la maîtrise exagérée des infrastructures du cyberespace.

1.1.7. L'indépendance économique, stratégique, diplomatique et son influence sur les postures

La réaction chinoise à la mise en cause des officiers chinois pour espionnage est essentielle. Elle se caractérise, à l'image de la réaction brésilienne vis-à-vis des Etats-Unis, par une franchise et une radicalité forte. Ces Etats pensent disposer d'une liberté d'action et d'une marge de manœuvre importante *[Espionnage : le Brésil et le Mexique haussent le ton] ; [Espionnage : Obama s'engage à s'expliquer auprès du Brésil] [Les services DNS de Google quittent le Brésil en anticipation d'une nouvelle loi] [Le gouvernement chinois aurait ordonné aux entreprises publiques de ne plus utiliser les services de firmes de consulting américaines].*

Leur indépendance financière, économique, scientifique, mais aussi en matière de renseignement est suffisamment aboutie pour leur offrir la possibilité de rompre des négociations diplomatiques, des échanges commerciaux, voire de prendre leur indépendance en matière d'infrastructures. La panoplie de réactions chinoises illustre donc l'impact essentiel de l'autonomie dans d'autres secteurs, afin de disposer de leviers de pression plus francs que de simples menaces.

Dans le même sens, certaines réactions fermes n'aboutissent pas, en raison de ce manque d'indépendance. L'exemple type est celui de l'Allemagne. En dépit de sa véhémence à l'égard des Etats-Unis suite à l'affaire Snowden, les Etats-Unis et le Royaume-Uni ont rapidement coupé court à

[64] BARNES Julian E., *Pentagon Digs In on Cyberwar Front*, The Wall Street Journal, 6 juillet 2012 : http://www.wsj.com/articles/SB10001424052702303684004577508850690121634 (consulté le 24 mars 2015).

toute prétention allemande d'enquêter sur les révélations d'E. Snowden, agitant la menace de la suspension de la coopération des trois pays en matière de renseignement. Encore un exemple renforçant le caractère déterminant de cette notion d'indépendance entre pays.

1.1.8. Le rôle des entreprises privées

Aussi, le rôle des acteurs privés semble être de plus en plus important. Au même titre que les Etats, les entreprises privées peuvent faire partie d'un axe de coopération et peser lourd à l'échelle internationale. Qu'il s'agisse de la gestion des infrastructures physiques du cyberespace, des protocoles ou encore des données et des services, les entreprises maîtrisent à elles seules presque la totalité des couches physiques, logiques et sémantiques du cyberespace. Les données transitent par elles, les Etats dépendent de leur connectivité, etc.

Au-delà des traditionnels GAFA qui s'imposent par leur puissance économique, les entreprises de cybersécurité viennent renforcer les capacités de certains Etats, notamment en matière d'attribution. Les Etats-Unis, avec Crowdstrike, ou encore la Russie avec Kaspersky, symbolisent la démarche d'attribution privatisée qui semble se généraliser. L'impact que peuvent avoir de telles entreprises sur les prises de position actuelles et futures des Etats est considérable. Ces entreprises sont donc un pivot essentiel à intégrer à l'analyse prospective.

1.1.9. Le ROI de l'usage de l'arme informatique

La notion d'utilité de l'usage de l'arme informatique doit également être prise en compte dans l'anticipation des postures des Etats. L'arme informatique est souvent présentée comme une arme peu chère, à la portée de tous, et aux effets redoutables, favorisant les acteurs plus faibles dans le cadre de conflits asymétriques. Mais force est de constater que ces avantages peuvent rapidement être battus en brèche par la réalité :

- Son faible coût est à relativiser. Il est nécessaire de disposer du matériel, de l'infrastructure nécessaire à son développement, mais aussi des talents humains. Le fait que les campagnes d'espionnage ou de sabotage les plus efficaces ont été développées par des Etats démontre au contraire qu'il est nécessaire de disposer de moyens important pour développer des armes informatiques capables de causer des dégâts suffisants pour remplacer l'arme traditionnelle.
- Le fait que l'arme informatique ne soit pas réutilisable vient aussi relativiser son faible coût. Une phase de redéveloppement est toujours nécessaire afin d'adapter l'arme à sa nouvelle cible.
- De plus, il a été démontré que l'ennemi apprend rapidement. Ce dernier peut en effet se protéger contre les attaques du même acabit à venir. L'impact de la réutilisation d'une arme informatique sur la même cible est donc incertain.
  L'ennemi peut également procéder à de l'ingénierie inversée sur ce programme informatique, et s'approprier l'outil afin de créer lui-même ses propres armes informatiques. Attaquer un Etat reviendrait-il à l'instruire ?
- Enfin, force est de constater que les effets d'une cyber arme sont loin d'être garantis.

Ainsi, rien ne permet d'affirmer que certains Etats privilégieront l'usage de l'arme informatique. Cette incertitude doit être prise en compte dans l'analyse prospective des postures étatiques.

Un élément peut toutefois faire pencher la balance en faveur de cet usage. Si la société civile est sensible aux problématiques d'espionnage et de protection de la vie privée, l'acceptabilité, par la société

civile, de l'usage de l'outil cyber peut être influencée par la notion de guerre « propre ». Les particuliers sont en effet sensibles à la possibilité de régler les conflits sans mettre en péril des vies humaines.

1.1.10. La riposte à la LIO n'est pas nécessairement de la LIO

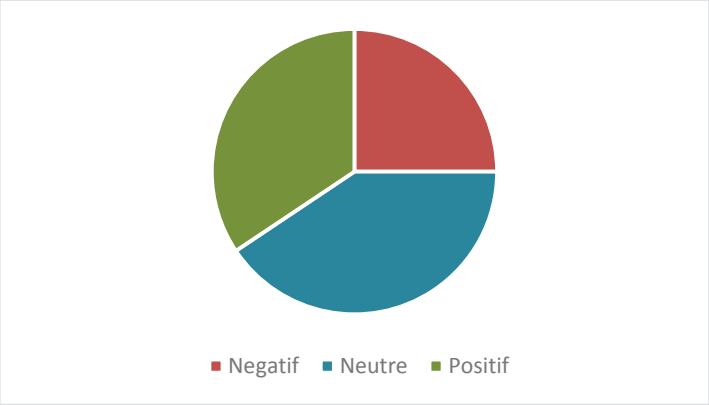
L'éventail de ripostes mises en œuvre par les acteurs est extrêmement large. Du politique, diplomatique, en passant par l'économique, le technique ou le juridique, les Etats savent qu'ils ont de multiples moyens de faire entendre leur voix sur le cyberespace. Ces axes de riposte sont appuyés par de nouveaux axes de coopération : le Brésil et l'Allemagne se sont présentés comme chefs de file d'un anti-américanisme croissant suite à l'affaire Snowden. Cet axe se renforce grâce aux travaux menés par le Brésil, notamment au sujet de la gouvernance internet. Mais ces réponses aussi variées soient-elles ne sont que la partie visible de l'iceberg. Elles font partie d'une opération plus globale de communication auprès des acteurs de la société civile. Objectifs :

- dans une logique de riposte ouverte : légitimer les activités de riposte de type LIO dans le cyberespace ; légitimer la surveillance et la maîtrise accrue des réseaux *[Brazil is importing a lot of surveillance technology]* ; légitimer l'acquisition de capacités et de puissance dans le cyberespace *[Amorim a annoncé son projet d'école de cyberdéfense]*
- dans une logique d'action clandestine : communiquer sur des valeurs chères à la société civile (neutralité du net, liberté d'expression, la « troisième voie ») *[Brazil gives up on local data storage, demands net neutrality]*

La stratégie est donc ici claire : communiquer sur les canaux traditionnels de réponse lors de rivalités étatiques, afin de préparer une riposte sous-jacente bien plus nocive. Cette riposte est toutefois destinée à rester sous le scope des radars judiciaires et politiques.

Cette stratégie est à mettre en perspective avec les éléments objectifs dont nous disposons sur certains Etats (cf. fiches pays). Le Brésil, par exemple, est en pleine montée en puissance quant à ses capacités offensives cyber (LIO). Sa stratégie de montée en puissance en LIO est ainsi masquée indirectement par son activisme juridique vis-à-vis de valeurs telles que la neutralité du net et la protection de la vie privée (législation, NetMundial…) *[Brazil gives up on local data storage, demands net neutrality]*, mais trahie par sa vision expansionniste en termes de maîtrise des infrastructures physiques du cyberespace (construction d'un câble BRICS dont ils auraient une grande maîtrise). *[Brazil seeks to digitally isolate itself]*

La communication du Brésil est donc bien ficelée : sa volonté de maîtriser le cyberespace étant légitimée par l'impérieuse nécessité d'échapper à l'espionnage américain. Cette communication est aujourd'hui perçue positivement par les acteurs de la société civile, ces derniers étant séduits par la « troisième voie » proposée par Dilma Roussef.



Tonalités des réactions recensées

Ainsi, Dilma roussef semble bien moins inquiétée en matière cyber qu'en matière de politique générale, économique et sociale. Ce versant de la position brésilienne n'est pas à négliger : **les contestations sociales peuvent se reporter en ligne** *[Anonymous ataca sites brasileiros em protesto contra Copa do Mundo]*. Les acteurs de la société civile tels que les hacktivistes peuvent alors faire de la stratégie brésilienne dans le cyberespace une cible privilégiée à décrédibiliser.

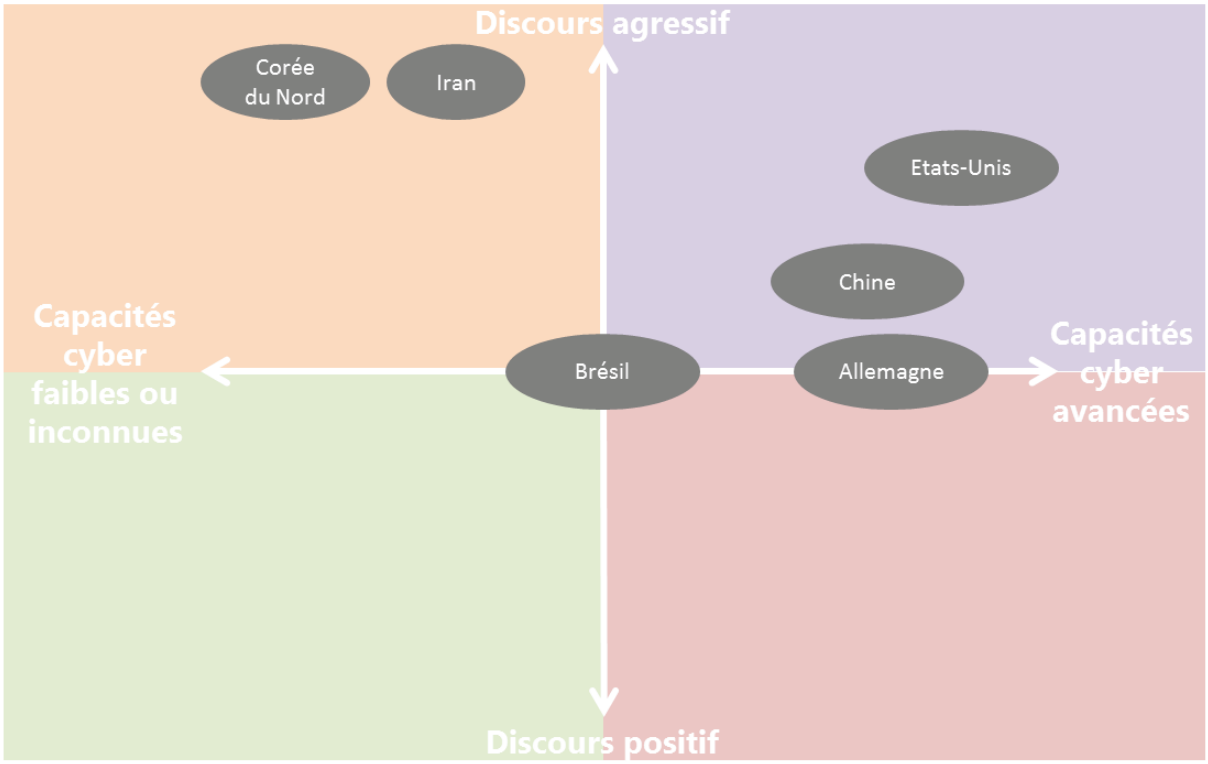
Mais cette stratégie de victimisation n'est pas toujours si efficace, comme le prouve l'exemple américain.

1.2. Conclusions : postures et perspectives

A ce stade de l'étude, il est nécessaire : de mettre en perspective les Etats selon la force de leur discours et leurs capacités réelles ; d'analyser les principaux facteurs susceptibles d'influer sur les positions des pays et acteurs, objets de l'étude ; de proposer quelques scénarios d'évolution globale à moyen terme, comme notamment l'émergence probable de plusieurs « blocs » susceptibles de partager des visions communes sur telle ou telle thématique.

1.2.1. Capacités cyber effectives vs. Discours et stratégie de communication

Le schéma ci-dessous représente une synthèse du positionnement des pays. Objectif : distinguer la réalité des perceptions, et mieux comprendre les postures des Etats. Cette synthèse repose sur l'analyse de deux critères. Le premier critère, la nature du discours, se fonde sur le vocabulaire employé par les officiels et représentants du pays, sa dimension négative ou positive, son agressivité, sa fermeté ou son caractère conciliant. Il s'agit d'examiner la stratégie de communication du pays. Ce pays se situe-t-il sur une stratégie de dissuasion par la menace, avec un discours agressif ? Ou est-il plus discret et plus axé sur la coopération internationale ? Le second critère, les capacités cyber effectives du pays, repose sur les travaux menés dans le cadre de l'Observatoire du Monde Cybernétique. Cet Observatoire constitue une base de données regroupant des informations vérifiées et quantifiables, proposant une photographie des capacités cyber d'un pays à un instant donné. Les menaces proférées par un Etat seront-elles suivies d'effet ? Les Etats les plus discrets sont-ils à craindre ? En effet, la montée en puissance d'un Etat quant à ses capacités réelles de lutte informatique offensive n'est pas nécessairement perceptible dans sa stratégie de communication. Il est donc crucial de disposer de ces deux points de vue.



1.2.2. Risques et conséquences, par pays

Plusieurs scénarios prospectifs peuvent être envisagés. Ces scénarios et leur déroulement (probabilités, réactions et conséquences), résultent de la mise en perspective des capacités des Etats avec, sur le moyen et long terme, l'occurrence des facteurs clés d'évolution identifiés ci-dessus. Ci-dessous, les tableaux condensent :

- la probabilité qu'un pays use de l'outil cyber (par type d'usage) ;
- le type de réactions que cela provoquerait en interne, mais aussi chez les autres Etats.

Ces tableaux se positionnent à moyen et long terme.

Allemagne

L'Allemagne dispose de capacités réelles. La société civile est relativement confiante en termes de protection de la vie privée. Le pays est actuellement porté sur des déclarations anti-NSA, ce qui lui permet de conserver l'adhésion de la société civile. Mais l'effectivité de ses déclarations contre la surveillance généralisée est remise en cause en raison de sa dépendance en matière de renseignement, vis-à-vis des Etats-Unis et du Royaume-Uni.

Risque : moyen.

Type d'usage	Risque	Conséquences / réactions				
		Hacktivistes	**Société civile**	**Entreprises**	**Acteurs judiciaires**	**Autres Etats**
Espionnage	Fort	Guerre de l'information (défigurations, etc.)	Rejet des autorités Démarche de protection de la vie privée	Perte de confiance	-	Chine : • Judiciarisation • Blocus économique • Riposte non-attribuée • Risque d'escalade

LIO en soutien des activités conventionnelles en OPEX	Moyen	Guerre de l'information Fuites de données délibérées	Acceptabilité importante Notion de guerre propre	-	Notion de seuil légal et notion d'agression informatique en jeu	Autres Etats : • Guerre de l'information par l'Etat ciblé • Riposte par proxy / non-attribuée • Risque d'escalade
Surveillance des particuliers	Moyen	Guerre de l'information Fuites de données	Rejet des autorités Démarche de protection de la vie privée	Perte de confiance	Possible saisine des tribunaux par des particuliers	Iran : • Riposte • Judiciarisation possible • Risque d'escalade

Brésil

Le Brésil est en pleine montée en puissance de ses capacités cyber. Son discours traduit une prise de conscience réelle, et est particulièrement ferme à l'égard des Etats-Unis. Le Brésil n'hésite pas à aborder la question de sa montée en capacités, quitte à tenir un discours disproportionné en matière de riposte. Le Brésil a une posture avantageuse vis-à-vis des autres BRICS, ce qui peut être le point de départ de la création d'un bloc / d'une alliance en matière de cybersécurité. Le discours du Brésil est véhément sur la question de la vie privée, et croissant sur ses capacités de LIO.

Risque : moyen à court terme. Fort à long terme.

Type d'usage	Risque	Conséquences				
		Hacktivistes	Société civile	Entreprises	Acteurs judiciaires	Autres Etats
Espionnage	Moyen	Guerre de l'information : • Défiguration • Mobilisations numériques	Avis mitigé : les particuliers sont, soit convaincus de l'importance de l'espionnage ; soit indignés		-	
Surveillance domestique	Fort	Guerre de l'information : • Défiguration • Mobilisations numériques	Rejet des autorités Contexte économique et social clivant	Perte de confiance	-	
LIO en soutien des activités conventionnelles en OPEX	Moyen	-	Acceptabilité importante Notion de guerre propre	-	Notion de seuil légal et notion d'agression informatique en jeu	
Guerre de l'information	Moyen		Soutien de la société civile	Participation de la société civile	-	

LIO ciblant les infrastructures critiques	Faible	Guerre de l'information Fuites de données délibérées	Acceptabilité importante Notion de guerre propre Rejet si riposte aux conséquences graves (physiques)	-	-	

Chine

La Chine dispose de capacités importantes. Son discours est discret, mais les entreprises privées et les gouvernements n'hésitent pas à mettre au jour les opérations menées par le pays. La Chine a démontré qu'elle peut servir de renfort pour ses pays alliés (Corée du Nord et affaire Sony).

Risque : fort. Impact d'une opération conjointe avec pays alliés : très fort.

Type d'usage	**Risque**	**Conséquences**				
		Hacktivistes	**Société civile**	**Entreprises**	**Acteurs judiciaires**	**Autres Etats**
Espionnage	Fort	-	Emergence de dissidents numériques	-	-	• Riposte • Judiciarisation possible • Risque d'escalade Attribution par une entreprise privée étrangère
Surveillance domestique	Fort	Emergence de dissidents numériques	Emergence de dissidents numériques	-	-	Attribution par une entreprise privée étrangère

LIO en soutien des activités conventionnelles en OPEX	?	-	Acceptabilité importante Notion de guerre propre	-	Notion de seuil légal et notion d'agression informatique en jeu	
Guerre de l'information	Fort	Emergence de dissidents numériques Rôle des Anonymous ou équivalent croissant	-	-	-	
LIO ciblant les infrastructures critiques	Faible	Guerre de l'information Fuites de données délibérées	Acceptabilité importante Notion de guerre propre Rejet si riposte aux conséquences graves (physiques)	-	-	• Riposte • Judiciarisation possible • Risque d'escalade Attribution par une entreprise privée étrangère

Corée du Nord

La Corée du Nord dispose aujourd'hui de capacités faibles, capacités qui contrastent avec la véhémence de son discours en matière cyber. Le pays se positionne en faveur de conflits asymétriques. Dans cette optique, le pays souhaite monter en puissance et forme des experts. Le pays a montré qu'il pouvait mobiliser ses voisins pour une attaque d'envergure. Il dispose également de l'indépendance suffisante par rapport à la communauté internationale pour mener des opérations sans craindre d'éventuelles sanctions internationales ce qui décuple sa marge de manœuvre à moyen et long terme.

Risque : très fort – sur le long terme pour les infrastructures critiques des Etats occidentaux.

Type d'usage	Risque	Conséquences				
		Hacktivistes	Société civile	Entreprises	Acteurs judiciaires	Autres Etats
Espionnage	Faible	-	-	-	-	• Riposte • Judiciarisation possible • Risque d'escalade • Attribution par une entreprise privée étrangère • Sanctions économiques • Sanctions diplomatiques
Surveillance domestique	Fort	-	-	-	-	
LIO en soutien des activités convention-nelles en OPEX	-	-	-	-	-	
Guerre de l'information	Fort		-	-	-	

LIO ciblant les infrastructures critiques	Fort	Guerre de l'information Fuites de données délibérées	Acceptabilité importante Notion de guerre propre Rejet si riposte aux conséquences graves (physiques)	-	-	

Etats-Unis

Les Etats-Unis disposent de capacités considérables qui ne sont plus à démontrer. Le pays investit dans la formation et la recherche et développement. En dépit d'une opinion de la société civile déstabilisée par l'affaire Snowden et de la perte de confiance générée, les Etats-Unis profitent encore de leur posture de cyber-puissance dominante. Leur discours est constant et ferme.

Risque : fort.

Type d'usage	**Risque**	**Conséquences**				
		Hacktivistes	**Société civile**	**Entreprises**	**Acteurs judiciaires**	**Autres Etats**
Espionnage	Fort	Guerre de l'information (défigurations, etc.)	Rejet des autorités Démarche de protection de la vie privée	Perte de confiance	Possible judiciarisation du conflit Désignation publique de l'ennemi	Chine : • Judiciarisation • Blocus économique • Riposte non-attribuée • Risque d'escalade

LIO en soutien des activités conventionnelles en OPEX	Fort	Guerre de l'information Fuites de données	Acceptabilité importante Notion de guerre propre	-	Notion de seuil légal et notion d'agression informatique en jeu	Autres Etats : • Guerre de l'information par l'Etat ciblé • Riposte par proxy / non-attribuée • Risque d'escalade
LIO ciblant les infrastructures critiques	Fort	Guerre de l'information Fuites de données	Acceptabilité importante Notion de guerre propre Rejet si riposte aux conséquences graves (physiques)	-		Iran : • Riposte • Judiciarisation possible • Risque d'escalade

Iran

L'Iran est en pleine montée en puissance de ses capacités cyber. Son discours et agressif et de nombreuses opérations de haut niveau lui ont été attribuées. Le discours iranien traduit sa volonté de contre-attaquer suite à Stuxnet. Cette contre-attaque se fera sur tous les plans : guerre de l'information, juridique et judiciaire, mais aussi réutilisation des codes l'ayant autrefois ciblée (Stuxnet) ; etc.

Risque : fort.

Type d'usage	Risque	Conséquences				
		Hacktivistes	Société civile	Entreprises	Acteurs judiciaires	Autres Etats
Espionnage	Fort	Guerre de l'information (défigurations, etc.)	Rejet des autorités Démarche de protection de la vie privée	-	Possible judiciarisation du conflit Désignation publique de l'ennemi	Israël : • Riposte discrète • Guerre de l'information encouragée
Guerre de l'information	Fort	Lutte interne contre le pouvoir en place	Sympathie avec la cause Aide internationale	-	-	Tout Etat : • Appui des opérations hacktivistes sur le territoire iranien • Rôle majeur de la presse et des réseaux sociaux • Isolation de l'Iran par la scène internationale
LIO ciblant les infrastructures critiques	Fort Risque de recyclage du code des malwares ayan ciblé le pays	Guerre de l'information Fuites de données délibérées Déstabilisation des autorités	Critiques de la sécurité nationale Mouvement de suivi des hacktivistes en ligne Craintes pour la sécurité quotidienne Sentiment d'insécurité et discours anxiogène	Inquiétudes pour la sécurité Critiques de la législation pas suffisamment protectrice Mise en cause d'entreprises pour négligences	Rôle majeur Enquêtes et investigations forensiques Attribution juridique acquise	Etats-Unis : • Riposte • Judiciarisation possible : précédent judiciaire à envisager ? • Risque d'escalade • Peut constituer le foncement d'un renforcement de la surveillance des traces numériques, de la législation pour lutter contre la cybercriminalité et le cyberterrorisme

[Page blanche]

Bibliographie

1.1. Ouvrages

UNIDIR, *The Cyber Index : International Security Trends and Realities*, United Nation Institute for Disarmament Research, Genève & New York, 2013, 140 pages.

1.2. Articles de recherche

ARTICLE 19, *Computer Crime in Iran: Online Repression in Practice 2013*, Free World Centre, Londres, 2013, 70 pages.

BAKER Prentiss O., *Psychological Operations within The Cyberspace Domain*, Air War college – Air University, 17 February 2010, 28 pages.

DIPERT Randall R., *The Ethics of Cyberwarfare,* Journal of Military Ethics, 2010, 28 pages.

DOBOVSEK B, *Perception of Cyber Crime in Slovenia*, Journal of Criminal

Justice and Security, Year 12, n°4, pp. 378-396.

HP SECURITY RESEARCH, *Profiling an enigma: The mystery of North Korea's cyber threat landscape*, episode 16, august 2014, 75 pages.

HUSSAIN GHAFFAR & DR. SALTMAN ERIN MARIE, *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it*, Quallim, 2014, 129 pages.

INTELCRAWLER, *Intelligence Report: Lizard Squad / Guardian of Peace (GOP)*, IntelCrawler, Los Angeles, 2015, 36 pages.

LEWIS JAMES ANDREW, Cybersecurity and Stability in the Gulf, Center for Strategic & International Studies, Middle East program, Janvier 2014, 6 pages.

McMILLAN SJ, *A Four-Part Model of Cyber-Interactivity: Some Cyber-Places are More Interactive Than Others*, University of Tennessee, Knoxville, 33 pages

MITTER S., WAGNER C., and STROHMAIER M., *Understanding the impact of socialbot attacks in online social networks*, In ACM Web Science 2013, May 2-4th, Paris, France, 2013, 6 pages. (Extended Abstract)

NATO, *Nato Military Policy On Psychological Operations*, 22 June 2012, Mc 0402/2, 13 pages.

TAIA GLOBAL WHITE PAPER, *Native Language Identification (NLI) Establishes Nationality of Sony's hackers as Rusian*, Taia Global, Etats-Unis, 2014, 25 pages.

THOMAS TL., *Hezballah, Israel, and Cyber PSYOP,* IOSphere, 2007, 35 pages.

TIGER SECURITY, *The state of the art of digital guerrilla during the 2014Brazilian World Cup: Analysis Report*, Tiger Security Srl, Italie, 2014, 7 pages.

1.3. Documents officiels

CABINET OFFICE, *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, London, 2011, 43 pages

GROUPE DE TRAVAIL INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE, *Protéger les INTERNAUTES : Rapport sur la cybercriminalité*, Paris, février 2014, 207 pages.

MINISTRERE DE LA DEFENSE BRESILIEN, *National Strategy of Defense, première édition*, MoD, 2008, 71 pages.

MINISTERE DE LA DEFENSE ESTONIEN, *National Defence Strategy Estonia*, MoD, 2011, 26 pages.

MINISTERE DE L'ECONOMIE ET DE LA COMMUNICATION ESTONIEN, *2014-2017- Cyber Security Strategy*, MEAC, 2014, 14 pages.

MINISTERE DE L'INTERIEUR ALLEMAND, *Cyber Security Strategy for Germany*, Federal Ministry of the Interior, Berlin, 2011, 15 pages.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *National Cyber Security Framework Manual*, CCDCOE, Tallinn, 2012, 233 pages.

1.4. Sites internet

COL DIETZ Lawrence D., *A Cyber PSYOP Primer*, TAL GLOBAL, 2011: http://www.talglobal.com/a-cyber-psyop-primer/

COLLINS Steven, *NATO and Strategic PSYOPS: Policy Pariah or Growth Industry?*: http://www.psywarrior.com/natostrategicpsyops.html

Pentagon Seeks to Manipulate Social Media for Propaganda Purposes, WashingtonBlog, 2011:

http://www.washingtonsblog.com/2011/07/pentagon-seeks-to-manipulate-social-media-for-propaganda-purposes.html

Psychological Operations In The Information Age, Mars 2012:

http://developingtomorrow.wordpress.com/2012/03/28/psychological-operations-in-the-information-age/

PsyOps and Socialbots – Infosec Institute – Pierluigi Paganini – septembre 2013:

http://resources.infosecinstitute.com/psyops-and-socialbots/

1.5. Bases de données spécialisées

http://cryptome.org/

http://www.statewatch.org/

1.6. Blogs

http://blog.crowdstrike.com/

http://cloudofdata.tumblr.com/

https://www.fireeye.com/blog.html

http://jeffreycarr.blogspot.fr

http://www.lancope.com/blog

https://www.schneier.com/

http://securelist.com/

http://www.symantec.com/connect/symantec-blogs/sr

1.7. Réseaux sociaux

https://twitter.com/AnonBRNews/status/476801321581158400

https://www.facebook.com/AnonBRNews

[Page blanche]

Cette étude prospective et stratégique a été réalisée par CEIS, pour le compte du Centre d'Analyse Technico-Opérationnelle de Défense (CATOD) dans le cadre de l'appel d'offres n°2013-36 intitulé : « Description de la manière dont la cybercriminalité et la lutte informatique sont abordées par les acteurs pouvant influencer le domaine »

Compagnie Européenne d'Intelligence Stratégique (CEIS)
Société Anonyme au capital de 150 510 €
SIRET : 414 881 821 00022 – APE : 741 G
280 boulevard Saint Germain – 75007 Paris
Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60